

on-ramp

Hackers in Jail, Part Two	4
Cellular Phone Biopsy	6
Elementary Switching	9
Hacking Smartphone	11
High School Mac Hack	15
Hacking Computer Shows	16
Nynex Voice Mail	18
The Magical Tone Box	22
Letters	24
Passageways to the Internet	32
More Meeting Advice	35
Book Review: Virtual Reality	37
Digital Locks	38
2600 Marketplace	41
News Roundup	42

## OUR ADDRESS:

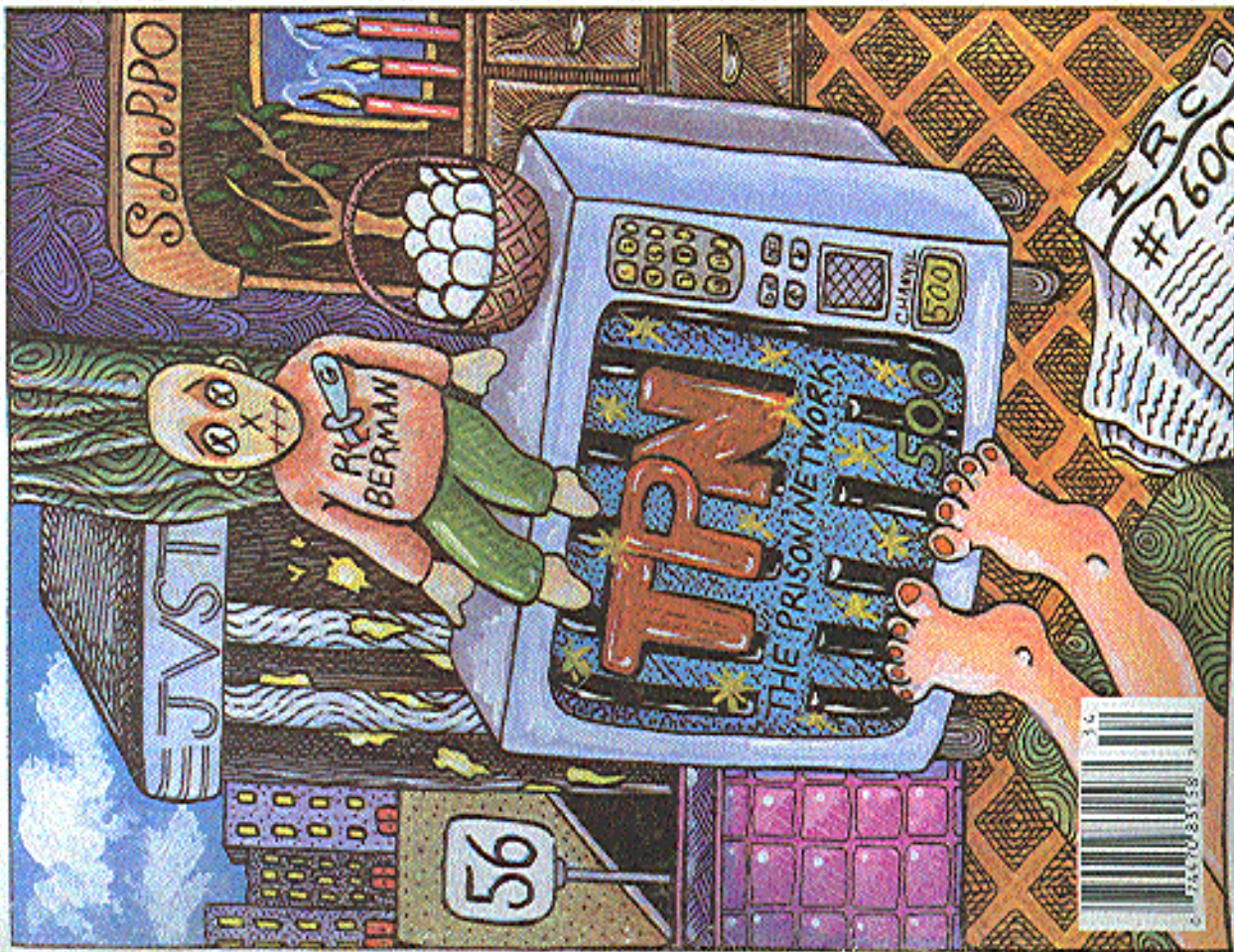
2600 Magazine  
PO Box 752  
Middle Island, NY 11953 U.S.A.

# 2600

The Hacker Quarterly

\$4

VOLUME TEN, NUMBER FOUR  
WINTER 1993-94

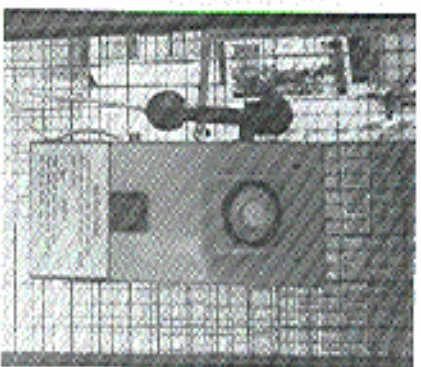




# INDIAN PAYPHONES

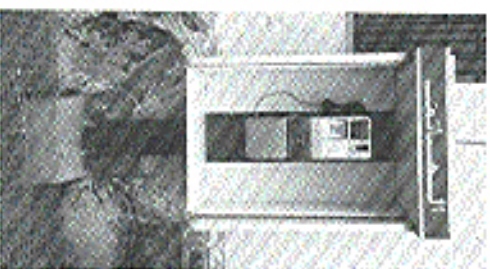


(complete with goat)



PHOTOS BY SYNTHETIC MAN

## AFRICA



CLOCKWISE FROM TOP: Vol, Kenya; Kampala, Uganda (photos by friend of Daniel Jones); Zagora, southern Morocco (photo by Drew Lehman).

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. TAKE US WHEN WE HAVEN'T GONE!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1993 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada -- \$21 individual, \$50 corporate (U.S. funds).

Overseas -- \$30 individual, \$65 corporate.

Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 at \$25 per year, \$30 per year overseas. Individual issues available from 1988 on at \$6.25 each, \$7.50 each overseas.

### ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:

2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:

2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099

INTERNET ADDRESS: 2600@well.sf.ca.us

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-751-2608

## STAFF

Editor-In-Chief

Emmanuel Goldstein

Office Manager

Tampyrol

Artwork

Holly Kaufman Sprunch

"At this time the Secret Service has no reason to believe that the suspect(s) in its investigation, or the plaintiff in this case, are aware of the nature of the Secret Service's investigation, who is under investigation by the Secret Service, what information is in the possession of the Secret Service, or who has provided information to the Secret Service in regard to this matter." Secret Service affidavit responding to CPFR Freedom of Information Act request concerning the breakup of the November 1992 Washington DC 2000 Meeting

Writers: Billie, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Ester, Mr. French, Bob Hardy, Inhuman, Kingpin, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plan, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Tommy The Cat, Mr. Upspelter, Dr. Williams, and one who writes Technical Expertise: Hugo Congrip, Puber Orsk, (see C. Tilyou, Shout Out: Robert Steele, Len Rose, Wiley.



# Hackers in Jail, Part Two

Yet again, we must pay sad tribute to a hacker who has been imprisoned. Last issue we mentioned that two New York hackers, Acid Phiber and Scorpion, had been sent to prison for six months for "crimes" that nobody was ever able to define in clear terms. Before them were the three Atlanta hackers, who served time for reading a worthless BellSouth document on a password-free computer. And Kevin Mitnick, locked up in solitary confinement because the authorities were afraid of what he could do if he got near a phone. Not to mention Shadowhawk and Len Rose, who downloaded programs that some huge company didn't want them to have and were sent away for it. They weren't the only ones but they were the ones you might remember by reading 2600 over the years. And now, there's one more.

What was unique about the Phiber Opik case was the attention it got. Here was a hacker who was not afraid to go public and show people exactly what it was he was talking about. It's precisely this kind of openness that we here at 2600 have been trying to get across for nearly ten years. After all, standing behind voice synthesizers and digital distortion tends to convey the image of somebody with something to hide. Phiber Opik was one of the first hackers to shed this mask and come forward with information. His internals went well beyond hacking - anything concerning high technology was a topic worth pursuing. Over the past couple of years, he guest lectured for various college courses on the subject of technology and the general public, made numerous appearances at panel discussions and conferences, was a frequent guest on

WBAT's *Off The Hook* radio program in New York where he would answer numerous telephone and computer related questions from listeners, and helped design three separate public access UNIX systems in New York City, the most recent one being Echo (echo.nyc.com), which introduced hundreds, if not thousands, of people to the Internet. Not exactly the life of a criminal, one has to admit. As people who have come to know Phiber well over the years, we've seen what his driving force has been: the ability to answer questions and figure things out. In the eyes of the U.S. Department of Justice, it was subversive.

On November 3rd, Phiber Opik was sentenced to a year and a day in federal prison. The charges dated back several years and were sufficiently vague to convince Phiber to plead guilty this past July. After all, a hacker can always be convicted for something and the mystery of not knowing what it is they're going to come after you for is enough to convince many people to plead guilty. (Read a little Kafka if you doubt this.) The penalty for being found guilty after pleading innocent can be much more severe. And there is also the financial consideration - legal costs can be crippling, as in the case of Craig Neidort, even after the government dropped its case against him. In Phiber's case, the charges were conspiracy and access to a federal interest computer. Conspiracy is very difficult to disprove, especially when you're friends with other hackers and you believe in sharing information. It also doesn't help when the government fears hackers as much as any national enemy. As for accessing

computers, this was never something that Phiber denied doing. But it happened years ago, it happened because of bad security, no damage was ever alleged to have been done, and Phiber always was willing to talk about security problems with anyone willing to listen. The government didn't want to hear it.

Judge Stanton, in sentencing him, said, "Invasion of computers is seductive to the young both because of the intellectual challenge and the risk. A message must be sent that it is serious.... The defendant stands as a symbol because of his own efforts; therefore, he stands as a symbol here today." In other words, because he has come to represent so much to so many, what better target for severe punishment? The total sentence was for a year and a day in prison, 600 hours of community service, and three years of supervised probation. The judge imposed no restitution because there was no evidence of any damage.

Assistant U.S. Attorney Geoffrey Benjamin was positively ecstatic with the decision. He said, "The sentence is important because it sends a message that it is a crime to intrude in public data networks. MOD was one of the biggest hacking organizations in the country. The case was very significant." MOD was the name of the group that Phiber and a few others were in at one point. Hearing it referred to as an "organization" only confirms how clueless the prosecutors were in this case. Basically, they succeeded in sending a few friends to prison for trespassing. Forgive us if we forego the champagne.

So what do we get out of this, we being the people on the receiving end of this message? Well, we've got another prisoner to take care of, at a cost

equivalent to four years in college. What we don't have is somebody who can help us hook into the Internet for the first time. We don't have the opportunity to hear another side of the story when the next technological innovation is heralded. We don't have someone to explain what might have gone wrong the next time the phone system crashes. What we've got is a warning - a warning not to stray from the safe curriculum, ask too many questions, expose embarrassing moths, or try to find answers through unconventional means.

Sending hackers to prison is a mockery of justice and one day will be recognized as such. Until that day comes, we can only hope that their lives will not be irreversibly harmed and that those of us on the outside won't push each other into a pit of paranoia as we desperately struggle to remain innocent.

On a personal level, we all feel a deep sadness here at 2600 for what has happened. We don't mean to diminish all of the other cases that have taken place and those that unfortunately will occur in the future. But this one hit rather close to home. It's going to be very difficult to go to a 2600 meeting, analyze the latest *Star Trek*, argue over UNIX, or hang out in our favorite Ukrainian restaurant without thinking of the familiar voices that have been locked out.

For those of you who would like to write to a hacker in prison, Scorpion's address is:

Paul Strig  
32095 054  
LEC Camp #1  
P.O. Box 2000  
Lewisburg, PA 17837  
Please remember that all incoming mail is read by prison authorities.



# cellular phone biopsy

by Kingpin

617

## RDT Syndicate

Cellular phones have been a popular topic discussed by media and the underground for the past couple of months. With the rumors about cellular phones causing cancer, cellular scanning laws, large flow of articles describing cell phones, and the recent news clips on cellular fraud, people of all kinds have become interested and aware of cellular technology. Many articles have been written on the technical aspect of cellular phones, but there is a lot of information dealing with the cellular phone itself which is not usually shared publicly with the entire community. As stated in the first issue of *Wired Magazine*, cellular phones have many hidden functions and abilities which the normal user does not know about.

Since owning my cellular phones, I have been constantly experimenting to uncover unknown functions. Like many people, I feel that obtaining free phone calls is not the only reason to reprogram and reconfigure a cellular phone. Going inside your cellular phone seems to be the most true form of hacking. Exploring somewhere where people don't want you to be, gaining knowledge which most people don't have, and having the ability to do things which most people cannot.

Starting at the beginning, getting an owner's manual for your phone will help explain some of the user-available functions. You should also try to get a hold of a service/technician's manual. These manuals usually contain the more technical side of the phone, including schematics and sometimes, reprogramming and reconfiguration codes to use from the keypad of the handset.

When you open up your phone, you should observe all of the components. The first one you should find is the EPROM (Erasable Programmable Read-Only-Memory). This chip is easily found, because it has a little glass window and a number,

usually 27xxx, somewhere on it. This 24, 28, or 40-pin chip contains the cellular phone's software, and other information which is "cast in stone." The data stored in this chip is unchangeable, unless you read the chip, change the code, and rewrite it.

Disassembling the code is a laborious task, but should definitely be done. The microprocessor in the phone is often a custom-made applications processor based on a specific instruction set (280, 8051, and 8085 microprocessors are all very common in cellular phones, but are not limited to these types). Be prepared to spend many hours exploring the code to find out how the phone operates and what kind of functions are available. Most EPROMs in phones have more capacity for data than actually needed, and sometimes there is plenty of room for customization.

Another key component is the EPROM (Electrically-Erasable Programmable Read-Only-Memory). Usually just battery-backed RAM, this chip can be programmed and configured to your liking from the keypad of your phone. In my own phones, the following (and plenty more) can be accessed and changed by using reprogramming codes:

### Electronic Serial Number (ESN)

Initializing the registry/memory (NIT REP)

Changing/Setting the Lock Code (LOCKCODE)

Allow Quick Recall (QRC SET)

Allow Quick Store (QST SET)

Turn the Wake-Up tone on/off (WUT SET)

Mobile to Land Hold (MLH CLR)

Land to Mobile Hold (LMH CLR)

Call Round-Up (CRU CLR)

Extended DTMF (EE SET)

No Land to Mobile (NLM CLR)

Home Alert On/Off (HAL CLR)

On/Off Diagnostics (ONL CLR)

System ID Enable/Disable (MAW)

Mobile Identification Number (MIN)

Service Provider ID (SIDH)

Initial Paging Channel (IPCH)

Extended Address On/Off (EX SET)

IPCH Scan Start - Bank A (IDCCA)

IPCH Scan Start - Bank B (IDCCB)

Access Overload class (ACCOC)

Group ID (GROUP ID)

Long-Distance Call Restriction (LU SET)

SID Max Issr (NWD ID)

System Selection (SI CLR)

Signal Strength Indicator (SSD CLR)

Audio receive On/Off

Transmit Audio On/Off

Supervisory Audio Tone On/Off (SAT)

Channel Number

Volume Control

Power Control

Hands-Free On/Off

As you can see, there is plenty of opportunity for configuration. Some phones require special codes to let you change the settings, and other phones require a special handset, cable, or dongle-key proprietary to the specific manufacturer. If your phone requires such a device, it is possible to modify an existing handset or build your own cable.

Anything that is stored in the EPROM can be changed one way or another. The EPROM can be read in most standard EPROM programmers. The RAM usually emulates a 2716 or 2764 EPROM, but by before you plug it into your programmer. Many manufacturers store the information on the EPROM in plain-text, as to not complicate it for the technicians who are performing tests on the phone.

Some companies are aware that their phones can easily be manipulated, so in order to increase security, a few steps are taken. Some phones contain LCC EPROMs instead of the standard DIP EPROMs. These EPROMs are about 1cm x 1cm, the size of the window on a standard EPROM. They perform just like standard EPROMs, except they are surface mounted, harder to erase (although they still use UV light), and because of the size, more difficult to desolder and/or clip onto. In some cases, instead of using an EPROM or RAM to store the ESN, a NOVRAM chip is used. This chip cannot be read by an EPROM programmer, thus making it extremely difficult to do without chip-specific hardware.

Security for changing the ESN is also incorporated into most of today's phones. Due to increasing problems with cell-cell operators, drug dealers, and other people using "cloning" techniques, security has increased greatly. An example follows: The software in one phone provides access to change the ESN three times from the keypad. This is done so the phone can be sold to another user, and be reprogrammed. Every time the ESN is changed, a counter stored in the NOVRAM of the CPU, keeps track. Once the ESN is reprogrammed three times, a flag is set in the EPROM and the NOVRAM, preventing any more access to the ESN from the keypad. It is possible to rid the flag in the EPROM, but since the NOVRAM is located in the CPU, and extremely difficult to read and program without special equipment, it cannot be changed and, in order to be able to use the phone again, it must be sent back to the manufacturer for a replacement EPROM and a clearing of the CPU NOVRAM. The only way to get around this security is to change the ESN by "hand", directly reading the EPROM, changing the ESN, and reprogramming. I am sure there are ways around this type of security. There always are.

There are many things which can be done by reconfiguring a cellular phone. For example, by setting the Service Provider's ID (SIDH) to 0000 (and sometimes the Group ID), the phone will be placed in "roaming mode". This mode basically means that you are not confined to the service of one cellular carrier, and can choose carriers depending on your location. I will not go into the advantages and disadvantages of roaming, which can be found in other articles.

Configuring the phone so it is able to receive cellular phone conversations is particularly fun. Since a cellular phone is able to receive much of the 800MHz band, by setting the audio receiver mode to constantly be active, you will be able to hear any audio transmitted on that particular channel. By changing channels, you can scan through the cellular frequencies, receiving other people's transmissions.



Another interesting trick which can be done is to transmit on a channel which is occupied. To do so, first set the transmit audio selection to constantly be active, and after finding a channel you want to interrupt, trigger the SAT (Supervisory Audio Tone). This will drop the person from the current call, and then you can transmit through the call site for about five seconds. I do not know exactly how this works, but I assume that you would have a higher priority for use of the channel, which would drop the other call.

Here is a partial list of cellular phone and integrated circuit manufacturers to aid in obtaining information:

AT&T: 800-225-6604  
Dallas: (408) 980-0414  
Inlet: 800-628-8686  
Motorola: 800-331-6456 (Repair)  
NEC: 800-338-9549  
NEC: 800-367-6321 (Customer Service)

NEC: 800-632-3531 (Technical Department)  
Novatel: 800-231-5100  
Novatel: 900-766-8283 (Cellular Accessories Sales)

Sanyo: 800-421-5013  
Sanyo: (201) 825-8080  
Sony: 800-222-7669  
Sony: (816) 891-7550  
Sony: (714) 229-4197 (Integrated Circuit Group)

Uniden: (317) 842-2483  
Uniden: (317) 842-1036 ex. 598 (Customer Service)  
Uniden: 800-447-0332 (Cellular Technical Support)  
VLSI: 800-473-8574  
VLSI: (408) 424-7227

This article should be used as a starting block, and was written to inform people of the vast possibilities of cell phones. You should experiment with your own phones to see what else can be done.

## HAVING TROUBLE FINDING US?

As most non-subscribers know, it can be next to impossible to find 2600 in your local neighborhood bookstore. But it's not as hard as you think. If you're in a place that you think we deserve to be in, all you have to do is:

1) *Ask an employee if they carry 2600.* They might be sold out or they may have hidden us in a "special" section. Some stores like to stock us behind other magazines, presumably so that they always know where we are.

2) *Give them our telephone number.* Tell them they should call us so we can hook them up. Say that you'd be awfully disappointed if they were to forget to do this. Appear imposing and capable of causing significant mayhem.

3) *Give us their address and phone number.* This will give us the opportunity to lean on them ourselves and get real friendly-like until we lose patience.

4) *Give up and subscribe.*

2600

PO Box 752

Middle Island, NY 11953

(516) 751-2600

## ELEMENTARY SWITCHING

By 910

Signals are sent over the telephone network to control its operation and indicate its status. Signalling is essential to the internal coordination of transmission and switching facilities. It also allows the user to submit requests to the network and allows the network to provide the user interpretable responses.

At the beginning of time, human beings employed at the local teleco central office watched for flashing lamps on their consoles to learn that someone wanted to make a call. The flashing was initiated by my Great Aunt Muriel turning a crank on her phone. The operator plugged her headset into Muriel's jack and determined through verbal interaction the person or number Muriel wanted. If the lamp at the receiving party's jack was valid, the operator rang the party's phone and connected Muriel's jack to the receiving party's. If the receiving party's lamp was lit, the operator informed Muriel that the line was in use.

If the receiving party was served by another exchange, the operator called an operator at the distant exchange through an interoffice trunk and told her the number of the receiving party. If the receiving party's lamp was valid, the distant operator rang the receiver's phone and completed the connection.

More recently, the request for service is made by simply lifting the handset, closing a 48 volt direct current (DC) circuit. The flow of current is interpreted by the switch at the central office as a request for service. This current carries two concurrent sine waves, one 3500Hz and one 4400Hz, which produce a reassuring sound in the user's earpiece, often called "dial tone". The flow of DC continues as long as the phone is off-hook, and the switching facility uses this information in supervising the line, specifically, in determining whether the line is still in use.

The number of the party to be called is

conveyed to the switch by the caller with either tones or pulses. The early telephone was equipped with a spring loaded rotating disk, which had numbered "finger holes".

After the caller spun the disk until blocked by a stationary "finger stop", the disk would unwind to its original position at a fixed speed. During its return the disk would interrupt the DC flow as many times as the number dialed was 4, as the disk revolved, the DC circuit would be broken four times for about 6/100 of a second, and restored in between each break for 4/100 of a second. Each pulse cycle took about 1/10 of a second. Newer, non-relay phones, capable of pulse dialing, interrupt the current similarly, using an electronic contact circuit. A very nimble finger can accomplish the same thing with the hang-up button. More modern phones emit a recurrent pair of sine waves to communicate numbers to the central office. On a standard dial pad, each button on the top row (1, 2, and 3) emits 697Hz; second row, 770Hz; third row, 852Hz; and fourth row (4, 5, and 6) 941Hz. Each button in the first column (1, 4, 7, and 9) emits 1209Hz; second column, 1336Hz; and third column (2, 5, 8, and 0) 1477Hz. These tone pairs are interpreted by the switching facility as the number pressed on the dial pad. Although ancient switches cannot interpret tones, raw (all) switches can interpret pulses.

The central office provides callers with an aural representation of the receiving party's phone in the act of ringing with a simultaneous pair of tones called "ring-back". They are 440Hz and 480Hz, and blip for two of each six seconds while the distant phone is ringing.

The famous "line-busy" signal is comprised of simultaneous 480Hz and 620Hz tones, blipping one half of each second until the caller hangs up. The "trunk-busy" (also called "reorder")



signal is issued when switching or transmission facilities are unable to handle the call. It is identical to the line-busy signal but sleeps at twice the rate.

When all goes well, the receiving party's telephone is sent a ringing signal, not audible at the earpiece, but usually unobtrusive a loud bell-chirping sounds, or flashing lights, often invoking considerable excitement. This is accomplished with a 20Hz signal of about 75 volts, issued for two of each six seconds until the ringing phone is picked up or the caller interrupts the flow of DC in her phone by hanging up.

A call to a party served by a central office other than one's own requires the use of one or more interoffice trunks. Older long distance lines used a 2600Hz tone to indicate that a trunk is available. When the switch began using the trunk, the caller's central office ceased its issuance of the tone. The distant office was alerted to an incoming request for service by this change.

More recently, interoffice signaling has been moved from the voice transmission circuit to a separate, dedicated circuit. A single data circuit can control thousands of voice circuits, conveying telephone number, trunk availability, and other information.

"Line-busy" signals are no longer sent from the distant office. A data signal is sent via the signal circuit, initiating the generation of the audible signal at the caller's office. Previously, sending an audio signal from the distant office required the use of a voice circuit, which is now left free for other users' conversation.

The caller's telephone number is also conveyed through the separate circuit. The distant office knows the caller's number, and the receiving party may also get it. It is sent to the receiving party's equipment as a burst of digital data, encoded by phase shift keying. The receiver's equipment must decrypt the signal, and display or otherwise act on it. Depending on the number, the call may be automatically rejected, preventing the phone from ringing, or it may be forwarded to another location.

## KNOW YOUR SWITCH

by Rebel

If you've ever wondered what kind of switch serves your exchange, you can just pick up your phone and listen. That's right - you can listen for particular sounds your line makes to find out whether you are on a #1 or #1A ESS, a #5 ESS, or a DMS 100 switch. Also, when you make a call, you can tell what kind of switch you're calling.

For example, when calling from a #1 or #1A ESS, which is an electronic switch, you will notice two short "bark-bark" sounding clicks before the phone number you are calling begins to ring. If you are calling a number that is on one of these switches, you will notice a click when the ringing line is picked up.

On digital switches such as the #5 ESS or the DMS 100, there are no clicks when calls are placed or when the other line picks up. However, there are ways to tell a #5 ESS from a DMS 100. In the New York Telephone network, if an exchange is served by a digital switch, you can dial that exchange plus the suffix "9901" and a recording will come on and tell you where the switch is located, what exchanges are on the switch, and what type of switch it is. But there is another way to tell for those outside New York. For instance, a #5 ESS has a slight single click before the dialtone when the phone is picked up. A DMS 100 has no click before the dialtone.

Also, when you call a number that is on a #5 ESS, you will sometimes get a partial first ring. When calling a number that is on a DMS 100 switch, you will always get a full ring on the first ring. Also, the first ring on a DMS 100 tends to be slightly longer than on the #5 ESS.

## Hacking Smartphone

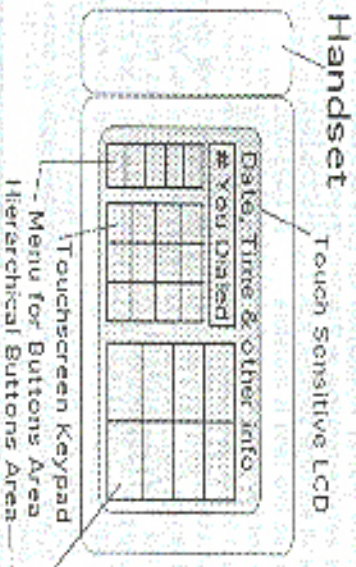
by Tech Rat

Smartphone is a soon to be released service available in some areas that will incorporate all the currently available services (call waiting, three way calling, call forwarding, caller ID, etc.) into one complete easy to use package, and combine that with a new type of phone that will access these services through an easy to use interface, which will also allow you to use custom services set up by third party providers available through Smartphone only.

The Smartphone itself has no dial and no keypad, instead, the device is about the

The interface is built around the concept of a hierarchical file system, similar to Windows or Macintosh, with a series of buttons on screen that lead you to other buttons down the menu structure. You can create and delete directory entries, and they are entered through an alpha-numeric keypad displayed on the LCD. You can set up a hierarchical structure for organizing your numbers such as "friends", "contacts", "relatives", and "emergency". Under each of these buttons on the menu tree is a listing of the names of people you have entered into the system for that button area.

Touching a displayed name on a particular button automatically dials the entry. To those of you who work with smaller "smart



size of a large office phone, having the hook and handset off to the side. The main unit consists of a touch-sensitive LCD screen that contains the interface. It sort of looks like a large Sharp Wizard with a phone handset attached. The computer that controls the Smartphone is a simple device, needing only a serial to be microprocessor and only about 128K of RAM. Upon starting, the phone reads the operating system from ROM, and then loads your phonebook from battery backed RAM, starts to the way a Sharp Wizard works.

systems, all of this will seem very academic. However, what makes the Smartphone really smart is the number of services being created to take advantage of its LCD screen and computer interface.

The first service is the white pages; imagine being able to look up anyone by dialing into the PB00 computer through a packet switching network and local dial-in point and accessing it legally through Smartphone. Anyone listed in the white pages is listed in this database stored by



the RBOC computer. You can search by area code, prefix, name, address, etc.... Any database type field is available here.

The next service is personal mailboxes. Here, you can retrieve voice messages, fax messages, email, etc.... Voices are played back through your handset, faxes are printed to your screen and can be stored locally if they are short, and E-mail can be read, but currently not replied to, since the smartphone lacks a keyboard that can be touch-typed on. This service also allows you to route your calls to another number you may be at at the time.

Next is something called Mach Services. This allows you to do all banking transactions (except deposits and withdrawals) through the Smartphone interface. In this mode, the LCD screen acts like a retarded ATM, except that it contains a few features not available on an ATM. They are: verify check; authorize credit card purchase; and checking transactions (wire money to another account). This service requires a PIN (obviously). Like all the other services, it is meant to be dialed into (and is therefore hackable, once put into service) and then accessed through the Smartphone, which is really just an LCD terminal similar to France's Minitel service.

Lastly are the Righttouch services, which allow you to turn on and off, at your discretion, call waiting, three way calling, call forwarding, caller ID, etc. As services are added, so are buttons on your interface. This service also requires a PIN.

After reviewing code for the interface that is being built into the Smartphone, I can honestly say that anyone with half a brain will be able to build a Smartphone compatible interface for their PC and be able to also dial into these services and hack away. While there is nothing about the interface that is unique, its touch screen and buttons would make it difficult for anyone to emulate without a windowing and mouse compatible computer.

All of these services and Smartphone itself are being installed as part of ISDN services, and will be made available to consumers probably near the end of 1995. Basically, to access these services, the

Smartphone dial a local number into the RBOC's packet switching network, then enters a code that corresponds to an address that connects to the service you wish to contact. While the dial-in number is always the same, it will be the addresses that vary, and it will be finding those addresses that will be the challenge of future hacking. As more services become available, you have the option of subscribing to them through the Smartphone, in which case the packet address of the service is added to your personal directory. Theoretically it should be possible to link a Smartphone with another Smartphone through the network to trade phone directories.

If you wish to try finding addresses within a packet switching network, here's the RBOC Packet for the New York metro area. These numbers are the ones I know, but there are certainly others that you can find.

- 212-385-2551
- 718-875-6504
- 914-723-2888
- 914-425-0202
- 516-559-2525
- 518-885-7878

In all cases, once connected, type 111 and then hit return. You'll see a prompt. Then try an address. It's similar to a regular phone number, like 2129250054 (this connects you to *Newsday*, a local newspaper). If you are smart, you'll be able to write a special scanner for such a network.

**IT'S A FACT.**  
If you lend your  
back issues to a  
friend, you will lose  
the issues and  
possibly your friend.  
**2600 BACK ISSUES**  
"Don't Let Them Go."

# They Can Never Win



45 Elder Drive  
Cleveland, Ohio 44114  
Phone (216) 892-7252

## TO ALL OHIO BELL EMPLOYEES:

As you know, Ohio Bell faces competitive challenges on every front. Increasing numbers of competitors are entering our markets and vigorously pursuing our customers. In this environment, information means competitive advantage and continued competitive vitality depends on preventing the unauthorized release of our proprietary information.

Recently, in spite of the face-to-face meetings, reports have been made regarding former employees accessing or copying Company information. Any such copying or accessing of information is improper and prohibited. All Company information is an asset of the Company and must be protected from unauthorized release. Marketing plans and analyses, product plans, switch replacement and cable plans, detailed sales and customer-specific data and other proprietary information are particularly sensitive. Such data must be kept confidential and should only be made available to authorized individuals, such as employees having a need to know such information in order to perform their jobs. Proprietary information should never be made available to [redacted] employees without appropriate written approval.

It is part of all our jobs to protect Company information. If you observe someone accessing Company information and you do not think the person has a legitimate reason to do so, ask the person's identity and inquire as to the purpose of the person's business. If the person is not an active employee with a reason to know such information, ask the person to leave the area and inform the Security Department as soon as possible. Should you have any questions relating to security of information, please contact the legal or Security Departments.



Controller



# Cool Letter Department

SHERIFF'S  
DEPARTMENT



DAN T. RICHARDS  
Sheriff

P.O. Box 1748  
Austin, Texas 78767

(512) 322-4610  
Fax 322-4735



October 2, 1992

Minor Threat

Mc  
Threat

Our office has recently received information that you or other persons of your acquaintance may attempt to gain access to the computer system of the Travis County Sheriff's Department.

This letter is to serve as legal notification of the criminal violations that such a breach would involve. Therefore, if any further information is received or a violation of applicable laws is attempted, the courts will be made aware that you have been served legal notice of the violations thereof. Pursuant to retirement of state laws, notwithstanding applicable Federal or Telecommunications Statutes, this office of the Travis County Sheriff's Department will prosecute to the full extent of the law, any and all such persons involved.

Investigator Michael O. Kenby-183  
Internal Affairs  
Travis County Sheriff's Department

cc: Inmate file

*Minor Threat always manages to get interesting letters like this. But getting one while in prison, now that's something....*

# High School Mac Hack

By The Bard

Following up on 999's article on high school PC hacking, I have some tips to pass on to hopeful high school Mac hackers...

To begin with, AppleShare is hard to hack. There are precious few Mac hacks around, so you must exploit the weakest link in the chain - the user.

## Collecting Passwords

There are thousands of ways to get passwords from people. The most obvious is simply asking for the password, or offering to help them login. Still, administration will probably detect most users with a paranoia about someone stealing their passwords - enough to make shoulder surfing impossible. One trick works really well, however: if you know enough programming to write a program with a passable Mac interface, you can get them to enter their passwords! Simply draw a dialog box with something like "Inward login, please reenter your name and password". (with some appropriate technobabble), and save the results to a text file, to be retrieved at leisure. Of course, if they've locked the hard drive, then you won't be able to put the program on in the first place. The solution is to make a startup disk with a slimmed down system, put your dummy program into the startup items folder, and leave it in the drive.

Don't forget that most people use obvious passwords, and if you see someone typing on the numeric keypad, try using his phone number or student ID.

## Getting Superuser Privileges

Not for the faint of heart, if you do spot a computer science teacher hard at work on his AppleShare, hang around discreetly, trying to look as stupid as possible. When he leaves the room for one reason or another, quickly leap over to his computer, make an alias of his AppleShare, and copy to disk. Then when he logs out for the day, you can go back to the computer he used, and open the alias AppleShare. If you're lucky, it should give you all his/her

privileges.

The joys of ResEdit and Norton  
(Not to mention Broadcast!)

If the hard disk isn't locked, you can use tools such as ResEdit to "personalize" applications (remember, you can really screw things up if you don't know what you're doing). I haven't taken a copy of Norton disk editor to the drive yet, but, since you can uncover hidden files, and hide visible ones, you can hide your password program, while digging for the password file (I haven't found it yet!).

Let me introduce you to a great extension called Broadcast. It enables you to send messages to other computers on AppleShare - all you have to have is a copy of it in the Extensions folder. Makes for great practical jokes - especially on Mac virgins.

I am personally opposed to destructive hacks. Destroying people's files, crashing the network, stuff like that bankrupts the hacker's name. Yet, there are thousands of non-destructive practical jokes for the Mac. For example, write a program that shuts down the computer when it is launched (use code from Spudwump in THINK Pascal), and put it in the startup folder. Thus, the computer burns off as soon as it loads up. (To get around this after the joker's gone stale, boot with the startup disk.)

## End Word

The one last place to infiltrate the system is to start early - late enough so that the AppleShare is loaded in, but early enough so the guards are not up. Try logging in as "admin" or "administration" with no password. Also, if you see something like "Fileguard" being installed, you can probably slip in an account with full privileges if you get in early enough!

Remember, most network supervisors hate what they can't control. They can snoop around your files, and do anything they want with them (remove copies of ResEdit...), but doing something as simple as DES encrypting a file called "List of passwords" or "Viral source code" can drive a supervisor crazy.



# hacking computer shows

by Walter S. Jaffee

The trading grounds of the ancient Mesopotamians, the desert auctions of Bedouin nomads and even the Crystal Palace Exhibition of 1851 can be taken as demonstrations of one proof: If you want to work the buyers into a frenzy, pack them into a tight space surrounded by wares - I mean wares - or do it?

Those who have attended any computer industry trade show or exposition must have been struck by the desire to own many of the products being displayed. Unfortunately, price is prohibitive and there is both crude and illegal. However, it is possible to convince those running the booths to give you what you want. Usually they will be delighted to do so, and offer to send you other products not on display. In a good show, I have collected as much as five thousand dollars worth of software, plus books and some peripherals.

This advice results from years of attendance at many shows, both as an observer and as a corporate representative. Every tip which follows has been used successfully, either by me or against me.

A successful show requires preparation. First, you must get yourself inside without paying. This is simple: ask yourself the question "what group can improve the success of this show?" Call the show organizers, present yourself as a representative of this group and, I promise, they'll send you a complimentary pass. Typically, I present myself as a member of the media. I have been affiliated with a mass media outlet for many years, which gives me a legitimate address and letterhead for this claim. You may want to create a dummy corporation for the same effect.

This raises a different question: should you pretend to be affiliated with a real group? On the one hand, it raises the possibility of their identifying you as a fake; on the other hand, it will greatly

increase your yield of goods collected. I have toyed with the idea of setting up a dummy consulting firm called "Walter S. Jaffee, Inc." (incorporation costs around \$65 in most states). I could then get the badge printer at a show to put WSJ as my corporate ID. Most computer salesmenures would sell their credentials for a good writeup in the *Wall Street Journal*. The WSJ badge would be magic.

Dress the part - obtaining a company T-shirt would be perfectly in line for regional media outlets. A suit would be better for a national firm. Have business cards.

Once in the doors, you have two basic routes to getting free things: you request review copies, or complain about copies you already "possess." I will take these in order.

If you presented yourself as a member of the media to get in the door, by all means keep up the disguise. Many sales people will see your badge and hand you their product without your saying a word. Others will have to be asked. Many will copy the information from your badge and mail you the product at home. Finally, many will tell you to contact them. By all means, do so. A typical conversation runs like this:

"Hello, Sally? This is Walter Jaffee, with WQQQ television; we met at the Aovon Expo last week."

"Of course, Walter, what can I do for you?"

"We're running a comparative review next month on word processors. We'll be looking at WordChopper 1.0, MicroMail Paragraph, and a few others. I was very impressed with the new release of PhallexWriter and would love to include it in the review."

"Do we have your address, Walter? I'll have that in the overnight mail."

Sometimes they send a crippled copy. Call back to explain that you have experienced computer users testing these programs in head-to-head style, and that

PhallexWriter will suffer grievously in such tests if it can't save, print, or copy. They'll send you the real thing.

Never give away that you are an experienced computer user yourself. Misuse terminology just slightly, to give the impression that you have been working in the field for a while, but don't feel comfortable with it.

For more specialized shows, present yourself as a representative of an organization with substantial buying power. Of course, you need to be high enough in the organization to influence purchase decisions, without being so high as to decide on a purchase yourself. Try being a "Systems Consultant" or the like. I highly recommend the *Dictionary of Organizations*, which you can find in any good library and which will give you an almost endless list of appropriate, real organizations which you may want to represent. The National Science Teachers Association is a perennial favorite. Beware, real members may be at the show. Your BS skills must be well-practiced to escape from such an encounter.

If the idea of collecting goods in this way bores you, try the second approach: complaining about the ones you "already have." Imagine the effect on a small company, which has shelled out 30% of its annual advertising budget to attend a show, of having a screaming, dissatisfied customer at the mouth of its booth. The sales representatives will do everything to get rid of you. At the MacWorld Expo in August, a young lady approached the booth in which I was working and gave a furious dressing-down to the company president, complaining of bugs in our software. Several things she said made it perfectly clear that she had never owned the software, but had seen our demo. However, rather than challenge her, one of the booth personnel ran over and gave her a copy of the new release. This got her out of the way.

Later in the day, I tried the same technique on another booth and found that it worked quite well. I think it works best when women use it against men.

The most serious weakness of the technique is that you can't use it on two booths anywhere near each other.

Finally, if you have anything to trade for goods, you can probably find the opportunity to do so. Groups of firm representatives get together for parties in which they trade software. You can get into these without much trouble if you have a friend in the booth. You can trade T-shirts for \$600 packages without guilt. Parties of homosexual or minority programmers take place at most major shows. These are excellent targets. You can also go booth-to-booth trading, though this is a bad idea until the last few hours of a multi-day show.

Big companies are just as generous as small ones. Many firms will want feedback from you; send some if you can. At the same time, job turnover in press/industry relations is so quick that the person to whom you promised a copy of your review might be gone by the next show anyway.

## MOVING?

Let us know several weeks in advance. For some reason the post office doesn't forward magazines so you might miss an issue if you don't let us know about your new address. Also, to make sure it's actually you changing your address and not some mischief maker, we ask that you include your address label with any correspondence. If you can't find that information, then use an official address change card from the post office. Please don't leave address changes on our answering machine or through email without label info.



# nymex voice mail

Following is a list of telephone exchanges, the type of service they can, the call code for the switch, the location of the switch, and the local telephone number for NYNEX voice mail. Customers can subscribe to this service and retrieve their messages or leave messages for other people by calling this number. This service allows you to leave a message for someone without ringing their phone. Messages that don't have this service are not recorded. No credit lines there are a couple of days in this list, but we advised that certain people should have them to get it.

## Manhasset (912)

206 414 NYNEX1600 N. 1624 St.	527-8072
207 414 NYNEX1602 N. 1624 St.	528-1202
210 414 NYNEX1700 N. 1724 St.	582-2122
211 414 NYNEX1701 N. 1724 St.	583-0282
212 414 NYNEX1702 N. 1724 St.	583-0283
213 414 NYNEX1703 N. 1724 St.	583-0284
214 414 NYNEX1704 N. 1724 St.	583-0285
215 414 NYNEX1705 N. 1724 St.	583-0286
216 414 NYNEX1706 N. 1724 St.	583-0287
217 414 NYNEX1707 N. 1724 St.	583-0288
218 414 NYNEX1708 N. 1724 St.	583-0289
219 414 NYNEX1709 N. 1724 St.	583-0290
220 414 NYNEX1710 N. 1724 St.	583-0291
221 414 NYNEX1711 N. 1724 St.	583-0292
222 414 NYNEX1712 N. 1724 St.	583-0293
223 414 NYNEX1713 N. 1724 St.	583-0294
224 414 NYNEX1714 N. 1724 St.	583-0295
225 414 NYNEX1715 N. 1724 St.	583-0296
226 414 NYNEX1716 N. 1724 St.	583-0297
227 414 NYNEX1717 N. 1724 St.	583-0298
228 414 NYNEX1718 N. 1724 St.	583-0299
229 414 NYNEX1719 N. 1724 St.	583-0300
230 414 NYNEX1720 N. 1724 St.	583-0301
231 414 NYNEX1721 N. 1724 St.	583-0302
232 414 NYNEX1722 N. 1724 St.	583-0303
233 414 NYNEX1723 N. 1724 St.	583-0304
234 414 NYNEX1724 N. 1724 St.	583-0305
235 414 NYNEX1725 N. 1724 St.	583-0306
236 414 NYNEX1726 N. 1724 St.	583-0307
237 414 NYNEX1727 N. 1724 St.	583-0308
238 414 NYNEX1728 N. 1724 St.	583-0309
239 414 NYNEX1729 N. 1724 St.	583-0310
240 414 NYNEX1730 N. 1724 St.	583-0311
241 414 NYNEX1731 N. 1724 St.	583-0312
242 414 NYNEX1732 N. 1724 St.	583-0313
243 414 NYNEX1733 N. 1724 St.	583-0314
244 414 NYNEX1734 N. 1724 St.	583-0315
245 414 NYNEX1735 N. 1724 St.	583-0316
246 414 NYNEX1736 N. 1724 St.	583-0317
247 414 NYNEX1737 N. 1724 St.	583-0318
248 414 NYNEX1738 N. 1724 St.	583-0319
249 414 NYNEX1739 N. 1724 St.	583-0320
250 414 NYNEX1740 N. 1724 St.	583-0321
251 414 NYNEX1741 N. 1724 St.	583-0322
252 414 NYNEX1742 N. 1724 St.	583-0323
253 414 NYNEX1743 N. 1724 St.	583-0324
254 414 NYNEX1744 N. 1724 St.	583-0325
255 414 NYNEX1745 N. 1724 St.	583-0326
256 414 NYNEX1746 N. 1724 St.	583-0327
257 414 NYNEX1747 N. 1724 St.	583-0328
258 414 NYNEX1748 N. 1724 St.	583-0329
259 414 NYNEX1749 N. 1724 St.	583-0330
260 414 NYNEX1750 N. 1724 St.	583-0331
261 414 NYNEX1751 N. 1724 St.	583-0332
262 414 NYNEX1752 N. 1724 St.	583-0333
263 414 NYNEX1753 N. 1724 St.	583-0334
264 414 NYNEX1754 N. 1724 St.	583-0335
265 414 NYNEX1755 N. 1724 St.	583-0336
266 414 NYNEX1756 N. 1724 St.	583-0337
267 414 NYNEX1757 N. 1724 St.	583-0338
268 414 NYNEX1758 N. 1724 St.	583-0339
269 414 NYNEX1759 N. 1724 St.	583-0340
270 414 NYNEX1760 N. 1724 St.	583-0341
271 414 NYNEX1761 N. 1724 St.	583-0342
272 414 NYNEX1762 N. 1724 St.	583-0343
273 414 NYNEX1763 N. 1724 St.	583-0344
274 414 NYNEX1764 N. 1724 St.	583-0345
275 414 NYNEX1765 N. 1724 St.	583-0346
276 414 NYNEX1766 N. 1724 St.	583-0347
277 414 NYNEX1767 N. 1724 St.	583-0348
278 414 NYNEX1768 N. 1724 St.	583-0349
279 414 NYNEX1769 N. 1724 St.	583-0350
280 414 NYNEX1770 N. 1724 St.	583-0351
281 414 NYNEX1771 N. 1724 St.	583-0352
282 414 NYNEX1772 N. 1724 St.	583-0353
283 414 NYNEX1773 N. 1724 St.	583-0354
284 414 NYNEX1774 N. 1724 St.	583-0355
285 414 NYNEX1775 N. 1724 St.	583-0356
286 414 NYNEX1776 N. 1724 St.	583-0357
287 414 NYNEX1777 N. 1724 St.	583-0358
288 414 NYNEX1778 N. 1724 St.	583-0359
289 414 NYNEX1779 N. 1724 St.	583-0360
290 414 NYNEX1780 N. 1724 St.	583-0361
291 414 NYNEX1781 N. 1724 St.	583-0362
292 414 NYNEX1782 N. 1724 St.	583-0363
293 414 NYNEX1783 N. 1724 St.	583-0364
294 414 NYNEX1784 N. 1724 St.	583-0365
295 414 NYNEX1785 N. 1724 St.	583-0366
296 414 NYNEX1786 N. 1724 St.	583-0367
297 414 NYNEX1787 N. 1724 St.	583-0368
298 414 NYNEX1788 N. 1724 St.	583-0369
299 414 NYNEX1789 N. 1724 St.	583-0370
300 414 NYNEX1790 N. 1724 St.	583-0371
301 414 NYNEX1791 N. 1724 St.	583-0372
302 414 NYNEX1792 N. 1724 St.	583-0373
303 414 NYNEX1793 N. 1724 St.	583-0374
304 414 NYNEX1794 N. 1724 St.	583-0375
305 414 NYNEX1795 N. 1724 St.	583-0376
306 414 NYNEX1796 N. 1724 St.	583-0377
307 414 NYNEX1797 N. 1724 St.	583-0378
308 414 NYNEX1798 N. 1724 St.	583-0379
309 414 NYNEX1799 N. 1724 St.	583-0380
310 414 NYNEX1800 N. 1824 St.	583-0381
311 414 NYNEX1801 N. 1824 St.	583-0382
312 414 NYNEX1802 N. 1824 St.	583-0383
313 414 NYNEX1803 N. 1824 St.	583-0384
314 414 NYNEX1804 N. 1824 St.	583-0385
315 414 NYNEX1805 N. 1824 St.	583-0386
316 414 NYNEX1806 N. 1824 St.	583-0387
317 414 NYNEX1807 N. 1824 St.	583-0388
318 414 NYNEX1808 N. 1824 St.	583-0389
319 414 NYNEX1809 N. 1824 St.	583-0390
320 414 NYNEX1810 N. 1824 St.	583-0391
321 414 NYNEX1811 N. 1824 St.	583-0392
322 414 NYNEX1812 N. 1824 St.	583-0393
323 414 NYNEX1813 N. 1824 St.	583-0394
324 414 NYNEX1814 N. 1824 St.	583-0395
325 414 NYNEX1815 N. 1824 St.	583-0396
326 414 NYNEX1816 N. 1824 St.	583-0397
327 414 NYNEX1817 N. 1824 St.	583-0398
328 414 NYNEX1818 N. 1824 St.	583-0399
329 414 NYNEX1819 N. 1824 St.	583-0400
330 414 NYNEX1820 N. 1824 St.	583-0401
331 414 NYNEX1821 N. 1824 St.	583-0402
332 414 NYNEX1822 N. 1824 St.	583-0403
333 414 NYNEX1823 N. 1824 St.	583-0404
334 414 NYNEX1824 N. 1824 St.	583-0405
335 414 NYNEX1825 N. 1824 St.	583-0406
336 414 NYNEX1826 N. 1824 St.	583-0407
337 414 NYNEX1827 N. 1824 St.	583-0408
338 414 NYNEX1828 N. 1824 St.	583-0409
339 414 NYNEX1829 N. 1824 St.	583-0410
340 414 NYNEX1830 N. 1824 St.	583-0411
341 414 NYNEX1831 N. 1824 St.	583-0412
342 414 NYNEX1832 N. 1824 St.	583-0413
343 414 NYNEX1833 N. 1824 St.	583-0414
344 414 NYNEX1834 N. 1824 St.	583-0415
345 414 NYNEX1835 N. 1824 St.	583-0416
346 414 NYNEX1836 N. 1824 St.	583-0417
347 414 NYNEX1837 N. 1824 St.	583-0418
348 414 NYNEX1838 N. 1824 St.	583-0419
349 414 NYNEX1839 N. 1824 St.	583-0420
350 414 NYNEX1840 N. 1824 St.	583-0421
351 414 NYNEX1841 N. 1824 St.	583-0422
352 414 NYNEX1842 N. 1824 St.	583-0423
353 414 NYNEX1843 N. 1824 St.	583-0424
354 414 NYNEX1844 N. 1824 St.	583-0425
355 414 NYNEX1845 N. 1824 St.	583-0426
356 414 NYNEX1846 N. 1824 St.	583-0427
357 414 NYNEX1847 N. 1824 St.	583-0428
358 414 NYNEX1848 N. 1824 St.	583-0429
359 414 NYNEX1849 N. 1824 St.	583-0430
360 414 NYNEX1850 N. 1824 St.	583-0431
361 414 NYNEX1851 N. 1824 St.	583-0432
362 414 NYNEX1852 N. 1824 St.	583-0433
363 414 NYNEX1853 N. 1824 St.	583-0434
364 414 NYNEX1854 N. 1824 St.	583-0435
365 414 NYNEX1855 N. 1824 St.	583-0436
366 414 NYNEX1856 N. 1824 St.	583-0437
367 414 NYNEX1857 N. 1824 St.	583-0438
368 414 NYNEX1858 N. 1824 St.	583-0439
369 414 NYNEX1859 N. 1824 St.	583-0440
370 414 NYNEX1860 N. 1824 St.	583-0441
371 414 NYNEX1861 N. 1824 St.	583-0442
372 414 NYNEX1862 N. 1824 St.	583-0443
373 414 NYNEX1863 N. 1824 St.	583-0444
374 414 NYNEX1864 N. 1824 St.	583-0445
375 414 NYNEX1865 N. 1824 St.	583-0446
376 414 NYNEX1866 N. 1824 St.	583-0447
377 414 NYNEX1867 N. 1824 St.	583-0448
378 414 NYNEX1868 N. 1824 St.	583-0449
379 414 NYNEX1869 N. 1824 St.	583-0450
380 414 NYNEX1870 N. 1824 St.	583-0451
381 414 NYNEX1871 N. 1824 St.	583-0452
382 414 NYNEX1872 N. 1824 St.	583-0453
383 414 NYNEX1873 N. 1824 St.	583-0454
384 414 NYNEX1874 N. 1824 St.	583-0455
385 414 NYNEX1875 N. 1824 St.	583-0456
386 414 NYNEX1876 N. 1824 St.	583-0457
387 414 NYNEX1877 N. 1824 St.	583-0458
388 414 NYNEX1878 N. 1824 St.	583-0459
389 414 NYNEX1879 N. 1824 St.	583-0460
390 414 NYNEX1880 N. 1824 St.	583-0461
391 414 NYNEX1881 N. 1824 St.	583-0462
392 414 NYNEX1882 N. 1824 St.	583-0463
393 414 NYNEX1883 N. 1824 St.	583-0464
394 414 NYNEX1884 N. 1824 St.	583-0465
395 414 NYNEX1885 N. 1824 St.	583-0466
396 414 NYNEX1886 N. 1824 St.	583-0467
397 414 NYNEX1887 N. 1824 St.	583-0468
398 414 NYNEX1888 N. 1824 St.	583-0469
399 414 NYNEX1889 N. 1824 St.	583-0470
400 414 NYNEX1890 N. 1824 St.	583-0471
401 414 NYNEX1891 N. 1824 St.	583-0472
402 414 NYNEX1892 N. 1824 St.	583-0473
403 414 NYNEX1893 N. 1824 St.	583-0474
404 414 NYNEX1894 N. 1824 St.	583-0475
405 414 NYNEX1895 N. 1824 St.	583-0476
406 414 NYNEX1896 N. 1824 St.	583-0477
407 414 NYNEX1897 N. 1824 St.	583-0478
408 414 NYNEX1898 N. 1824 St.	583-0479
409 414 NYNEX1899 N. 1824 St.	583-0480
410 414 NYNEX1900 N. 1924 St.	583-0481
411 414 NYNEX1901 N. 1924 St.	583-0482
412 414 NYNEX1902 N. 1924 St.	583-0483
413 414 NYNEX1903 N. 1924 St.	583-0484
414 414 NYNEX1904 N. 1924 St.	583-0485
415 414 NYNEX1905 N. 1924 St.	583-0486
416 414 NYNEX1906 N. 1924 St.	583-0487
417 414 NYNEX1907 N. 1924 St.	583-0488
418 414 NYNEX1908 N. 1924 St.	583-0489
419 414 NYNEX1909 N. 1924 St.	583-0490
420 414 NYNEX1910 N. 1924 St.	583-0491
421 414 NYNEX1911 N. 1924 St.	583-0492
422 414 NYNEX1912 N. 1924 St.	583-0493
423 414 NYNEX1913 N. 1924 St.	583-0494
424 414 NYNEX1914 N. 1924 St.	583-0495
425 414 NYNEX1915 N. 1924 St.	583-0496
426 414 NYNEX1916 N. 1924 St.	583-0497
427 414 NYNEX1917 N. 1924 St.	583-0498
428 414 NYNEX1918 N. 1924 St.	583-0499
429 414 NYNEX1919 N. 1924 St.	583-0500
430 414 NYNEX1920 N. 1924 St.	583-0501
431 414 NYNEX1921 N. 1924 St.	583-0502
432 414 NYNEX1922 N. 1924 St.	583-0503
433 414 NYNEX1923 N. 1924 St.	583-0504
434 414 NYNEX1924 N. 1924 St.	583-0505
435 414 NYNEX1925 N. 1924 St.	583-0506
436 414 NYNEX1926 N. 1924 St.	583-0507
437 414 NYNEX1927 N. 1924 St.	583-0508
438 414 NYNEX1928 N. 1924 St.	583-0509
439 414 NYNEX1929 N. 1924 St.	583-0510
440 414 NYNEX1930 N. 1924 St.	583-0511
441 414 NYNEX1931 N. 1924 St.	583-0512
442 414 NYNEX1932 N. 1924 St.	583-0513
443 414 NYNEX1933 N. 1924 St.	583-0514
444 414 NYNEX1934 N. 1924 St.	583-0515
445 414 NYNEX1935 N. 1924 St.	583-0516
446 414 NYNEX1936 N. 1924 St.	583-0517
447 414 NYNEX1937 N. 1924 St.	583-0518
448 414 NYNEX1938 N. 1924 St.	583-0519
449 414 NYNEX1939 N. 1924 St.	583-0520
450 414 NYNEX1940 N. 1924 St.	583-0521
451 414 NYNEX1941 N. 1924 St.	583-0522
452 414 NYNEX1942 N. 1924 St.	583-0523
453 414 NYNEX1943 N. 1924 St.	583-0524
454 414 NYNEX1944 N. 1924 St.	583-0525
455 414 NYNEX1945 N. 1924 St.	583-0526
456 414 NYNEX1946 N. 1924 St.	583-0527
457 414 NYNEX1947 N. 1924 St.	583-0528
458 414 NYNEX1948 N. 1924 St.	583-0529
459 414 NYNEX1949 N. 1924 St.	583-0530
460 414 NYNEX1950 N. 1924 St.	583-0531
461 414 NYNEX1951 N. 1924 St.	583-0532
462 414 NYNEX1952 N. 1924 St.	583-0533
463 414 NYNEX1953 N. 1924 St.	583-0534
464 414 NYNEX1954 N. 1924 St.	583-0535
465 414 NYNEX1955 N. 1924 St.	583-0536
466 414 NYNEX1956 N. 1924 St.	583-0537
467 414 NYNEX1957 N. 1924 St.	583-0538
468 414 NYNEX1958 N. 1924 St.	583-0539
469 414 NYNEX1959 N. 1924 St.	583-0540
470 414 NYNEX1960 N. 1924 St.	583-0541
471 414 NYNEX1961 N. 1924 St.	583-0542
472 414 NYNEX1962 N. 1924 St.	583-0543
473 414 NYNEX1963 N. 1924 St.	583-0544
474 414 NYNEX1964 N. 1924 St.	583-0545
475 414 NYNEX1965 N. 1924 St.	583-0546
476 414 NYNEX1966 N. 1924 St.	583-0547



411	REC'D	RECORDING	135th Ave.	542-2385
412	REC'D	RECORDING	135th Ave.	542-2385
413	REC'D	RECORDING	135th Ave.	542-2385
414	REC'D	RECORDING	135th Ave.	542-2385
415	REC'D	RECORDING	135th Ave.	542-2385
416	REC'D	RECORDING	135th Ave.	542-2385
417	REC'D	RECORDING	135th Ave.	542-2385
418	REC'D	RECORDING	135th Ave.	542-2385
419	REC'D	RECORDING	135th Ave.	542-2385
420	REC'D	RECORDING	135th Ave.	542-2385
421	REC'D	RECORDING	135th Ave.	542-2385
422	REC'D	RECORDING	135th Ave.	542-2385
423	REC'D	RECORDING	135th Ave.	542-2385
424	REC'D	RECORDING	135th Ave.	542-2385
425	REC'D	RECORDING	135th Ave.	542-2385
426	REC'D	RECORDING	135th Ave.	542-2385
427	REC'D	RECORDING	135th Ave.	542-2385
428	REC'D	RECORDING	135th Ave.	542-2385
429	REC'D	RECORDING	135th Ave.	542-2385
430	REC'D	RECORDING	135th Ave.	542-2385
431	REC'D	RECORDING	135th Ave.	542-2385
432	REC'D	RECORDING	135th Ave.	542-2385
433	REC'D	RECORDING	135th Ave.	542-2385
434	REC'D	RECORDING	135th Ave.	542-2385
435	REC'D	RECORDING	135th Ave.	542-2385
436	REC'D	RECORDING	135th Ave.	542-2385
437	REC'D	RECORDING	135th Ave.	542-2385
438	REC'D	RECORDING	135th Ave.	542-2385
439	REC'D	RECORDING	135th Ave.	542-2385
440	REC'D	RECORDING	135th Ave.	542-2385
441	REC'D	RECORDING	135th Ave.	542-2385
442	REC'D	RECORDING	135th Ave.	542-2385
443	REC'D	RECORDING	135th Ave.	542-2385
444	REC'D	RECORDING	135th Ave.	542-2385
445	REC'D	RECORDING	135th Ave.	542-2385
446	REC'D	RECORDING	135th Ave.	542-2385
447	REC'D	RECORDING	135th Ave.	542-2385
448	REC'D	RECORDING	135th Ave.	542-2385
449	REC'D	RECORDING	135th Ave.	542-2385
450	REC'D	RECORDING	135th Ave.	542-2385
451	REC'D	RECORDING	135th Ave.	542-2385
452	REC'D	RECORDING	135th Ave.	542-2385
453	REC'D	RECORDING	135th Ave.	542-2385
454	REC'D	RECORDING	135th Ave.	542-2385
455	REC'D	RECORDING	135th Ave.	542-2385
456	REC'D	RECORDING	135th Ave.	542-2385
457	REC'D	RECORDING	135th Ave.	542-2385
458	REC'D	RECORDING	135th Ave.	542-2385
459	REC'D	RECORDING	135th Ave.	542-2385
460	REC'D	RECORDING	135th Ave.	542-2385
461	REC'D	RECORDING	135th Ave.	542-2385
462	REC'D	RECORDING	135th Ave.	542-2385
463	REC'D	RECORDING	135th Ave.	542-2385
464	REC'D	RECORDING	135th Ave.	542-2385
465	REC'D	RECORDING	135th Ave.	542-2385
466	REC'D	RECORDING	135th Ave.	542-2385
467	REC'D	RECORDING	135th Ave.	542-2385
468	REC'D	RECORDING	135th Ave.	542-2385
469	REC'D	RECORDING	135th Ave.	542-2385
470	REC'D	RECORDING	135th Ave.	542-2385
471	REC'D	RECORDING	135th Ave.	542-2385
472	REC'D	RECORDING	135th Ave.	542-2385
473	REC'D	RECORDING	135th Ave.	542-2385
474	REC'D	RECORDING	135th Ave.	542-2385
475	REC'D	RECORDING	135th Ave.	542-2385
476	REC'D	RECORDING	135th Ave.	542-2385
477	REC'D	RECORDING	135th Ave.	542-2385
478	REC'D	RECORDING	135th Ave.	542-2385
479	REC'D	RECORDING	135th Ave.	542-2385
480	REC'D	RECORDING	135th Ave.	542-2385
481	REC'D	RECORDING	135th Ave.	542-2385
482	REC'D	RECORDING	135th Ave.	542-2385
483	REC'D	RECORDING	135th Ave.	542-2385
484	REC'D	RECORDING	135th Ave.	542-2385
485	REC'D	RECORDING	135th Ave.	542-2385
486	REC'D	RECORDING	135th Ave.	542-2385
487	REC'D	RECORDING	135th Ave.	542-2385
488	REC'D	RECORDING	135th Ave.	542-2385
489	REC'D	RECORDING	135th Ave.	542-2385
490	REC'D	RECORDING	135th Ave.	542-2385
491	REC'D	RECORDING	135th Ave.	542-2385
492	REC'D	RECORDING	135th Ave.	542-2385
493	REC'D	RECORDING	135th Ave.	542-2385
494	REC'D	RECORDING	135th Ave.	542-2385
495	REC'D	RECORDING	135th Ave.	542-2385
496	REC'D	RECORDING	135th Ave.	542-2385
497	REC'D	RECORDING	135th Ave.	542-2385
498	REC'D	RECORDING	135th Ave.	542-2385
499	REC'D	RECORDING	135th Ave.	542-2385
500	REC'D	RECORDING	135th Ave.	542-2385

260 Internet meeting!  
 January 26, 1994  
 beginning 12 noon (EST)  
 on irc channel #2600

# ANNOUNCING

the first  
 2600 Internet meeting!  
 January 26, 1994  
 beginning 12 noon (EST)  
 on irc channel #2600

*(If you don't understand any of this, don't worry. We'll explain it in a future issue.)*



# The Magical Tone Box

by Fiberlyte

## Intro

The tone box is my latest mad invention. This device will satisfy your thinking needs well into the future. There is a new technology out called DAST: Direct Analog Storage Technology. What this is is an EEPROM which writes analog data directly, without A/D or D/A, on a single chip. What this means for you is, any tone related box you need is yours with this simple and very compact project. The cutoff for the high frequency output is at 2700 Hz, so red box tones and blue box tones will fit in, so there shouldn't be any problem. Besides, phones cut off at around 3000 to 3500.

## Advantages

1. Compact package and low voltage.
2. Better than a microcassette recorder, because when their batteries go down, the amplitude as well as the frequency decreases, resulting in unworthy tones and pissy operators. When the batteries go down on this (from 5 down to 3.5v) it gets stuck in play mode, so it has its own 10-batt alarm. Thus, no loss of quality.
3. Record any tones. One day you can have a red box, the next a blue box. Any tone can be yours.

## Purchasing

Radio Shack is where you can (never) find this ISD1000A. That was my problem - none of the local ones had it. I should take this opportunity to bitch about Radio Shack and their incompetence, but you all would rather get on with the box. The part number is ISD1000A and is made by Archer

and the chip will run you exactly \$18.80 including tax. The total cost will be around the price of a Radio Shack 33 memory red box conversion, but probably a bit more.

## Pre-Construction

You will want to check inside your computer for a Soundblaster, as this is needed to create tones, or if you don't have one, you could record red box tones from a Radio Shack conversion. What I am saying is, you need something that generates tones that you will want to record.

The following is what I used, not including the electronic components.

## Parts List

- ISD1000A (the chip)
- Small 6VDC battery (an Energizer AA4 will be perfect)
- Case (I use a film case, you know those little black and gray canisters)
- 16 Ohm speaker (go to a dollar store and buy some cheap Walkman headphones)
- 28 pin socket (do not buy the Radio Shack ones if you can help it, find one with an open design, instead of Radio Shack's weird design)
- Soldering iron, of course

## Microphone

The breadboard is important. What you will be doing is building the record circuit on the breadboard, and then the play circuit right on a 28 pin socket. You can pop the chip into the breadboard when you need to record and then pop it back into the play circuit when you are ready to play. This will prevent any etching and will keep the play circuit small.

As soon as you buy the chip, open the package. Inside there will be a

manual. Turn to page 6 and buy all those components and some solid wire. Skip S4 and R7-R14 since we will start recording at the beginning address, and also skip the 8 ohm speaker and the electric microphone, since you will be using a normal, higher quality microphone and a 16 ohm headphone speaker.

## Building

When you get home, unpack everything. Breadboard the circuit on page 6, noting that you will choose the simpler construction (bottom right corner). Then solder the play circuit that is on page 7 onto the 28 pin socket. Remember that you will try the chip if you solder directly onto it, so use the socket! If you must use the Radio Shack socket, try to make sure no rosin or solder splatters down the pins into the dips. I had this problem on two sockets which wouldn't allow me to play. Pop the chip into the recording circuit, load up QUARTER VOC or use the Radio Shack dialer or whatever else and record. Recording instructions are found on page 7. Then pop the chip into the play circuit. If it works then you now have a red box. Remember, as long as you have the tones, you can record them.

## How to Build the Film Case

### Container

Take the top off of the case and your headphone speaker should fit perfectly in the gray cap. Cut a hole in the top and glue the speaker into the

cap. You might want to use a speaker grille. Next, cut a hole in the bottom of the back cylinder big enough for your pushbutton switch. You should know how to wire up a switch. The chip, battery, socket, switch, and speaker all fit in perfectly. Everything fits in mine, but you might need to cut off the bottom part of the speaker, the unnecessary plastic part.

### Use

If you can find BlueBEEP, versions 004 and above, you can use the red box tones included. The QUARTER VOC that I use has worked successfully on all phones to a live AT&T operator. In places where the Radio Shack didn't work, the VOC did. As a red box the simple play circuit is fine because all you have to do is hold down the switch. Even though blue boxing is not possible for most people, the tone box can be used as a blue box. For a blue box, you need to do some addressing, which is explained in the manual. Depending on which pin (pins 1-10 only) you connect to ground you can address that corresponding address in memory. So, for a blue box you would set for address 1 the 2600 blasi, address 2 the KP1, and address 3 the ST. So, to seize, hit 1, 2, dial on the phone's keypad (or your own dialer), then 3.

## WRITE FOR 2600!

SEND YOUR ARTICLES TO:  
2600 ARTICLE SUBMISSIONS  
PO BOX 99  
MIDDLE ISLAND, NY 11953  
INTERNET: 2600@well.sf.ca.us  
FAX: (516) 751-2608



# LETTERS TO REMEMBER

## Fun Telco Numbers

**Dear 2600:**  
I am writing in regards to Mousse Kalif' request for the ANAC for 310818. Well, there are two that I've found - on Pacific Bell phones you use 311-2345 and the 114 that you published works only on QTE phones. I also found that on QTE payphones, oftentimes pressing 111 will get you a complete test for payphones. It is "meta-driven" and is surprising "user friendly". I have used these three numbers in 838 and parts of 113 with 100 percent success on 211-2345 and 114 but only about 50 percent success with 111.

Beetle Bailey  
Arcadia, CA

**Dear 2600:**

I remember reading somewhere in your magazine that you published a list of local unnumbered services. Could you tell me the most recent issue that would have those for my area (813, Clearwater, FL)?

Here are a few of the ones I can remember, and I know they work in my and the surrounding calling areas:

311 and 711 identify your phone number. 117 occasionally leaves you with an open line. 112 is the Provider Test Set which has the following items: 2 - line test, 3 - coin collect test, 4 - coin refund test, 5 - coin relay testing, 6 - coin test, 7 - party ground test, 8 - ringer test, 9 - party 2 ringer test, 0 - full test, 10 - express telephone test, 12 - reverse line, 13 - line open, 14 - complete data mode, 15 - express test 1, 15 - express test 2, 17 1A coin relay test.

Macgyver, Interred  
Clearwater, FL

The exact same thing happens in area code 210 and 211 when dialing 111. Additional tests are: 18 - 5.02 - ATDS, 19 - Access to other tests, 2 - Midway test, 3 - Zero tone test, 5 - three tone test, 6 - two tone test, 7 - two tone exposure test, 8 - to access SLIC bypass circuit, 9 - to test regular SLIC circuit.

**Dear 2600:**

Hello again, here's a number your readers might like. It is an 800 number for AT&T information. But here's the catch: It's a TDD line so not only can you call for free but you can use your terminal too. All you have to remember is to type "GA" whenever you're done talking. It means go ahead and when you're totally done type "SK" to stop keying. You get the point. The number is 800-855-1155. I've found that the TDD operators are a bit nicer than talking to voice operators.

It's not much but I've been reading the mag for a while so I had to send something in even if it's possibly into the bin.

Uncle Waldo

## Hacking Traffic Lights

**Dear 2600:**

In the process of gearing up for the 1996 Olympics, Atlanta city officials announced several months ago that they were going to begin to upgrade the city's traffic lights. By far the majority of the traffic lights here are "amber" lights, with an pressure plate or flow sensitivity at all.

This announcement got me thinking: Anyone can create any experiment in a hacker's traffic light controllers? I find myself curiously curious about how these demand things work. Especially the "white/green" ones.

Lane Wolf  
Atlanta

Traffic lights can be a lot of fun to play with. Many people aren't aware of how the sensors work or even where they're located. More recently we've heard of traffic lights that can instantly turn green when exposed to a strobe light. This is apparently to allow ambulances to get through intersections more easily. We've heard rumors of rapidly flashing headlights turning the some effect which could definitely lead to some interesting traffic situations. It goes without saying that if you're going to hack traffic lights, you should be very careful not to put anyone's life in danger. So we won't furnish our readers' intelligence by saying it.

## Past Hacker Prime?

**Dear 2600:**

Ever since I've had a consistent knowledge of computers, I've wanted to hack. I haven't always known it was called hacking, but I've just had the mental itching skin to hacking. The problem is, basically, I neither have the equipment nor the know-how needed. Right now I'm 15 years old and about to start my junior year of high school and I feel that I'm almost just my prime for hacking (this may just be a popular misconception). But, regardless of my age or academic standing, I feel I should start now. So I was wondering if you could assist me in the right direction in terms of literature and an affordable, but good, system.

Darkhold Page  
Pittsburgh

We don't really recommend one system over another because everybody's needs and tastes are different. What you need to do is play around on as many different systems as you can in order to find out what you're comfortable with. We advise using "freedom" systems or those in school or computer stores. Otherwise you run the risk of getting something you don't want or can't use. Read some of the literature featured in 2600 in order to become more familiar

with the culture. Any good bookstore or library should provide you with much material. With regards to age, you are hardly your own prime. Most hackers are young because young people tend to be adaptable. As long as you remain adaptable, you can always be a good hacker.

## Info and Questions

**Dear 2600:**

This is the best ISP magazine I've found - keep up the good work. I'm pretty new to hacking, but there are a few questions I would like to ask.

What is the ANAC for area code 201? What are the issues for certain information about voice mail, COCCOT, radio payphones, and ISP boxes (red, blue, green)? What is a silver box? Would it be possible to form some sort of phreak and hacker directory?

I have noticed that some COCCOTs in New York, after you get the unrestricted dialtone, have a long distance block on the line, but I also noticed that they dial some sort of extender owned by the service provider to the COCCOT. There is something fellow readers might want to try: dial a number direct from a COCCOT and insert the correct coinage. Then if this particular COCCOT dials an extender number and it is audible, hook up a telephone pickup microphone (readily available from Radio Shack) to a DTMF decoder and then experiment from there. If the COCCOT does not use an extender, just hook it from there. If you are not sure, find out by listening carefully to the COCCOT dialing in the background and if it is using an extender then try clipping onto the line or any other way that will work. I hope this has helped some people in the HF community.

An interesting number is (206) 625-0830. It's some service called Free Phreak. Also, there was an interesting number in (201) 664-2300 but all of a sudden all the numbers in 644-23xx are continuously busy with no chance of getting through. The strange thing is that this is not a real busy signal - it's a fake. Now just in case you wanted to know what was so special about this time, it was some sort of test to speech converter that would transfer you to various extensions. There were some interesting extensions like trash tone shell, Bellcode directory, and others.

Whisper

The ANAC for at least part of New Jersey is now the same as New York, 528. In many digital switch boxes 511 also works. Silver boxes are making more than enough such good pads that can produce an error now of tones (A,B,C,D). Other than relay tests and digital testing applications, there don't seem to be many uses for these extra tones, at least not yet. The tones you're interested in are converted in some form to nearly all of our tones. One day soon we hope to have a comprehensive index. Reader directories have been tried before but they're usually filled with inaccuracies and taken at respect by few engineers.

**Dear 2600:**

This letter is concerning the article written about

the cable describable. Upon looking for a 75-100pf variable cap, I noticed that there was no one around that carried that size of a variable cap. After talking to some friends who are EE's (electrical engineers), they suggested using a smaller variable cap, and just have a fixed capacitor to that their needs would add up to be within the 75-100 range. Example: using three 22pf fixed caps, and one 4.34pf variable cap, and just tune the variable cap. This works since the total cap. is added up when they're placed in series. I have yet to go out and try this, but I am going to. I will write back with results.

Also, there are MCT phones around here that make out the mouthpiece. Even when you call up someone else it remains in again. I cannot use my "quarter" on it. I really hate the Fax Bell phones it does work on, but I was wondering if anyone knew of a method to get the MCT phone mouthpieces to unroute. Thanks.

Will Chung  
San Luis Obispo

**Dear 2600:**

A year in your Spring 1993 issue stood where you can purchase a phone that has A, B, C, and D keys. I work with a family operated business. We manufacture a DTMF encoder which goes into meters, photos, systems, and other applications. The encoders are sold separately. We carry all types of encoders, 12 key and 16 key (which has ABCD).

According to the response someone gave to the letter, it seems that someone at 2600 Magazine wants one of the keypads with the ABCD. If interested, can we swap a subscription for a keypad?

Eppo Communications  
P.O. Box 20228  
Palmdale, CA 91378  
(916) 644-5444

Send a keypad and we'll send you a subscription. How's that?

## Potential Discovery

**Dear 2600:**

After setting up my answering machine with the wrong number recording (to distract '69's after a song), I noticed that when a call was placed from a COCCOT, the message would be played and the COCCOT, recognizing the tones, would hang up and return the caller's money. Displaying the wrong number tones after a conversation gave the same response. Do you know if this is standard of all COCCOTs or just my area?

Maldoror  
Florida

If a gate kept that some cheaply made COCCOT simply listens for the interrupt tones and answers that there was no connection made if they appear. What a wonderful thing.

## Security Concerns

**Dear 2600:**

A friend of mine was recently contacting a 2600



subscription. "Of course," he said. "I'd probably put me right onto the Fed list."

This brought to mind a few interesting questions. What messages are taken to insure a subscriber's privacy? As the staff of 2600 has always taken an interest in the individual citizen's privacy, I have always assumed you don't sell subscribers' addresses to any kind of mailing lists. But what else is going on? Is there any possibility of outgoing 2600 mail being monitored by some form of Federal agency that you're aware of? If so, is there anything being done to prevent it?

**Radiation X**

**California**  
All we ever tell you is that we do everything possible to maintain our subscribers' privacy. We don't show our mailing list to anyone else. If I had to imagine Federal agents looking down the street and addresses on every piece of mail we send out we would not give a lot.

**Dear 2600:**

I have been considering subscribing to your zine, 2600, but I have second doubts. I am not wishing to subscribe because of the price, but I have heard a rumor that wheedle someone subscribes, they are put on a Fed list. I really don't want to have the Feds pointed on me if there is some hook around my area. If they really do get a list of subscribers, then the chance of that happening are greatly multiplied by what they usually would be. I'm sure.

Is this just a rumor that 2600 is run by/w/ith the Feds, and subscribers are put on a list, or someone is able to GET a list of subscribers fairly easy?

**Based The Freak**

As we said, we don't show the list to anybody. But really, if 2600 were run by Feds, do you think we'd tell you?

### Starting a Meeting

**Dear 2600:**

I picked up my last copy of 2600 this summer. I'm no hacker but I liked the idea of the "Quarter" and having had a college electronics education, proceeded to assemble it. I ran into timing and frequency problems but by attending the August Chicago meeting I was able to resolve my problems by working with some very helpful fellows. I would especially like to thank the "Proseur" for supplying the 6.50 stock as well as his expert technical advice. Seemed like a nice bunch and quite a milrow time was had by all. I thought World War III would break out from what I read in your magazine about previous meetings, but quite the opposite proved true! Let me know how I can start a meeting in my area if possible, as well as how I can further educate myself in this definitely sneaky hobby. Thanks much. (I can't make the next meeting as I got sent away to a rehab.)

Johnny "The Quarter" Burpo  
Rubber Room Keshinghouse  
Uplstate, NY

If you want to start a meeting in your area, just contact us with a place that you have in mind. It should be publicly accessible and fairly open. There is also some degree of responsibility which you must take in order to ensure that things go smoothly. The best way to start the process is to call us at (516) 751-2600 and leave a number where you can be reached.

### Questions

**Dear 2600:**

I'm new to phreaking. I was at a recent New York meeting and I want to learn more. I have a few questions:

- 1) Do you know still work? Is there any site we go to use them? If not, how can you explore the phone system's hidden numbers as you state could with a blue box?
- 2) What does an ESS or crossbar switch look like? Is it a hardware? Would it fit on a desk? Is it one switch per grade? More? Fewer?
- 3) Are 2600's phones tapped? Will mine be once I've called and faxed you?
- 4) I'm pleased to report that my Radio Shack experience was nothing like that of The Apple. If Esprit/Elie I just walked in, asked for 43-141, gave them fake info, paid, and walked out. Then again, I didn't buy a switch or any wire, so that may have been it. In any case, perhaps it's best to make separate tips.
- 5) What should I do to protect myself from searches and seizures at 2600 meetings? Why did people actually give me security contact information at the November meeting in Washington?

**M**

**Great Neck, NY**  
Give her more and do things so in certain places, a blue box would still work. Think the United States, it's pretty rare however. A crossbar switch or a huge non-wired network filled with cabling relays, racks, and wires. ESS switches are computers that take up much less room and hardly make any noise. It would be nice if we could answer #3. For more details on meeting strategy, we suggest reading the article on page 35.

**Dear 2600:**

The article by Borellig in the Spring issue mentions a cellular service manual marked through Motorola form #68-093-00660. I have tried to acquire this manual through my sources at Motorola Canada, and have been told first cut that it can't be had. Can 2600 or whoever give me a hand in its acquisition?

**DY**

**The word is out.**

**Dear 2600:**

In the USA (in Boston I think) there's an anti-car theft tracking device called "Injekt". Stolen cars transmit a signal to specially equipped police cars, so the police know the car you're driving is stolen, but you don't know that they know.  
The same system is being introduced in the UK

under a different name very soon and I was wondering about ways to get around it (generally for educational uses). This of course excludes finding the damn thing and ripping it out so the cops end up receiving a worse paper hit on a sheet count.  
Can you or any of your readers help?

### Why Hack Cable?

**Dear 2600:**

Your little magazine blew me away. I used to get the old 7AP back in the early eighties and I thought this sort of thing was dead. It's a good thing it isn't.  
Anyway, your cable TV describer is basically just a bandpass or band stop filter that might still use a kind of scrambling, where a "jamming" signal is mixed with the video and your box notices it out. But from the deserializer given, I wouldn't even try to build one - you could come up with any of several circuits. In the future, please give us a schematic; a picture is worth a thousand words.

The Graf and Shesst book on video scrambling is probably the most direct source. Your best library may well have it or can get it for you.

But a more relevant question might be: why hack the cable TV? If you just want to enjoy the trip, great, but the vast majority of the stuff on cable really sucks and you will spend way too much time watching this dogshit. I had free unlimited cable for five years and finally had to physically unplug the cable so as to "dry out".

I started to keep reading your expensive parent cage litter and I would really like to see more on UNIX. Especially more on how to get "real" UNIX on your PC so you can play with it and also on UNIX history and fundamentals.

Finally, for you crypto books: Are any of the old NSA cryptex machines (boxes with model numbers like KG- or KY- something) now in the public domain and out there with hackers or hamsters? I'm given to understand those things were just beautifully built, but then opens so see the ugly Pentax makes.

**A-String**

**Letcher, KS**

### How to Learn About Your CO

**Dear 2600:**

There is a very simple way to learn about your local phone company - go to the central office! Find out where the CO is in your area and head on down with some notebooks and other academic necessities. Tell whoever is working there you are doing a project (for school) on the phone company (it's your way through this explanation as necessary), and that you wanted to see just how things work. Act real innocent (and dress like) and the people there should give you a tour. In any town, I went for multiple tours, learning new things each time. You can see how a call is routed, and get a glimpse of the ESS computers. But

more importantly, you can get gear into off of papers on the walls and general baloney. You can get phone company internal numbers and other useful information. At our New England Telephone office, there were a few terminals with external AT&T desktop modems. So visit your local CO today!

### Observations

**Dear 2600:**

I just wanted to comment on a couple of things from your Autumn 1992 issue. First of all, from your "Shopper's Guide to COCOT's" article, I've found great use of the "combo box". By eliminating the pretty much worthless keypad circuit in it (which lets you know that a number has been successfully stored in memory), I was able to keep both crystals, as well as two memory switches to activate the crystals, internal (eliminating the keypad circuit for space). This way, when the dialer is right side up, I get the normal tones, and when I hold it upside down, I get the second crystal (the concept was mentioned in a letter "The Facts on ACTD" by Kirgion in the same issue, the extra space was needed so that I could use Radio Shack memory switches PN 275-000 because I was unable to find anything smaller).

I've found that here, the operators like to come on line and bother you for no apparent reason (I'd have to assume that it happens when I send the tones too quickly - one after another, so rather than storing five \*5's in the P1 location, it's best to store five \*5's and a pause. This way you can hit the P1 several times and not have the tones run on too quickly). Speaking of operators coming on line for no reason, I dialed a number on one phone, it asked for 55 cents, so I looked at three "quarters", after which I got a loud "beep" and an "Operator - please deposit 55 cents". I responded "I already dropped some money" in "not stating an amount" and without another word I was connected to the party I had dialed (which I ended up hanging up on figuring that the conversation would end up being mentioned anyway). How odd!

I still haven't found a way to place local calls using the red box here, and if anyone has information on how to do it, I'd appreciate it. And as far as I've been able to find, all the COCOT's I've run across here in California are never modded in the "dial the 800 number and let them hang up on you" trick doesn't work at all (the phone never beeps you even here the dial tone). I did find an odd one though where I dialed the 800 number, the phone clicked a couple of times and then gave me a dial tone which I was able to dial from using the COCOT keypad. It was apparently a fluke because I haven't been able to do it again on the same COCOT (or any other COCOT).

Finally, there was some guy who wrote in advertising his BBS (Tim Shock) claiming to offer free dial access to all 2600 readers. In this guy jacking or spoofing? I called the thing and he's got five lines

**Hook**

**Belmont, MA**



cell forwarded to a single line, real access only. BBS system (disguised to look like a multi-line system), which won't give you access until you've been "self-book verified". He even has a list upon login of the "most downloaded files", which all just happen to be hard-to-find files. But upon examination of his file base, the file names listed don't even exist! He even mentioned that he didn't want any "womanly" photos, or "pecks", but I can't think of anything a plebeian or hacker would want to do more than give some girly BBS his real name and home phone number. One, either a very paranoid system (in which case he shouldn't advertise his BBS in a hacker magazine to begin with), or something fishy is going on in Chicago Falls!

**The Lung**  
Suncoast Southern California

It is possible to activate the ACTS computer on local radio by coding in on a long distance number using a carrier access code. That's one way a real box would work on a local call. If that kind of dialing is allowed in your area. As for bulletin boards, all we can say is that we're not opposed with any except for our own voice BBS. Anything is possible out there.

### New Technology

Dear 2600:

Enclosed is a copy of an advertisement for Modem Maze I and Modem Maze II. Modem Maze I secures your modem by forcing the hacker. By attaching Modem Maze I to your existing modem, you make your computer system virtually undetectable. When a hacker attempts to call your modem, Modem Maze I intercepts the call by answering with a realistic sounding "hello". The hacker will simply hang up, not realizing that a computer system even exists on the other end. Only someone who knows the proper codes and procedures can gain access to the modem. Modem Maze II only allows pre-dialled calls using Caller ID.

**Julian**  
Cleveland

Would we love to hear that "realtime recording" holds?

### Modern Back Door

Dear 2600:

I do not know if this is the kind of stuff you are interested in but I have some interesting information on the Digiprem 9600 Serial modem and possibly any other Digiprem 9600 model.

I bought my modem for \$150, a good deal for a 9600 internal modem. Digiprem sells a 14.4 modem called the Scout Plus for around \$220. They will let you upgrade the Scout to the Scout Plus for \$30. The Scout Plus also includes a fax. Well, here is where the fun starts. There is an undocumented command for the modem. It is AT\*Z21A1T20. This command turns your 9600 Scout into a 14.4 Scout Plus. I'm not sure if AT\*Z1 actually makes the 9600 as fast, but the

modem connects with others at 14.4 and the CPS jumped from 1100 to 1500. That's one hell of an improvement for 2000\$.

### Foreign Pay Phone Flash

Dear 2600:

In the Autumn 1993 issue of 2600 you asked "Does Bahrain have payphones?"

Bahrain has no public payphone booth in the main plaza in downtown Doha. Bahrain's capital city. Unfortunately, I don't have enough time to search through various responses to find a picture for you.

I can tell you, however, that these public payphone booths are all attendant operated by private enterprises, and while they are metered payphones, they are not coin operated, one pays the attendant for the number of message units rung up on the phone.

Bahrain's telephone network is in its infancy stage and being installed primarily with the help of Japanese firms. It is an extremely modern, all-digital network using the latest satellite transmission technologies to bind the remote valleys together with the outside world. It explains the wireless communication system that is still used in parts of the country where the new aspect hasn't yet reached. There is no reason to think that coin operated phones won't be appearing on Bahrain's shores in the future, but as of November 1992, there were none.

**LN**  
APO AE

Your father is being proof that there's nothing 2600 readers can't find out.

### How to Really Abuse a Payphone

Dear 2600:

Just a while ago I picked up a copy of the Summer '93 issue and since then have read it from cover to cover many times. Reading the article about using the Modem Maze's emergency sound qualities to produce the required quarter tones. Unfortunately, the Modem Maze is too slow to produce the sounds up in speed. I do have a solution for all of the people who don't have the experience to build the Quarter described. It involves finding a payphone with no coin sensor (I got really, and with the wire going into the payphone exposed and in a pin or metal conduit. Use a knife and strip the wire going in to the phone without cutting it. Next get a set of head phones and cut the cable in half, stripping the wires on the plug end. Use alligator clips to attach the wires together and plug it into a tape recorder. Next record as you put a quarter into the phone, hang up, get your quarter back and rewind the tape. Now all you have to do is play the tape into the phone's microphone for a quarter. Make sure you put electrical tape on the the phone's wires so it doesn't

short out. I have tried this and it does work, but you must make sure that you have the alligator clips on the right wires on the phone cord. You might want to practice the part with the wire stripping at home to get it down. Other than that, have fun!

**Peter**

Manchester, TX

### Technology Moves Backwards

Dear 2600:

I am writing to you in your capacity as the great unknown of AT&T's fine network. When the Public Phone 2000's came out, they were the first visible sign of AT&T's desire about being the deliverer of the telecom revolution. Global information convergence, one I checked my e-mail from airports a few times, just for the novelty value. Not long after they appeared, just about all special functions (calendar, information services) were disabled on all phones, thus dumbing them down to no more than regular pay phones. No one seems to have commented on this setback. I can only imagine that sophisticated public throughout with services for anonymous login and subscription must have suddenly seemed like a risky proposition. Do you know if there were any specific incidents that called this to the telecommunications' attention? Was there any explanation provided?

**Martin**

That is the fear we've heard of a few it's certainly not the first time a good idea has been discontinued.

### Corrections

Dear 2600:

In your Spring '93 issue, there are two wrong numbers in your "Getting Your Fix" article. I have provided the correct numbers: Texas Union (311) 689-3888 and TRW (214) 390-9191.

**Jeff**

Brown you.

While checking around local files in the dip files on the Internet, I found some information on the digital counterpart to the red box: the green box, which will supposedly return someone's money once they've used a pay phone in cell phone. The rates are: 2600 Hz for 90 ms, 3000 Hz for 60 ms, 2600 Hz for 300 ms, and then (it is not specified) whether this should follow immediately or after a silence) 1100 Hz+1700 Hz (the duration of this tone is not specified either).

On my Amiga, I've managed to synthesize the right tones or a near thing to them. I haven't yet used them. The reason is that while I know the point of making and generating is for a beginner to figure things out on his own by trying them, I also know that one shouldn't go showing 2600 Hz tones into one's own phone without knowing exactly what one is doing. So I turn to you for advice. Is this safe? Are you going to get into the kind of trouble doing this that you

would blue boxing? It seems like a great alternative to building all my friends Radio Shack red boxes or copies of "The Quarter," but I don't want to screw around without knowing what I'm doing.

**King of Birds**  
Chapel Hill, NC

If you're asking whether engaging in phone fraud from your house is safe, our answer is definitely not. Don't there's nothing wrong with finding out whether or not a words or ideas can be our eyes.

### Red Box Concerns

Dear 2600:

Regarding "True Colors, Autumn 1993, Page 9" - in a quote from your section on red boxing, you said: "Use of the above parameters in a real red box is probably the safest method of phreaking, since it forces you to use a coin phone. Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe. Do not use!" How do you back up the claim that using a "real red box" is safer than using the 6.5536 modified phone dialer? They both accomplish the same task, that is simulating a quarter tone, however one just does it more precisely than the other. As long as your coin goes through on an entrance-free, automated system (e.g. AT&T Long Distance), what difference does it make? Does the extra precision of the "real red box" worsen your chances of being detected, and somehow immediately detected at the payment? I will answer to the fact that red boxing today is very unsafe, at best, but I do not see how using the "real red box" versus using the 6.5536 modified dialer, makes any difference. Please explain.

**Anonymous**

Dear 2600:

First off let me say I've been an avid reader the last couple of years (and missing an issue here and there prolonged me to become a subscriber). Your publication has brought me many happy hours. Keep up the excellent work!

What concerned me though, was Bill's article "True Colors" in your Autumn, '93 issue. He says, "Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe! Do not use!" There are some local kids here in the (905) area that insist to me that it's perfectly safe as long as you don't try using it with auto-penned online. When I held them above the article one of them told me he'd read it but that it was just unsafe in some places and the equipment here wasn't sensitive enough to detect the red box. Any more information on this?

**NEWS**

Dear 2600:

I just finished reading the Fall issue of 2600 and I read the article on various color boxes. In the sub-article about red-boxes, it mentioned that red boxing was very dangerous. What is this shift? Do you know something that I don't? A lot of red boxing goes on in 612 and I have never heard of anyone actually getting



charged with any crime for not leaving. Although the video has become more privy to red boating activities, nothing has come of it, so far.

**Concerned**  
As explained in a letter in our Winter 1993-94 issue, that particular workstation will always produce scores of 1111 0111 and 2200 1111, and the display will always be 54.62 ms on and off. The concern is that, apparently, it would not be difficult for those who have to be looked for by the phone company. We're aware of this ever actively happening.

## How Easy It Is

Dear 2600:

My school is running on an Ethernet, ICLAS system, (IBM Classroom Administration). It is a real easy network to hack, and the thing that happened a few weeks back that really showed me how loose the security was, was this: A hacker wanted to get in to the network as sysop with a valid password when, he said he had, the teacher was 10 feet behind him. With this ICLAS software when you login as sysop or supervisor, it makes this really loud annoying sound. I am really surprised that the teacher, who is also the computer coordinator for our school, did not notice. It just goes to show that even with a title like "Network Computer Coordinator" people can't do a simple job of watching if someone logs in as sysop right in front of your face!

**CopKiller**  
Berkeley, MD

Dear 2600:

I just read the review of NIPASS in the Autumn 1993 issue, and I must tell you that there is a much better and cheaper way to accomplish the same results or better. I have an NLM on my BBS (see Phreak #40) which will create a temporary SUPERVISOR equivalent account with a name that you specify.

The name of this wonderful NLM is TEMPLOR. And all you have to do is stick this preppy on a floppy and type LOAD A:TEMPLOR at the server. An account will be inserted into the system with SUPERVISOR privileges, which will allow you to create an account using SYSDON, among other things.

The advantages in this are obvious over NIPASS... no change to the SUPERVISOR password, doesn't generate a broadcast, and it doesn't cost you \$245. Plus, you don't have to call the company every time you want to use it.

This program is, of course, solely to demonstrate how insecure an unlocked NetWare 3.x file server is, and should never be used for any other purpose!

## Bypassing Restrictions

Dear 2600:

First off let me say that The Hacker Quarterly is one of the best publications I have read in a long time. It talks of all the things that Mr. Computer Science Prof should have told you but wouldn't, most likely

because it might endanger his/her control over students. However, I am sending this mail mainly because our two-Nazis systems (I don't really know if he is a Nazi, or just scared of free access to information) has so severely restricted our access to the Internet that most of the newsgroups are academic related or free-time conversation topics. Anything that might pertain to socially relevant behavior (including anything involving the government rephased, etc.) has been deleted. In fact this morning over 1000 newsgroups have been removed out from our system. Is there any way for a person to get around this restriction over net access for users or access Internet before the screening process goes into effect?

I have tried to get more info on Internet, but even anything more than a story-like explanation of the system is impossible around here. Shameful, doesn't even use his own computer science students.

Any help would be greatly appreciated.  
Lost and registered in  
NB, Canada

**Your story is not at all accurate, unfortunately. Question: people in charge feel the need to restrict or cut off access. Again from making sure we never have had people like that, the best thing we can do is look for ways around it. Since you already have access to the Internet, it shouldn't be too difficult to hook out to another user that isn't as restrictive. Perhaps you could create accounts with a student or another school or subscribe to a cheap public FIDO system. You'd be free over to his/her system, avoiding it possible.**

## A Way Around Caller ID?

Dear 2600:

I recently finished last issue's article on Caller ID. After reading this interesting piece, I came up with a thought for jamming CID.

1) Call xxx-xxxx and hang up immediately before you hear the ring. This will send a flag through to the called party, prompting their CID unit to answer, provided CID uses a normal modem hooking. It will attempt to connect, even though there is nothing to connect to.

2) Call xxx-xxxx immediately after you hang up. If you use an auto-dialer and time this right you should be able to get through with two or three seconds between the calls. The called party will receive the ring, but the CID unit will not have recovered in time to receive the signal from the relay. This would allow a quick and easy way around Caller ID, especially if 947 is not available. I would try this myself but Caller ID is not yet available in my area (i.e., New York Tel hasn't flipped the night switch yet.)

**Lenox**

Sorry, it doesn't work. The Caller ID box is a state of perpetual receiving; it doesn't have to make a connection. The data is sent between the first and second rings and the Caller ID box is designed for that one specific moment.

## School Phone System

Dear 2600:

My school's got an interesting phone system. Because all the numbers on campus start with the same two digits (2 and 5), every phone on campus is set so you only need to dial the last five digits to get where you need to go. For example, for dorm you dial 3-xxxx, and offices can be had by dialing 6-xxxx and 5-xxxx.

What's interesting is that this town also has other phone exchanges, such as 237 and 256. However, to dial these exchanges you need to hit "9" first, and then dial the full number. To dial cell free numbers, you hit "9" and then the full number. "9" also works for this.

I'm fairly sure the school has its own signaling system, but it doesn't quite make sense. I've tried to hit both "9" and "7" at public campus phones, with no luck whatsoever. It only works on phones in the dorms. Hitting either of those at public phones produces an alarm of alternating high and low pitched tones.

What hacking potential exists? Can you please explain how this works? It's fairly interesting, and I'm quite curious how the system differentiates between the phone in my room and the public speakerphone outside my building.

**News**

## Chiropract

There is plenty of hacking potential in any system like that and it involves dialing all sorts of other numbers. You have to keep looking until you find something that you differently. Your room phone has a different class of service as a public hall phone as the restriction level is not the same. No doubt there are other restrictions levels as well.

## 2600 Wins Over Class

Dear 2600:

I recently picked up my first copy of your magazine and couldn't put it down for days. It is the source for information I have been looking for that you can't find anywhere else. By showing how different systems can be manipulated, I have gained a much better understanding in their operation. One of my current classes is an operating systems class in which I am studying how a UNIX-like system works. By demonstrating a shell process that uses many of the features available in UNIX, your article gave me a much more tangible grasp of the system than my class ever could. Thanks for the enjoyment.

**MG**

Georgetown, TX

## The Honesty Test

Dear 2600:

I just finished perusing your Autumn '93 issue, and immediately wished it had arrived at the local Barnes and Noble just a week earlier. That week, while applying for a job at an arcade of all places, I was

zined to (and took) one of the very honesty tests you described in your magazine.

The manager I submitted my application to referred to the test (formally called a "PSI Examination") as a personality evaluation, completed so the company could ascertain "what kind of a person I am." Previous to taking this test I had not been familiar with this type of evaluation, so I went in knowing and expecting nothing. Almost immediately after reading the first few questions, I pegged the "new" for what it was, with its misleading questions geared to force one to trip up.

Unfortunately, even realizing the testmaker's motives, I screwed up according to your article. I attempted to answer The Questions in a way that normal, mostly honest people would (even down to knowing the lowest denomination on the question referring to the approximate value of all monies or penniless value from a one-job recession.) On a better note, the job wasn't all that important to begin with, and it takes me not that an honesty test might have had me a job with this company. Incidentally, the manager of the arcade "The" had no clue how the test was scored or evaluated when I inquired. What she did know was that the possible answers are all assigned a number, and the numbers chosen by the test-taker are recorded and read over the phone to the district headquarters of the company. The company presumably feeds the numbers into its computer and our boss over's rating as an honest individual. There was also a free-form written part of the test where the test-takers asked if there were any inconsistencies make concluding questions on the test that we would like to comment on. Needless to say, I wrote them an essay...

The Vampire Club/rifle

JOIN THE LITERARY  
WORLD!  
HAVE A LETTER  
PUBLISHED IN 2600.  
2600 Letters  
PO Box 99  
Middle Island, NY  
11953  
2600@well.sf.ca.us



## PASSAGEWAYS TO THE INTERNET

- Eindhoven University, Netherlands** 219-980-6866 300-2400  
 +31 40 430032 300-9600  
 +31 40 435049 300-2400  
 +31 40 455215 2400
- University of Manitoba**  
 204-275-6100 2400 or less  
 204-275-6132 9600 & 14.4
- University of Washington**  
 206-685-7724 2400  
 206-685-7796 9600 and above
- Columbia University, New York, NY**  
 212-854-1812 1200-2400  
 212-854-1824 1200-2400  
 212-854-1896 1200-9600
- New York University**  
 212-995-3600 2400 and lower  
 212-995-4343 2400 and up
- Southern Methodist University, TX**  
 214-368-1721  
 214-368-3131
- University of Pennsylvania**  
 215-898-0834 9600+  
 215-898-4781 1200  
 215-898-6184 2400
- Case Western Reserve University, OH**  
 216-368-8888
- South Bend, IN**  
 219-237-4116 300-2400  
 219-237-4186 300-2400  
 219-237-4413 300-2400  
 219-262-1082 300-2400
- Fort Wayne, IN**  
 219-481-6905 300-1200
- Northwest, IN**  
 219-980-6653 300-2400
- Purdue University, IN** 219-989-2900 VAX  
**University of Maryland, College Park, MD** 301-403-4444 v.32 bis  
**Illinois State University** 309-438-8070 9600 E71  
**ISUNET** 309-438-8200 9600 N81-LANACS  
**DePaul University, IL** 312-362-1061 9600 E71  
**Cisco Terminal Servers, Chicago** 312-413-3200 7 bits mark parity  
 312-413-3212 8 bits no parity  
**Ball State University, IN** 317-285-1000  
 317-285-1108  
**Kokomo, IN** 317-455-2426 300-1200  
**Purdue University, IN** 317-494-6106  
**Indiana University East** 317-973-8265 300-1200  
**University of Central Florida** 407-823-2020  
**University of Maryland, Baltimore, MD** 410-333-7447 v.32 bis  
 410-789-7854 2400  
**University of Pennsylvania, Oakland** 412-621-2582 300-2400  
 412-621-5954 300-2400  
**University of Pennsylvania, Greensburg** 412-836-7123 300-2400
- 412-836-9997 300-2400  
**University of Pennsylvania** 412-938-4063  
**Laval University, MO** 418-656-3131 STV32 bis  
**Laval University, MO** 418-656-7700 2400  
**University of New Mexico** 505-277-5950 IBM 300-2400  
 505-277-6390 IBM 7171 300-1200  
 505-277-9990 CDCN 300-2400  
 505-277-9993 CDCN 9600  
 505-277-9994 CDCN 1200-9600
- Southwest Texas State University** 512-245-2631  
**University of Waterloo, ONT** 519-725-5100  
**Simon Fraser University, BC** 604-291-4700 2400  
 604-291-4721 2400 (v.42bis)  
 604-291-5947 14.4  
**University of Victoria, BC** 604-721-2839  
 604-721-6148  
**University of Kentucky** 606-259-1200 1200  
 606-258-1996 v.32 bis or lower  
 606-258-2400 2400  
**Eastern Kentucky University** 606-622-2340 2400-9600  
**Princeton University, NJ** 609-258-2530 2400 OUTDIAL  
**Princeton University, NJ** 609-258-2630 9600 OUTDIAL (ATDT9 7d 5d code)  
**Rider College, Lawrenceville, NJ** 609-896-3959 9600  
**Vanderbilt University, TN** 615-322-3551 2400  
 615-322-3556 2400
- 615-343-1524 High speed (v.32 bis v.42 bis)  
**University of Tennessee at Knoxville** 615-974-3021  
 615-974-4282  
 615-974-6711  
 615-974-6741  
 615-974-6811  
 615-974-8131  
**Northeastern University, Boston, MA** 617-373-8660 14.4  
**University of Nevada, Las Vegas** 702-895-3955  
**George Mason University, Fairfax, VA** 703-993-3536  
**Humboldt State University, Arcata, CA** 707-826-4621 2400  
**University of Houston** 713-749-7700 300-1200  
**DECserver** 713-749-7740 2400 DECserver  
 713-749-7750 19 200 Xyplex  
**Colorado College, Colorado Springs, CO** 719-389-6574  
 719-389-6759  
 719-389-6889  
 719-389-6890  
**University of California at Santa Barbara** 805-893-8400 300-2400  
**Bloomington, IN** 812-855-4211 300-1200  
 812-855-4212 1200-2400  
 812-855-9656 1200-2400  
 812-855-9681 9600



<b>Southwest, IN</b>	814-827-4486 300-2400
812-944-8725 300-2400	<b>Sherbrooke University, QUE</b>
812-944-9820 300-2400	819-569-9041 2400
812-945-8114 300-1200	819-821-8025 Zyxeil
<b>University of Pennsylvania,</b>	<b>Bishop University, QUE</b>
<b>Johnstown</b>	819-822-9723 2400
814-269-7950 300-2400	<b>Michigan Tech</b>
814-269-7970 300-2400	906-487-1530
<b>University of Pennsylvania,</b>	<b>Pomona/Pitzer College, CA</b>
<b>Bradford</b>	909-621-8455
814-362-7558 300-2400	<b>Sacramento State, CA</b>
814-362-7597 300-2400	916-456-1441
<b>University of Pennsylvania,</b>	<b>Wake Forest University, NC</b>
<b>Titusville</b>	919-759-5814



## HACKERS FOR "BOB"

## MORE MEETING ADVICE

by The Indicator of D.C.

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

These two paragraphs are the First and Fourteenth Amendments to the Constitution. The First says that as a citizen you have a legal right to peacefully assemble and the federal government cannot take that right away from you. It does not say that a State has to allow you to assemble. This was the case until June 9, 1868. The Fourteenth Amendment applied the Constitution and its protections to the States. Before this, each individual State could prohibit the free assembly of persons.

Presently, we can gather on public space and discuss whatever subject comes to mind. There are exceptions to this, however. You cannot stand on the corner of Broadway and discuss the violent overthrow of the government. Nor can you discuss the intimate details of your love life.

So what have we learned? The First and Fourteenth amendments allow us to gather for meetings anywhere we want, and no one can stop us. Right? Wrong! The Constitution applies to governments and is limited in its application of powers to private industry. For example, in Washington, D.C. there is a law called Unlawful Entry. It states that any person who willfully remains on any property after being asked to leave by the rightful owner or person then in charge is guilty of a misdemeanor and subject to arrest. The constitutionality of this law has been tested and affirmed. Your local jurisdiction may have a law similar to this under different names (Criminal Trespass or Trespassing). The easiest way to find out is to pick up a (909) phone and call your local police department. Ask them. Don't be afraid. You cannot get in trouble for being a concerned citizen.

What is the basis for these laws? Consider this:

You own a beautiful piece of property that overlooks a great seascape. People are using your property for religious gatherings and artistic inspiration without your permission. If the constitution applied to private property you couldn't stop these people. But since it does not, you can have them removed or arrested, if your local law allows.

Of the 20 2660 meetings that take place throughout the U.S., 13 take place in malls, five in other private places, and two are unknown to this writer. Cincypri Center and Amtrak are private institutions. It sounds like the Galleries on South University and Union Station are also private but I cannot tell by their names. Malls are almost exclusively privately owned. I cannot recall seeing a government owned mall lately. Being privately owned, the rightful owner or the person then in charge can ask you to leave (depending on your local law). The sad thing is that you will have to follow his directions and then follow up with a civil suit. What you have that suit on is another problem. It would not fall under a racial bias, nor a gender bias. If you do not leave at their request, you leave yourself vulnerable to arrest. What does this mean to us dedicated 2660ers?

When you are attending a 2660 meeting, be sure to know the law in your area. If you are hosting a party or attending a party at a mall or on other private property, be informed. When approached by a security officer, police, or the management, don't go on blabbering how the First Amendment allows you to gather any place you like. It doesn't. Instead, do the following:

- 1) If the area you are meeting in has stores, purchase some merchandise that is sold in these establishments prior to your meeting. When approached by the charging person, explain that you have just made purchases from the establishments. Does he/she really want to throw out a buying customer?
- 2) Explain to the charging person your intentions of the gathering. Don't forget class points. You chose this area because of a) its successful reputation, b) its great location, c) the fine merchandise, d) all of the above. This sounds like a bunch of crap (which it is); but it will strengthen any court case you bring about in the future.
- 3) As a last resort, inform team of your research into the local laws and ordinances of



# BOOK REVIEW

Virtual Reality

By Howard Rheingold

Published by:

Touchstone, Simon & Schuster Inc.

New York, NY

Distributed in Canada by:

General Publishing

Don Mills, ONT

416 pages, \$12.00 (United States)

Reviewed by W. Ritchie Benedict

The first time I ever heard the term Virtual Reality was not in connection with computers, but was in reference to the mental world we all carry around with us in our heads. When, I suppose, does reality we describe what happens on the latest frontier in computer technology. About a month ago, I had an opportunity to observe virtual reality in action at a display at the Calgary Stampede. There were the enclosed computer workstations with participants wearing monitors depicting the scores transmitted into the headsets, which in the distance looked a game with a lot of stairways. One participant became so entranced in attempting to zip his opponent that he tumbled back into the arena. Outside, and in language that had to be deleted. Such is the power of this ultra-realistic technology.

We are still a long way from the realism of the handbook depicted on TV's Star Trek: The Next Generation, but at the present rate, it won't be long before we see extraordinary developments. Although, in only 15 years, we have gone from the first crude video game "Pong" to CD-ROM with stereo sound and prodigious amounts of memory. The author in his first detailed exploration of the "Virtual Age" is one Howard Rheingold, the editor of the Whole Earth Review, who (appropriately) lives in the San Francisco Bay area. He traces the dream of the new era back to the Chrenamir Chromascope 3D movies of the 1930's. A man named Morton Heilig actually made plans for an "Experience Theatre" back in 1955, and patented a head-mounted stereoscopic television display. In 1960, Heilig is still alive, in the states, and is delighted to see the seeds of his dream coming to fruition. William Gibson, the well-known science-fiction writer, had the honor of originating the word cyberspace (in his 1984 novel *Countdown*), which is now used widely to describe the virtual computer-generated reality that is the subject of this book. The point is made that the computer industry in its early years was not oriented towards the highly creative approaches that virtual reality needs.

I recall a computer demonstration I attended back in the very early 80's when you could touch the screen to choose an option. This in turn led to give-

ment into trouble. Both can be arrested, but the case of innocence for Bill is very strong. It must be proven in court, requiring the expense of thousands of dollars for an attorney. A court-appointed attorney can be assigned, depending on financial need, with his/her cost coming out of taxpayer money.

One can see the parallels of this story to that of 2600 meetings. Yes, 2600ers gather in places to discuss illegal acts. Are they conspiring to commit these offenses? Maybe. It depends upon each individual person. Let's say a conversation was entered dealing with the sale, not possession, of proprietary information. No one from the discussion group does anything to forward the idea of the sale. Is this legal? Yes, under the First Amendment. What if one of the members contacts an underground fence offering the document for sale based on information he discussed at the meeting? Is this conspiracy? I'm sure Law Enforcement could substantiate enough evidence to bring about the arrest of the discussion group, but would they have enough evidence to prove "beyond a reasonable doubt" their case in court? Maybe not. However, they have succeeded in harassing the group and costing both the taxpayers and the group members several thousands of dollars in court and attorney's fees. Do you have any means of redress? You could try to sue for damages incurred due to the inconvenience of the arrest, but if the Law Enforcement agency did its job correctly, you will not win.

I cannot speak for all states but the basic for most laws are the same. As mentioned earlier, call your local police or the nearest state police office. You cannot get in trouble for asking. Also ask for examples and a written reply.

The writer is "heavily involved" with the law enforcement community.

## THE 2600 VOICE BBS

NOW OPEN 24 HOURS A DAY  
(10288) 0700-751-2600  
JOIN THE FUN!

mounted sensors. The author was one of the first to by a NASA prototype in 1968 that demonstrated the amazing potential capabilities of the system - the near drawback being a time lag when the operator moved his hand. So, what good is it all, other than the ultimate in video-game realism? Well, for starters, it holds promise for architectural design, flight training, planetary exploration, medical and optical research, and even simulated sea. There are currently no less underway to bring the dimension of tactile sensation to the armature, possibly by means of a lightweight body suit with many sensors built into it. There is undoubtedly going to be a race (already in the very early stages) between Japan and America to see who will reap the glory (and the profits) of producing the first viable system for the public. There are applications to the amusement park field so Disney will naturally be interested. Finally, virtual reality may change our perspective of what we think of as "real" forever, making it hard to determine what is an illusion and what is not. Rheingold does an excellent job of detailing all of the various elements that go into producing virtual reality. He even mentions a couple of potential dangers in the concluding chapter. What if the virtual worlds turn out to be so seductive that people will want to spend all of their lives there instead of in the so-called "normal" reality? Addition to other words: Then there is the weapons potential - it has always been easier to kill people if you are disconnected from them by machines, as any border plot from World War II will tell you. A doctor could zap robots with a laser-mounted cannon combined with a virtualized system, without ever leaving the comfort of his presidential palace many miles away. However, we must not let us be lulled into a false sense of security. There is a huge potential for psychological or physically handicapped individuals to experience things that would otherwise be closed to them forever. It seems that eventually we may never have to leave our homes in order to perform work, entertain ourselves, or learn new skills. Healey's *Brain Wave* may yet prove to be prophetic. Ultimately it may change the way we look at ourselves as human beings or perhaps we will start to view ourselves as hybrids between human and computer. It will be that profound a change.

The book gives the average person a surprising insight into just how far along the road to a sensor fusion reality we are. Ironically, it takes the very, a self virtual reality device to do so - i.e., the print word. Well, everyone has used reading at one time or another to turn off the annoyances of the "real" world. The author is that in the future there will be a new and fantastic means of doing so. This is a book that will leave you gasping - don't miss it!

intimidating. If possible, give them a copy of the law. Ask them to have the police respond. When an officer arrives, explain that this security officer is unlawfully asking you to leave when you wish to stay. But if a police officer asks you to leave, do not! Do not ask for his name and badge number, you can see that. If you can't, find his car and write down the ID number. Then call the station he is from and ask to speak to a supervisor. Inform the supervisor of the squad car number, the description of the officer, and what happened. Make a written complaint if possible.

You must remember to be calm and rational during these proceedings. If not, you could be placed under arrest for disorderly conduct or some such. Although not what you were originally bothered with, the security officer has succeeded in his task to get rid of you.

2600 meetings are great ideas for the free exchange of ideas and are, in theory, what this country was founded upon. But, they are not worth getting arrested for if you are wrong. There are plenty of legal places to hold meetings. Try a public park or parking area. Call your local seat of government and ask to use their meeting room. How about that for irony? Using a government establishment to hold a 2600 meeting! Under the First Amendment, they cannot deny you. Look at the court record of such groups as the KKK. They must and march on any public space they like with the proper permits. 2600ers can do the same.

In writing this, a few friends have raised valid questions, which I am sure other 2600ers will ask. What about conspiring to commit a crime? Isn't meeting to discuss committing crimes illegal? Yes and no.

Conspiracy is defined as an agreement to perform an illegal act. Most states, in defining the acts that constitute conspiracy, require an overt act. The best definition would be an example itself. John and Bill are eating dinner while discussing robbing a bank. They talk about the getaway car, what type of gun to use, and the best time to commit the robbery. Both finish dinner and go their separate ways until they meet at work the next day. John tells Bill he bought the gun and obtained the getaway car. As of this moment, John and Bill can be arrested for conspiring to commit a bank robbery.

The First Amendment protects our freedom of speech to a degree. If John and Bill had not done anything else but talk about the bank robbery, no harm could have come to either of them. Since John purchased the gun and getaway car, he showed his intentions to follow through with their plan. This was the overt act. This was what got

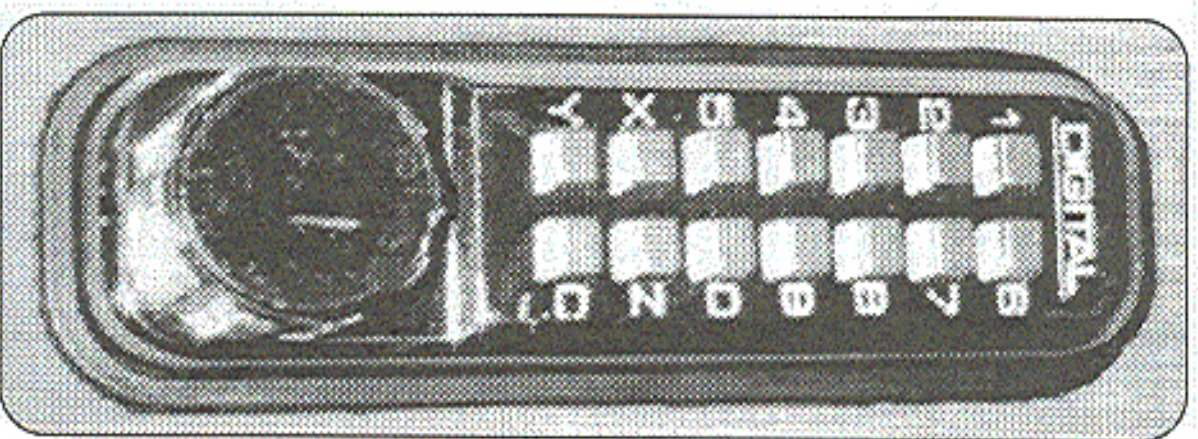


# DIGITAL LOCKS

ANOTHER CONTRADICTION IN TERMS

With only 1287 possible combinations, the fully mechanical Digital locks are sure to be a hit with the kids. Even still, we backed one (the one pictured in fact) and found the experience dull if not plodding. Call us sentimental, but for some reason, it just wasn't as fun as cracking a Simplex lock. Besides, they're hard as hell to find in the first place.

The lock's combination is always five alphanumeric characters long, chosen from a possible ten digits (0-9) and three letters (X-Z), and the order doesn't matter. Be sure to press the "C" before each combo entry to clear the lock.



Digital locks:  
Not as fun as Simplex.

02948	02949	02950	02951	02952	02953	02954	02955	02956	02957	02958	02959	02960	02961	02962	02963	02964	02965	02966	02967	02968	02969	02970	02971	02972	02973	02974	02975	02976	02977	02978	02979	02980	02981	02982	02983	02984	02985	02986	02987	02988	02989	02990	02991	02992	02993	02994	02995	02996	02997	02998	02999																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
03000	03001	03002	03003	03004	03005	03006	03007	03008	03009	03010	03011	03012	03013	03014	03015	03016	03017	03018	03019	03020	03021	03022	03023	03024	03025	03026	03027	03028	03029	03030	03031	03032	03033	03034	03035	03036	03037	03038	03039	03040	03041	03042	03043	03044	03045	03046	03047	03048	03049	03050	03051	03052	03053	03054	03055	03056	03057	03058	03059																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																									
03060	03061	03062	03063	03064	03065	03066	03067	03068	03069	03070	03071	03072	03073	03074	03075	03076	03077	03078	03079	03080	03081	03082	03083	03084	03085	03086	03087	03088	03089	03090	03091	03092	03093	03094	03095	03096	03097	03098	03099	03100	03101	03102	03103	03104	03105	03106	03107	03108	03109	03110	03111	03112	03113	03114	03115	03116	03117	03118	03119	03120	03121	03122	03123	03124	03125	03126	03127	03128	03129	03130	03131	03132	03133	03134	03135	03136	03137	03138	03139	03140	03141	03142	03143	03144	03145	03146	03147	03148	03149	03150	03151	03152	03153	03154	03155	03156	03157	03158	03159	03160	03161	03162	03163	03164	03165	03166	03167	03168	03169	03170	03171	03172	03173	03174	03175	03176	03177	03178	03179	03180	03181	03182	03183	03184	03185	03186	03187	03188	03189	03190	03191	03192	03193	03194	03195	03196	03197	03198	03199	03200	03201	03202	03203	03204	03205	03206	03207	03208	03209	03210	03211	03212	03213	03214	03215	03216	03217	03218	03219	03220	03221	03222	03223	03224	03225	03226	03227	03228	03229	03230	03231	03232	03233	03234	03235	03236	03237	03238	03239	03240	03241	03242	03243	03244	03245	03246	03247	03248	03249	03250	03251	03252	03253	03254	03255	03256	03257	03258	03259	03260	03261	03262	03263	03264	03265	03266	03267	03268	03269	03270	03271	03272	03273	03274	03275	03276	03277	03278	03279	03280	03281	03282	03283	03284	03285	03286	03287	03288	03289	03290	03291	03292	03293	03294	03295	03296	03297	03298	03299	03300	03301	03302	03303	03304	03305	03306	03307	03308	03309	03310	03311	03312	03313	03314	03315	03316	03317	03318	03319	03320	03321	03322	03323	03324	03325	03326	03327	03328	03329	03330	03331	03332	03333	03334	03335	03336	03337	03338	03339	03340	03341	03342	03343	03344	03345	03346	03347	03348	03349	03350	03351	03352	03353	03354	03355	03356	03357	03358	03359	03360	03361	03362	03363	03364	03365	03366	03367	03368	03369	03370	03371	03372	03373	03374	03375	03376	03377	03378	03379	03380	03381	03382	03383	03384	03385	03386	03387	03388	03389	03390	03391	03392	03393	03394	03395	03396	03397	03398	03399	03400	03401	03402	03403	03404	03405	03406	03407	03408	03409	03410	03411	03412	03413	03414	03415	03416	03417	03418	03419	03420	03421	03422	03423	03424	03425	03426	03427	03428	03429	03430	03431	03432	03433	03434	03435	03436	03437	03438	03439	03440	03441	03442	03443	03444	03445	03446	03447	03448	03449	03450	03451	03452	03453	03454	03455	03456	03457	03458	03459	03460	03461	03462	03463	03464	03465	03466	03467	03468	03469	03470	03471	03472	03473	03474	03475	03476	03477	03478	03479	03480	03481	03482	03483	03484	03485	03486	03487	03488	03489	03490	03491	03492	03493	03494	03495	03496	03497	03498	03499	03500	03501	03502	03503	03504	03505	03506	03507	03508	03509	03510	03511	03512	03513	03514	03515	03516	03517	03518	03519	03520	03521	03522	03523	03524	03525	03526	03527	03528	03529	03530	03531	03532	03533	03534	03535	03536	03537	03538	03539	03540	03541	03542	03543	03544	03545	03546	03547	03548	03549	03550	03551	03552	03553	03554	03555	03556	03557	03558	03559	03560	03561	03562	03563	03564	03565	03566	03567	03568	03569	03570	03571	03572	03573	03574	03575	03576	03577	03578	03579	03580	03581	03582	03583	03584	03585	03586	03587	03588	03589	03590	03591	03592	03593	03594	03595	03596	03597	03598	03599	03600	03601	03602	03603	03604	03605	03606	03607	03608	03609	03610	03611	03612	03613	03614	03615	03616	03617	03618	03619	03620	03621	03622	03623	03624	03625	03626	03627	03628	03629	03630	03631	03632	03633	03634	03635	03636	03637	03638	03639	03640	03641	03642	03643	03644	03645	03646	03647	03648	03649	03650	03651	03652	03653	03654	03655	03656	03657	03658	03659	03660	03661	03662	03663	03664	03665	03666	03667	03668	03669	03670	03671	03672	03673	03674	03675	03676	03677	03678	03679	03680	03681	03682	03683	03684	03685	03686	03687	03688	03689	03690	03691	03692	03693	03694	03695	03696	03697	03698	03699	03700	03701	03702	03703	03704	03705	03706	03707	03708	03709	03710	03711	03712	03713	03714	03715	03716	03717	03718	03719	03720	03721	03722	03723	03724	03725	03726	03727	03728	03729	03730	03731	03732	03733	03734	03735	03736	03737	03738	03739	03740	03741	03742	03743	03744	03745	03746	03747	03748	03749	03750	03751	03752	03753	03754	03755	03756	03757	03758	03759	03760	03761	03762	03763	03764	03765	03766	03767	03768	03769	03770	03771	03772	03773	03774	03775	03776	03777	03778	03779	03780	03781	03782	03783	03784	03785	03786	03787	03788	03789	03790	03791	03792	03793	03794	03795	03796	03797	03798	03799	03800	03801	03802	03803	03804	03805	03806	03807	03808	03809	03810	03811	03812	03813	03814	03815	03816	03817	03818	03819	03820	03821	03822	03823	03824	03825	03826	03827	03828	03829	03830	03831	03832	03833	03834	03835	03836	03837	03838	03839	03840	03841	03842	03843	03844	03845	03846	03847	03848	03849	03850	03851	03852	03853	03854	03855	03856	03857	03858	03859	03860	03861	03862	03863	03864	03865	03866	03867	03868	03869	03870	03871	03872	03873	03874	03875	03876	03877	03878	03879	03880	03881	03882	03883	03884	03885	03886	03887	03888	03889	03890	03891	03892	03893	03894	03895	03896	03897	03898	03899	03900	03901	03902	03903	03904	03905	03906	03907	03908	03909	03910	03911	03912	03913	03914	03915	03916	03917	03918	03919	03920	03921	03922	03923	03924	03925	03926	03927	03928	03929	03930	03931	03932	03933	03934	03935	03936	03937	03938	03939	03940	03941	03942	03943	03944	03945	03946	03947	03948	03949	03950	03951	03952	03953	03954	03955	03956	03957	03958	03959	03960	03961	03962	03963	03964	03965	03966	03967	03968	03969	03970	03971	03972	03973	03974	03975	03976	03977	03978	03979	03980	03981	03982	03983	03984	03985	03986	03987	03988	03989	03990	03991	03992	03993	03994	03995	03996	03997	03998	03999	04000	04001	04002	04003	04004	04005	04006	04007	04008	04009	04010	04011	04012	04013	04014	04015	04016	04017	04018	04019	04020	04021	04022	04023	04024	04025	04026	04027	04028	04029	04030	04031	04032	04033	04034	04035	04036	04037	04038	04039	04040	04041	04042	04043	04044	04045	04046	04047	04048	04049	04050	04051	04052	04053	04054	04055	04056	04057	04058	04059	04060	04061	04062	04063	04064	04065	04066	04067	04068	04069	04070	04071	04072	04073	04074	04075	04076	04077	04078	04079	04080	04081	04082	04083	04084	04085	04086	04087	04088	04089	04090	04091	04092	04093	04094	04095	04096	04097	04098	04099	04100	04101	04102	04103	04104	04105	04106	04107	04108	04109	04110	04111	04112	04113	04114	04115	04116	04117	04118	04119	04120	04121	04122	04123	04124	04125	04126	04127	04128	04129	04130	04131	04132	04133	04134	04135	0







## Foulsups and Blunders

Over the past couple of years, Suffolk County (New York) officials have been planning a state-of-the-art computer system to handle everything from emergency phone calls to the police and the departments to fingerprint data and court records. The system so far has cost \$15.9 million, is two years overdue, and last but not least, doesn't work. It was designed by Unisys and is supposed to do all kinds of magical things in an average of 3.5 seconds. In early tests, the system froze up entirely. More recent tests have seen crashes occur as long as 30 seconds to complete and an unexplained instance of garbage being sent throughout the network. According to County Executive Assessor John Gallagher, "It began to act strangely and started printing information into the records machine that was usually withheld to the information called in." All in all, the system has failed time over. The county executive has repeatedly lost faith and has referred to it as "unreliable and unreliable." The system uses A-15 mainframe computers.

## Touch Tone Registration

Colleges across the country are using a new method of registering students: touch tone phones. We checked out two universities near our old founded sister systems opening at first. At Suffolk Community College, students simply dial (516) 696-4710. The only information required by the system is the student's Social Security number. Armed with this information, anyone can change the past student's schedule, adding or dropping courses to their heart's desire. Of course, you also need a copy of the current academic schedule in order to obtain the proper four digit extension numbers. This schedule is available throughout the campus. The State University of New York at Stony Brook has a more secure system. Yes, they use the Social Security number as the student identifier, but at least they have the good sense to require a password. Of course, without exception, the password is the student's birthdate (MMDDYY). If friends are meaning to the words "meaning instructions", Right now, they're having pretty slow. Oh yes, the number for their system is (516) 633-2193.

## Electronic Mayhem

Earlier this year, materials were started when an electronic highway sign on I-95 in Connecticut suddenly announced "You All Suck." The person who did this, and somehow managed to get caught during it was an accident. He thought it was just a computer bulletin board system and that there was no password protection whatsoever.

In a similar story, a UC San Francisco student changed the outgoing message on the University Health Insurance Plan to say that the system had poor security. After initially calling the number for information, the student was able to see the flaws in the system. It was

deliberately simple," he said. "The message actually offered a 'Change personal profile' option, so I pressed it to see what would happen. Before I knew it, it was helping me change the menu and outgoing message, and I didn't even need a password." The student notified the campus strategists and the University Health Insurance Office but declined to give his name, fearing disciplinary action. He said he wanted people to know that "teachology is a really powerful tool."

## The Latest From The U.K.

According to British Telecom, insects by "organism and well-equipped stimulant" on BT's 110,000 payphones rose from about 6,500 by January 1993. But September 1991 to record 6,500 by January 1993. But thanks to a "determined campaign", the number of insects has since been cut by around 50 percent. Part of this campaign includes psychophones that speak saying "Warning - tamper alarm, police have been informed." Warning tamper tones are also being used. They really go all out on these studies, by the way. They have frog, chrys, grass releases, you name it. But best of all are the sometimes startling conclusions they reach. Like "These figures show there is a direct relationship between the number of snakes and the number of payphones in working order." Ouch.

Telephone competition is heating up in the U.K. Mercury, the number two company, recently announced that its new mobile phone service (One-2-One) a joint venture with US West) was offering free off-peak local calls. Mercury's Lord Young claimed that "with the free calls, you'd be mad to use a BT phone." But a London newspaper, *The Independent*, wrote, "On present terms, anyone ringing one free BT phone from the socket and replacing it with One-2-One would be advised to annual in accountant or a psychiatrist. For Lord Young's free calls are only free once you have bought a handset for 250 pounds and paid a monthly fee of twenty 15 pounds, and are prepared to pay tariffs up to 17 times those charged by BT to use the Mercury telephone at peak periods."

For those of you in Ireland, dialing US allows you to call any number within England. For instance, to reach (071) 2234567 in London, from Ireland you would dial 03 071 2234567. Domestic information is available at 190. Great Britain information at 197. International information is available by dialing 114, or 10 if calling from old style A/B numbers. The international prefix is 16. So to call in here at 2600, using the United States country code of 1, you would dial 16 1 316 7512600 999 is the number for emergency calls, 1601 is the prefix for toll-free calls, called Freephone, 1199 gives you an 18 hour advance weather forecast from most locations. To call Ireland Direct from the United States, dial 800-553-6382 for AT&T, 800-383-0193 for MCI, or 800-473-0133 for Sprint. From Canada, dial 800-461-2050. From France, 1900 333. Spain, 900 990 333. The Netherlands, 06 072 0333, and

Belgium/Northern Ireland, 0800 89 0353. If you haven't figured it out yet, Ireland's country code is 353.

In Perth, Scotland, the first uses of Call Return for the British Isles are underway. According to BT,

"Customers using the service will enter a simple code on their telephone and an automatic voice at the exchange will immediately give details of the last calling number, whether or not the call was answered at the time. A second code will enable the number to be dialed automatically by the exchange if the customer wishes to return the call immediately, or the number can be noted so that the customer can ring back at a more convenient time." Caller Display is the British version of Caller ID and it's being introduced in the same stepwise style as it is in the States. BT claims that 90 percent of its customers intend to use it to support the service and that 74 percent "could see no reason why anyone would want to prevent the display of their number." They also claimed that when blocking was made available, only 20 percent of all calls used it. BT expects these services to be available to more than 95 percent of its customers in 1994. They also refer to the new technology as the CT signaling process.

In more British news, the competition to Proseidy has begun. On April 16, 1993, the biggest change in national and international dialing codes in 25 years will take effect. On that fateful day, which also happens to be Easter Sunday, presumably to emphasize the importance of the event, an extra digit is 1. So London, which only a couple of years ago was 01 and is now 011 or 081, will soon be 0111 or 0181. The toll-free code of 0800, the mobile codes of 0860 and 0840, and the information and entertainment services code of 0991 will remain unchanged. The general idea is for codes beginning with 01 and eventually 07 to be geographical in nature, 01 to be more service numbers, 07 to be for "lifestyle" numbers (the same idea as AT&T's EasyReach service), and 08 to be for specialty oriented premium services. 04, 05, 06, and 09 are not going to be used right now. Five other (London, Sheffield, Nottingham, Leicester and Bristol) will get brand new city codes. Their current codes are 0353, 0142, 0601, 0553, and 0272 respectively. The corresponding new codes will be 0113, 0114, 0115, 0116, and 0117. Nottingham and Bristol will add a 9 in front of all local numbers, the other cities will add a 2. And, finally, the international dialing code will change from 010 to 00. This is in keeping with the new European Community standard, as is the transition of the emergency number from 999 to the standard 112. If you know anyone in the U.K., it's probably best to leave them alone for a while.

There are no insurance times.

So which collect service is really cheaper? Here's what we were able to figure out. For a collect call from our Long Island office to an abandoned warehouse in San Francisco, the rate we got for dialing 04 with AT&T was \$2.20 for the first minute and 25 cents per minute thereafter. By using AT&T's 1-800-OPERATOR service, the rate was \$1.79 for the first minute and 24 cents for each additional minute. MCI's rates were a bit harder to interpret. To start with, none of their operators know the rates. Each time you ask, you're transferred to the "rate operator" which is a great way of saying customer service. Anyway, their rate for a 04 call to the same number was either \$3.36 or \$2.20 for the first minute and 26 cents per minute thereafter. It really depends who you ask. By using MCI's 1-800-COLLECT service, the rate for the same call is \$1.79 for the first minute and 24 cents for each additional minute, identical to 1-800-OPERATOR. Their's started to get complicated when we asked about the 04 calls. We tried to make a call to the government mansion in Albany, NY. AT&T's 04 rate was 1.85 for the first minute and 20 cents for each additional minute. We got different answers for using 1-800-OPERATOR, ranging from it being impossible because it was within the same state to \$1.85 for the first minute and 21 cents for each minute thereafter. MCI charged \$1.82 for the first minute and 20 cents for each additional minute using 04 and their 1-800-COLLECT rate (we think) is \$1.65 for the first minute and 20 cents for each additional minute. One MCI representative quoted us a rate of one cent a minute for a night call and four cents a minute for a day time call. We know right away that those numbers were bogus but we have to wonder how many people would have fallen for it. With this kind of service, it's no wonder MCI has never attached their name to any advertisement of 1-800-COLLECT. Incidentally, AT&T ran a very strange promotion for their 1-800-OPERATOR service, or so they claim. Up until December 5th, there were no surcharges on collect calls and all daytime collect calls cost 15 cents a minute. If those numbers were true, that it was actually cheaper to call somebody collect than to call them direct. We should point out that it took an average of five minutes to get an answer to a single rate question from either company. It's no wonder consumers are totally confused since the companies themselves can't seem to figure it out. There remains in the United States, unlike Great Britain, doesn't occur on one day. It's with us all the time.

## Fantasy World

People just love it when we publish information on Walt Disney World. So here's some helpful hints on their Guest Messaging Service, which everyone staying at the Walt Disney World Resort gets. Everyone. To receive messages from anywhere in the world, all you have to do is dial (407) 871-1588 (only the last five digits are necessary from within the park). Call into your room number and your secret password. You can easily remember your secret

## Collect Your Wits

So which collect service is really cheaper? Here's what



password because it's set to the first four letters of your last name. Messages also stay alive for three days after you check out, unless you delete them. While you can no longer get messages once you've checked out, you are still able to access old messages by calling (407) 827-1699.

## Start the Insanity!

New dual purpose phone cards are starting to appear in the United States, credit collections are springing up in hot pursuit. Phone companies are encouraging this behavior by producing colorful and unique telephone cards, sometimes centered around special events. The Democratic Convention in New York City in 1992. On September 25th, Richmond, Virginia hosted the first International Credit Card Co-terminus. Co-terminus means see this telephone for cards making the current ecstasy that is our stamp collectors constantly experience. You can find over publishers of more than 400 telephone cards by getting the 1993 ICS Telephone Card Catalog available for \$5 from Lisa Overholt, P.O. Box 8241, Melville Beach, IL 33738. You can also get information on a publication called International Telephone Cards by writing to 2035 Major Road, Colchester, Essex CO1 1X, Great Britain.

## Insuring Profits

Who really benefits from phone fraud? One has to wonder when all of a sudden the phone companies turn into insurance brokers. For \$1,200 a month (don't get caught in the sales pitch), AT&T will cover all fraudulent phone calls above \$55,000. This, naturally, doesn't include the sign-up fee. If AT&T fails to verify the customer of the fraud, the insurance only has to pay \$12,500. Sprint has a similar program, no co-insurance designed to provide the best service possible or the lowest cost. We'd like to know how much fraud would have to occur for the phone companies to lose even one cent on this plan.

## New Numbers

Did you know that BellSouth is experimenting with three digit N11 codes? 211, 311, 511, 711, and 811 are going to be used for the next two years for various "pay" services run by independent companies. Does this mean you'll be able to be ripped off by a 900 number without having to dial ten digits? Anything's possible.

Meanwhile, in Canada, 111 is being allocated for deal people who will be able to reach a relay services operator with a TDD text telephone.

Just when you thought you were safe from 900 numbers, AT&T is arranging to have the 900-555 exchange after still more pay services. The reasoning is that since many major companies have 900 calls, they don't block calls to 900-555 since everybody knows 555 is information and information wants to be

free, etc. So AT&T's plan would put victims services in the 555 exchange that are "business related" and have nothing to do with entertainment. (This means that USA Today's 900-555-5555 number would now certainly have to vacate.) Despite this restriction, it still sounds to us like AT&T is taking advantage of a security hole to push more pay services down our throats.

The 200 area code has reportedly been allocated to AT&T for its "new number" personal communications system. Other reports indicate that the 500 area code is being allocated to multiple carriers for similar services. We don't know if this means subscribers or AT&T's employees will have to change their phone numbers. It would be pretty ironic though, since the service's initial selling point was that you would never have to change your number again.

Some new country codes for some new countries, the new Yugoslavia (Serbia and Montenegro) - 381 (formerly 38); Croatia - 385; Slovenia - 386; Macedonia (not the Greek one) - 389; and Bosnia/Herzegovina - 387. Don't expect to get through on that line one for quite some time.

## Journalistic Integrity

Our local daily paper, *Monrovia*, picks itself out being technologically savvy. All too often, though, their attitudes fall flat. For instance, a story this summer scrawled "Husker Floral Plan for Big Bad Alcock." In other words, somebody who can turn on a radio and listen to unrecorded phone calls is seen, in *Monrovia's* eyes, as a hacker. Also, according to *Monrovia*, a pen register is a manual box roughly the size of a VCR, which is connected to telephone wires and prints out the telephone numbers of any outgoing calls. But with the flick of a switch, it can also be used to listen to phone conversations. Not any pen register we've ever seen. The RASIS Shuck CPA-1000 came out ten years ago and could fit in the palm of your hand. We suspect the professional snafu is even smaller. And pen registers are not used to listen in on phone calls. If they are, then they stop being pen registers. It's really quite simple.

## The Joy of New Technology

Begun and Morris County, New Jersey, probation officials are experimenting with a computerized monitoring system to replace the ordeal of visiting probation officers. Once a month, probation clients will be given a number to report any changes in their status and any problems they may have had with the law. It should probably go without saying that it's a 900 number. A computer speaks to them and, according to officials, it's very effective. "We have had people report violations that normally would not be reported to our probation officers," said Judge Del Preone, chief of probation in Morris County. "Clients believe there

is a verification system built in. They think the great computer network in the sky will schedule each up with them if they're lying." Law enforcement types just love to spread those misperceptions around.

## Caller ID News

BC Tel of British Columbia, Canada is offering a Caller ID option we haven't seen yet here in the States. Alternate Number Display (ANND) allows a number unique to the customer and different from his/her phone number to show up on the caller party's Caller ID box. The number can't be called back and anyone who tries will get a message to the effect of "The party you are trying to reach does not accept calls at this number." It costs \$3 a month for this privilege.

We discovered a brand new feature of Cable and Wireless 800 numbers. As some local Caller ID boxes are able to read data from Cable and Wireless long distance calls, to other words, if you have your own 800 number and it has feeds in other areas, you will see Caller ID, you will be able to see those numbers from around the country show up on your Caller ID box. It requires that ANND information from the calling party is being picked up by Cable and Wireless and transferred into Caller ID data on the called end. The good part about this is that companies (or people) with 800 numbers can now see who's calling them immediately without having to wait for the termination of the end of the month. The current shenanigans being going through ANI's rather expensive and inefficient special equipment. With this new method, all that is needed is a Caller ID box. The bad part is that the technology could easily be extended over to regular long distance calls, not just 800 calls. For now, it appears that this is some time away. The Cable and Wireless system is still rather spotty and unpredictable. We would caution numbers that post Caller ID data to us would not post the data through the 800 number, although nobody could tell us why.

## Corporate Ideas

Some helpful hints on choosing a good password from the Information Security Office of Sacramento: 1) Combine letters and numbers, such as the name and number of a release or friend, e.g., HISA-105; 2) Take the first or last letters from each word of a phrase, e.g., WADIASN (I Was A Dark Asid Steering Night) or EPISODEY (ONE BEAD these tanks CO BE SAFE evaded); 3) Remove all vowels from a common word or words, e.g., TRSCTR (TRP S&C R&TY-4) While it is long as possible, with a minimum of 4 characters. They also remind employees not to use any of these examples, as many people will be reading this.

Here's another corporate tip: Please don't feed the debugger driver. Programers are being designed that say "Property Dispose of Proprietary Information. Dumpster Diving is a Real Threat." According to our corporate source, "proprietary company information can travel fast once it's in the hands of a hacker. Hackers communicate via computer networks and even have their own underground newsletters." 2600

*Magazine, the Hacker Quarterly*, based in New York. "Our source goes on to advise us that "a good way to protect dumpster divers is to either direct sensitive material to mail in containers and arrange to have the letters picked up by the mail carrier, with instructions to destroy them." Our corporate source did indeed use company documents to us was, incidentally, a dumpster.

## Tidbits

Here are some fun facts. In 1992, New Jersey Bell disconnected 379,240 accounts, up from 275,895 in 1988. Supposedly, this is something about the economy. The number of business accounts disconnected was only 12,201 down from 19,478 in 1991. New Jersey Bell handles three million residential accounts and 524,000 business accounts. There's an interesting service operating at (503) 220-2222 which gives you a free doorway into the Internet. The only catch is that you have to call using AT&T. Other carriers will give you a busy signal. From this site (in Spanish, not), you can look into various systems you get what you want or read Usenet newsgroups. You can get more details by emailing support@speedway.net.

For a demonstration of AT&T's True Voice service, call 800-692-2000. AT&T claims that they've figured out a way to make callers sound clearer and more natural than over the phone. To us it sounds like they're just limiting up the volume a bit. Either way, you can expect this service to spread to your area sometime soon.

AT&T has raised the mass of information yet again. Now it is as 75 cents every time you look up a number anywhere in the country. Overseas information (which only a couple of years ago was free and a half call is free in many parts of the world) now costs a whopping \$3.95 per request. When getting the number costs several times as much as making the call, it's quite likely that fewer calls will be made. Does it take a genius to figure this out?

As most of us know, hacker conferences in the United States tend to cause a bit of commotion. But sometimes it surprises even us. A recent flyer for Pumpoon II (Philadelphia) promised that "very proceeds above the conference costs will be used to help the victims of last year's conference." How could anybody resist a promotion like that?

And finally, Caller ID has come to the rescue once again. An escaped prisoner was captured when he called the mother-in-law from a phone booth. The mother-in-law had Caller ID, enabling the cops to zero in on his location. Next time he probably won't call in.



# 2600 MEETINGS

- Ann Arbor, MI**  
 Gathered on South University.  
**Austin**  
 Northcross Mall, across the skating rink from the food court next to Pope Wood  
**Baton Rouge, LA**  
 In The LSU Under Building, between the Tiger Pause and Swenson's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9220, 5528, 9613, 9722, 9733, 9735.  
**Bloomington, MN**  
 Mall of America, food court.  
**Boise, ID**  
 Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-5432, 5559, 9700, 9758.  
**Boston**  
 Prudential Center Plaza, Terrace Food Court. Payphone: (617) 638-8522, 3415.  
**Buffalo**  
 Eastern Hills Mall (Crowned by boxes near food court).  
**Chicago**  
 Century Mall, 2828 Clark St. in the 3rd Coast Cafe.  
**Cincinnati**  
 Kenwood Town Center, food court.  
**Columbus, OH**  
 City Center Mall, outside the lower level entrance to Marshall Fields.  
**Danbury, CT**  
 Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphone: 203-746-3956, 203-754-8954.  
**Fort Lauderdale**  
 West Hollywood Shopping Alley, 266 South State Road 7. Call your mall for details or changes: 305-880-9214, 1906.  
**Houston**  
 Galactic Mall, 2nd story overlooking the skating rink.  
**Kansas City**  
 Food court at the Oak Park Mall in Overland Park, Kansas.  
**Los Angeles**  
 Union Station, corner of May & Alameda. Inside main entrance by bank of phones. Payphones: 213-672-8238, 9388, 9656, 9619, 9620, 213-625-9523, 9594, 213-674-9849, 9872, 9913, 9926.  
**Madison, WI**  
 Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 751-9746, 6914, 5916, 9223.  
**Memphis**  
 Hickory Ridge Mall, Wincrest Rd. in the food court. Payphones: 901-368-4117, 4018, 4019, 4020, 4021.  
**New York City**  
 Citicorp Center, in the lobby, near the payphones: 133 E 57th St., between Lexington & 5th. Payphones: 212-223-9011, 8827, 212-308-8044, 8182.  
**Philadelphia**  
 30th Street Artlink Station at 30th & Market, under the "Starwalk" sign. Payphones: 215-222-6880, 9881, 9779, 9789, 9832, 215-387-9751.  
**Pittsburgh**  
 Parkway Center Mall south of downtown on Route 279 in the food court. Payphones: 412-629-8228, 5927, 5934.  
**Poughkeepsie, NY**  
 South Hills Mall, at Route 9. By the payphones in front of Panda Shack, next to the food court. Payphones: 814-287-9323, 9894, 9895.  
**Raleigh, NC**  
 Crabtree Valley Mall, food court.  
**Rochester, NY**  
 Marketplace Mall, food court.  
**St. Louis**  
 Galactic, Highway 40 and Brentwood, lower level, food court area, by the freeters.  
**San Francisco**  
 4 Embarcadero Plaza (malls). Payphones: 415-392-5923, 415 6.  
**Seattle**  
 Washington State Convention Center, first floor. Payphones: 206-220-9714, 5167.  
**Washington DC**  
 Pentagon City Mall in the food court.  
**EUROPE**  
**Granada, Spain**  
 47 Km E-10 in Pinar, Antonio de Avencio Street.  
**London, England**  
 Trocadero Shopping Center (near Piccadilly Circus) next to VHS machines, 7 pm to 8pm.  
**Munich, Germany**  
 Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hauptbahnhof - Hauptstrasse). Birthplace of Hacker-Packer beer. Payphones: +49-89-591-503, +49-89-599-541, 542, 543, 544, 545.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.



## The Shirt

You won't find it in clothing stores. (We did, but that's a long story.) The 2600 Hacker Shirt could be the fashion statement of the nineties. After all, anything is possible. Two-sided, white lettering on black background, blue box schematic on the front, hacker newspaper articles on the back. \$15 each, two for \$28. K. L. XL.



## The Video

Annual footage of Dutch Jackson, pioneering a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told*. This version tells the whole story and runs about 30 minutes. \$10. VHS, NISC format only.



### 2600 SUBSCRIPTIONS

- INDIVIDUAL**  
 1 year/\$21  2 years/\$38  3 years/\$54  
**CORPORATE**  
 1 year/\$50  2 years/\$90  3 years/\$125  
**OVERSEAS**  
 1 year, individual/\$30  1 year, corporate/\$65  
**LIFETIME**  
 \$260 (also includes 1984, 1985, 1986 back issues)  
**2600 BACK ISSUES**  
 1984  1985  1986  1987  1988  
 1989  1990  1991  1992

### OVERSEAS: ADD \$5 PER YEAR OF BACK ISSUES)

(Individual back issues for 1993 to present are \$6.25 each. \$7.50 overseas - we don't have Priority Mail boxes to check out so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11959

TOTAL AMOUNT: