INDIAN PAYPHONES

(comeplete with goat)

PHOTOS BY SYNTHETIC MAN

AFRICA

CLOCKWISE FROM TOP: Voi, 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 WHERE WE HAVEN'T GONE!
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 CPSR Freedom of Information Act request concerning the breakup of the November 1992 Washington DC 2600 Meeting.

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Kingpin, Knight Lightning, Kevin Mittnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Tommy The Cat, Mr. Upsetter, Dr. Williams, and one who waits.

Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Shout Outs: 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 Phreak 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 Optik 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 Optik was one of the first hackers to shed this mask and come forward with information. His tutorials 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 WBAI’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 (echonyc.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 see 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 Optik 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 Neidorf, 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 Berman 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 truths, 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 Stira
32095-054
LEC Camp #1
P.O. Box 2000
Lewisburg, PA 17837

Please remember that all incoming mail is read by prison authorities.
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 ahold 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. Z80, 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 EEPROM (Electronically-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 repertory memory** (INIT 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)
- **Horn Alert On/Off** (HAL CLR)
- **Online Diagnostics** (ONL CLR)
- **System ID Enable/Disable** (MAN)
- **Mobile Identification Number** (MIN)
- **Service Providers ID** (SIDH)
- **Initial Paging Channel** (IPCH)
- **Extended Address On/Off** (EX SET)
Security for changing the ESN is also incorporated into most of today's phones. Due to increasing problems with call-sell 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 EEPROM and the NOVRAM, preventing any more access to the ESN from the keypad. It is possible to rid the flag in the EEPROM, 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 EEPROM 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 EEPROM, 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 receive 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 cell 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
- AT&T: 800-232-5179 (Cellular Services)
- Dallas: (408) 980-0414
- Intel: 800-628-8686
- Motorola: 800-331-6456 (Repair)
- NEC: 800-338-9549
- NEC: 800-632-3531 (Technical Department)
- Novatel: 800-231-5100
- Novatel: 800-766-8283 (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)
- Novatel: 800-447-0332 (Cellular Technical Support)
- VLSI: 800-473-8574
- VLSI: (408) 434-7227

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
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 telco 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 unlit, 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 unlit, 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 350Hz and one 440Hz, 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 (except ten times for 0). If the number dialed was 4, as the disk rewound, 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-rotary phones, capable of pulse dialing, interrupt the current similarly, using an electronic control circuit.

A very nimble finger can accomplish the same thing with the hang-up button. More modern phones emit a concurrent 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 (*, 0, and #) 941Hz. Each button in the first column (1, 4, 7, and *) emits 1209Hz; second column, 1336Hz; and third column (3, 6, 9, and #) 1477Hz. These tone pairs are interpreted by the switching facility as the number pressed on the dial pad. Although ancient switches cannot interpret tones, new (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 bleep 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, bleeping 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 bleeps 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 inciting 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 signalling 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 short burst of digital data, encrypted 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.
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 size of a large office phone, having the hook and handset off to the side. The main unit consists only 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 small 16 bit microprocessor and only about 128K of RAM. Upon startup, the phone reads the operating system from ROM, and then loads your phonebook from battery backed RAM, similar to the way a Sharp Wizard works.

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 similar "smart" 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 RBOC 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 dials 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 Pac-net for the New York metro area: These numbers are the ones I know, but there are certainly others that you can find.

<table>
<thead>
<tr>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>212-385-2551</td>
</tr>
<tr>
<td>718-875-6504</td>
</tr>
<tr>
<td>914-723-2666</td>
</tr>
<tr>
<td>914-425-0202</td>
</tr>
<tr>
<td>516-599-2525</td>
</tr>
<tr>
<td>516-665-7878</td>
</tr>
</tbody>
</table>

In all cases, once connected, type HH 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."
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 some 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 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.

Comptroller
October 2, 1992

Mr. [Name]

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 breech would involve. Thereafter, 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 requirement 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 G Hemby 703
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 infect 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 "Invalid 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 blackens 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 Shutdown.p in THINK Pascal), and put it in the startup folder. Thus, the computer turns off as soon as it loads up. (To get around this after the joke'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 warez - I mean wares - or do I?

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 theft 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 difficult 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 sale-creatures would sell their grandmothers for a good writeup in the Wall Street Journal. The WSJ badge would be magic.

Dress the part — printing 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 Acorn 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, Microfluff Paragraph, and a few others. I was very impressed with the new release of PhallusWriter 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
PhallusWriter 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 anything 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 booths. 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.
**nynex voice mail**

Following is a list of telephone exchanges, the type of switch they're on, the CLL 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. Exchanges that don't have this service are not included.

We regret that there are a couple of gaps in this list but be advised that certain people risked their lives to get them.

Thanks to KELCO

MANHATTAN (212)

<table>
<thead>
<tr>
<th>Exchange Code</th>
<th>Address</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>206 #1A</td>
<td>W. 18th St.</td>
<td>929-8070</td>
</tr>
<tr>
<td>207 #1A</td>
<td>E. 56th St.</td>
<td>355-1088</td>
</tr>
<tr>
<td>210 #5B</td>
<td>E. 37th St.</td>
<td>682-2022</td>
</tr>
<tr>
<td>215 #1A</td>
<td>E. 30th St.</td>
<td>693-0085</td>
</tr>
<tr>
<td>216 DMS</td>
<td>W. 36th St.</td>
<td>630-2580</td>
</tr>
<tr>
<td>219 #1A</td>
<td>Varick St.</td>
<td>334-9280</td>
</tr>
<tr>
<td>221 DMS</td>
<td>W. 42nd St.</td>
<td>575-7500</td>
</tr>
<tr>
<td>222 #1A</td>
<td>Manhattan Ave.</td>
<td>662-9554</td>
</tr>
<tr>
<td>223 #1A</td>
<td>E. 56th St.</td>
<td>750-5277</td>
</tr>
<tr>
<td>225 DMS</td>
<td>Varick St.</td>
<td>334-9280</td>
</tr>
<tr>
<td>229 DMS</td>
<td>E. 97th St.</td>
<td>369-6608</td>
</tr>
<tr>
<td>242 #1A</td>
<td>W. 18th St.</td>
<td>929-8070</td>
</tr>
<tr>
<td>243 #1A</td>
<td>W. 18th St.</td>
<td>929-8070</td>
</tr>
<tr>
<td>245 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>246 #1A</td>
<td>W. 50th St.</td>
<td>262-0940</td>
</tr>
<tr>
<td>247 DMS</td>
<td>W. 50th St.</td>
<td>767-8030</td>
</tr>
<tr>
<td>249 DMS</td>
<td>E. 79th St.</td>
<td>452-0166</td>
</tr>
<tr>
<td>251 DMS</td>
<td>E. 30th St.</td>
<td>447-2800</td>
</tr>
<tr>
<td>252 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>255 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>256 DMS</td>
<td>E. 18th St.</td>
<td>307-7330</td>
</tr>
<tr>
<td>261 DMS</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>262 DMS</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>263 DMS</td>
<td>E. 30th St.</td>
<td>447-2800</td>
</tr>
<tr>
<td>265 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>266 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>270 DMS</td>
<td>E. 37th St.</td>
<td>692-2022</td>
</tr>
<tr>
<td>272 DMS</td>
<td>E. 37th St.</td>
<td>476-5300</td>
</tr>
<tr>
<td>274 #5E</td>
<td>Varick St.</td>
<td>274-8180</td>
</tr>
<tr>
<td>278 DMS</td>
<td>E. 36th St.</td>
<td>630-2580</td>
</tr>
<tr>
<td>280 #1A</td>
<td>Manhattan Ave.</td>
<td>662-9554</td>
</tr>
<tr>
<td>281 DMS</td>
<td>Convent Ave.</td>
<td>234-3122</td>
</tr>
<tr>
<td>283 DMS</td>
<td>Convent Ave.</td>
<td>234-3122</td>
</tr>
<tr>
<td>284 DMS</td>
<td>E. 17th St.</td>
<td>345-1490</td>
</tr>
<tr>
<td>289 #1A</td>
<td>E. 26th St.</td>
<td>860-2680</td>
</tr>
<tr>
<td>296 #5E</td>
<td>W. 18th St.</td>
<td>736-0344</td>
</tr>
<tr>
<td>297 DMS</td>
<td>E. 37th St.</td>
<td>476-5300</td>
</tr>
<tr>
<td>298 #1A</td>
<td>E. 79th St.</td>
<td>736-0344</td>
</tr>
<tr>
<td>317 #1A</td>
<td>E. 56th St.</td>
<td>737-0335</td>
</tr>
<tr>
<td>318 #1A</td>
<td>E. 37th St.</td>
<td>734-5344</td>
</tr>
<tr>
<td>319 #1A</td>
<td>E. 37th St.</td>
<td>736-0344</td>
</tr>
<tr>
<td>320 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>322 #5B</td>
<td>W. 50th St.</td>
<td>562-2040</td>
</tr>
<tr>
<td>324 DMS</td>
<td>E. 30th St.</td>
<td>630-2580</td>
</tr>
<tr>
<td>325 DMS</td>
<td>E. 30th St.</td>
<td>527-1300</td>
</tr>
<tr>
<td>326 #5B</td>
<td>E. 30th St.</td>
<td>527-1300</td>
</tr>
<tr>
<td>328 DMS</td>
<td>E. 30th St.</td>
<td>947-2869</td>
</tr>
<tr>
<td>331 #1A</td>
<td>E. 30th St.</td>
<td>683-0085</td>
</tr>
<tr>
<td>332 #1A</td>
<td>E. 30th St.</td>
<td>683-0085</td>
</tr>
<tr>
<td>333 DMS</td>
<td>E. 30th St.</td>
<td>447-2800</td>
</tr>
<tr>
<td>334 DMS</td>
<td>E. 18th St.</td>
<td>463-0041</td>
</tr>
</tbody>
</table>

Page 18  2600 Magazine  Winter 1993-94
ANNOUINCING
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 FyberLyte

Intro

The tone box is my latest mad invention. This device will satisfy your phreaking 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 lo-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.

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 A544 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

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, noticing 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 fry 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 slithers down the pins into the clips. 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 black 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 blast, 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.
LETTERS TO REMEMBER

Fun Telco Numbers

Dear 2600:

I am writing in regards to Mouse Balls’ request for the ANAC for 310/818. Well, there are two that I’ve found: on Pacific Bell phones you use 211-2345, and the 114 that you published works only on GTE phones. I also found that on GTE payphones, oftentimes pressing 111 will get you a complete test for payphones. It is “menu-driven” and is surprisingly “user-friendly.” I have tried these three numbers in 818 and parts of 213 with 100 percent success on 211-2345 and 114 but only about 50 percent success with 111.

Beetle Bailey
Arcadia, CA

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 “dumb” lights, with no pressure plates or flow sensitivity at all.

This announcement got me thinking. Anyone out there have any experience in hacking traffic light controllers? I find myself extremely curious about how these damned things work. Especially the “intelligent” ones.

Lone 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 supposedly to allow ambulances to get through intersections more easily. We’ve heard rumors of rapidly flashing headlights having the same 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 insult our readers’ intelligence by saying it.

Past Hacker Prime?

Dear 2600:

Ever since I’ve had a conscious knowledge of computers, I’ve wanted to hack. I haven’t always known it was called hacking, but I’ve just had the mental inklings akin 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 enter my junior year of high school and I feel that I’m almost past my prime for hacking (this may just be a popular misconception). But, regardless of my age or scholastic ranking, I feel I should start now. So I was wondering if you could steer 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 friends’ 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 past your 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 H/P 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 that contain information about voice mail, COCOTs, telco payphones, and H/P 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 COCOTs 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 COCOT. Here is something fellow readers might want to try: dial a number direct from a COCOT and insert the correct coinage, then if this particular COCOT 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 COCOT does not use an extender, just hack it from there. If you are not sure, find out by listening carefully to the COCOT 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 H/P community.

An interesting number is (206) 626-0830. It's some service called Free Phone. Also, there was an interesting number at (201) 644-2300 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 is a fake. Now just in case you wanted to know what was so special about this line, it was some sort of text to speech converter that would transfer you to various extensions. There were some interesting extensions like touch tone shell, Bellcore directory, and others.

**Whistler**

The ANAC for at least part of New Jersey is now the same as New York: 958. In many digital switches, 511 also works. Silver boxes are nothing more than modified touch tone pads that can produce an extra row of tones (A,B,C,D). Other than telco tests and internal military applications, there don't seem to be many uses for these extra tones, at least not yet. The topic you're interested in are covered in some form in nearly all of our issues. One day soon we hope to have a comprehensive index. Hacker directories have been tried before but they're usually filled with inaccuracies and taken as gospel by law enforcement.

**Dear 2600:**

This letter is concerning the article written about the cable descrambler. Upon looking for a 75-100pf variable cap., I noticed that there was no one around that carried that large 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 so that their totals would add up to be within the 75-100 range. Example: using three 32pf 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 are 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 MCI phones around here that mute the mouthpiece. Even when you call up someone else, it re-mutes it again. I cannot use my "quarter" on it. Luckily there are Pac Bell phones it does work on, but I was wondering if anyone knew of a method to get the MCI phone mouthpieces to unmute. Thanks.

**Will Chung**

San Luis Obispo

**Dear 2600:**

A letter in your Spring 1993 issue asked 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 radios, phones, 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 needs one of the keypads with the ABCD. If interested, can we swap a subscription for a keypad?

**Pipo Communications**

P.O. Box 2020

Pollock Pines, CA 95726

(916) 644-5444

Send a keypad and we'll send you a subscription.

**Potential Discovery**

**Dear 2600:**

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

**Maldoror**

Florida

It's quite likely that some cheaply made COCOTs simply listen for the intercept tones and assume that there was no connection made if they appear. What a wonderful thing.

**Security Concerns**

**Dear 2600:**

A friend of mine was recently considering a 2600
subscription. “Of course,” he said, “it’d probably put me right onto the Fed List.”

This brought to mind a few interesting questions. What measures 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?

**Dear 2600:**

I have been considering subscribing to your zine, 2600, but I have second doubts. I am not resisting to subscribe because of the price, but I have heard a rumor that when/if someone subscribes, they are put on a fed list. I really don’t want to have the finger pointed on me if there is some hack around my area. If they really do get a list of subscribers, then the chances 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/with the Feds, and subscribers are put on a list, or someone is able to GET a list of subscribers fairly easy?

**Bleed 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 first 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 Citicorp meeting I was able to resolve my problems by working with some very helpful fellows. I would especially like to thank the “Phoenix” for supplying the 6.50 rock as well as his expert technical advice. Seemed like a nice bunch and quite a mellow time was had by all (I thought War World 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 further educate myself in this delightfully sneaky hobby. Thanks much. (I can’t make the next meeting as I got sent away to a re-hab.)

**Johnny “The Quarter” Burpo**

Rubber Room Restinghouse

Upstate, 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 blue boxes still work? Is there any safe way to use them? If not, how can you explore the phone system’s hidden numbers as you once could with a blue box?


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 II Evangelist. 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 trips.

5) What should I do to protect myself from searches and seizures at 2600 meetings? Why did people actually give mall security correct information at the November meeting in Washington?

**M**

Great Neck, NY

Blue box tones still do things so in certain places, a blue box would still work. Within the United States, it’s pretty rare however. A crossbar switch is a huge room-sized monster filled with clicking 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 Bootleg in the Spring issue mentions a cellular service manual marketed through Motorola, item #68-093-00a60. I have tried to acquire this manual through my sources at Motorola Canada, and have been told flat out that it can’t be had. Can 2600 or whoever give me a hand in its acquisition?

**DY**

Weston, ONT

The word is out.

**Dear 2600:**

In the USA (in Boston I think) there’s an anti-car theft tracking device called “lojack”. Stolen cars transmit a signal to suitably 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 (purely for educational uses). This, of course, excludes finding the damn thing and ripping it out so the cops end up arresting a waste paper bin on a street corner.

Can you or any of your readers help? Owen Halifax, UK

Why Hack Cable?

Dear 2600:

Your little magazine blew me away. I used to get the old TAP 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 descrambler is basically just a bandpass or band stop filter that might kill one kind of scrambling, where a "jamming" signal is mixed with the video and your box notches it out. But from the description 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 Sheets book on video scrambling is probably the most direct source. Your local 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 too much time watching this dogshit. I had free unlimited cable for five years and finally had to physically uproot the cable so as to "dry out".

I intend to keep reading your superior parrot cage liner 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-heads: Are any of the old NSA cypher machines (boxes with model numbers like KG- or KY- something) now in the public domain and out there with hackers or hamfesters? I'm given to understand these things were just beautifully built, but then again so are the toys Pantex makes.

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 accessories. Tell whoever is working there you are doing a project (for school) on the phone company (b.s. your way through this explanation as necessary), and that you wanted to see just how things work. Act real innocent (and dress nice) and the people there should give you a tour. In my 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 great info off of papers on the walls and general bulletins. You can get phone company internal numbers and other useful information. At our New England Telephonic office, there were a few terminals with external AT&T dataport modems. So visit your local CO today!

How to Learn About Your CO

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 COCOTs" article, I've found great use of the "combo-box". By eliminating the pretty much worthless beeper 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 mercury switches to activate the crystals, internal (eliminating the beeper 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 ACD" by Kingpin in the same issue, the extra space was needed so that I could use Radio Shack mercury switches PN 275-040 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 *'s in the Pl location, it's best to store five *'s and a pause. This way you can hit the Pl 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 kicked in 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 monitored 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 COCOTs I've run across here in California are newer models and the "dial 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 (Tin Shack) claiming to offer free elite access to all 2600 readers. Is this guy joking or something? I called the thing and he's got five lines...
call forwarded to a single line, real names only. BBS system (disguised to look like a multi-line system), which won’t give you access until you’ve been “call-back verified”. He even has a list upon logon of the “most downloaded files”, which all just happen to be hacker/phreaker 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 “wannabe’s, phonies, or pheds”, but I can’t think of anything a phreaker or hacker would want to do more than give some pseudo BBS his real name and home phone number. Gee, either a very paranoid syndop (in which case he shouldn’t advertise his BBS in a hacker magazine to begin with), or something fishy is going on in Canoga Park!

**The Lung**

Sunny Southern California

It is possible to activate the ACTS computer on local calls by coming in on a long distance carrier using a carrier access code. That’s one way a red 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 affiliated 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 Mate I and Modem Mate II. “Modem Mate I secures your modem by foiling the hacker. By attaching Modem Mate I to your existing modem, you make your computer system virtually undetectable. When a hacker attempts to call your modem, Modem Mate 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 Mate II only allows predefined calls using Caller ID.

Julian

Cleveland

Would we love to hear that “realistic sounding hello”.

**Modem 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 Digicom 9600 Scout modem and possibly any other Digicom 9600 model.

I bought my modem for $150, a good deal for a 9600 internal modem. Digicom sells a 14.4 modem called the Scout Plus for around $220. They will let you upgrade the Scout to the Scout Plus for $50. 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*Z1/AT*Z0. 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 1600. That’s one hell of an improvement for nothing.

Antoch

**Foreign Pay Phone Flash**

Dear 2600:

In the Autumn 1993 issue of 2600 you asked “does Bhutan have payphones?”

Buried deep in my Bhutan photo files there is a photo of the public payphone booth in the main plaza in downtown Thimphu, Bhutan’s capital city. Unfortunately, I don’t have enough time to search through unsorted negatives to find a picture for you.

I can tell you, however, that these public payphone booths are all attendant operated by private entrepreneurs - 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.

Bhutan’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 replaces the wireless communications system that is still used in parts of the country where the new network hasn’t yet reached. There is no reason to think that coin operated phones won’t be appearing on Bhutanese streets in the future, but as of November 1992, there were none.

LN

APO AE

Your letter is living 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 toll fraud in pay phones, I began to think about using the Macintosh’s exceptional sound qualities to produce the required quarter tones. Unfortunately, the Mac I have is too slow to produce the sounds up to speed. I do have a solution for all of the people who don’t have the expertise to build the Quarter described. It involves finding a payphone with no one around it (no one!), and with the wire going into the payphone exposed (not in a pvc or metal conduit). Get 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 mouthpiece 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  
Manchaca, TX

**Technology Moves**

**Backwards**

Dear 2600:  
I am writing to you in your capacity as the great unmasker of AT&T’s true motives. When the Public Phone 2000’s came out, they were the first visible sign of AT&T’s rhetoric about being the deliverer of the telecom revolution, global information convergence, etc. 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 (modem, 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 sprinkling public thoroughfares with avenues for anonymous login and mischief must have suddenly seemed like a risky proposition. Do you know if there were any specific incidents that called this to the telemarketers’ attention? Was there any explanation proffered?

Martin

This is the first we’ve heard of it but 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 File” article. I have provided the correct numbers: Trans Union (313) 689-3888 and TRW (214) 390-9191.

Jeff

Bless you.

Dear 2600:

While cruising around text files in the ftp sites on the Internet, I found some information on the logical counterpart to the red box: the green box, which will supposedly return someone’s money once they’ve used a pay phone to call you. The tones are: 2600 Hz for 90 ms, silence for 60 ms, 2600 Hz for 900 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 hacking and phreaking is for a beginner to figure things out on his own by trying them, I also know that one shouldn’t go shooting 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. But there’s nothing wrong with finding out whether or not it works, at least not in 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 modded 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 call goes through on an operator-free, automated system (e.g. AT&T Long Distance), what difference does it make? Does the extra precision of the “real red box” lessen your chances of being detected, and somehow immediately detained at the payphone? I will consent 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 modded dialer, makes any difference. Please explain.

Anon.

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 prompted me to become a subscriber). Your publication has brought me many happy hours. Keep up the excellent work!

What concerned me though, was Billsf’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 (505) area that insist to me that it’s perfectly safe as long as you don’t try using it with telco personnel online. When I told them about 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?

Nexus

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 redboxes, it mentioned that red boxing was very dangerous. What is this shit? 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
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 neo-Nazi sysadmin (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 tea-time conversation topics. Anything that might pertain to socially deviant behavior (hacking, learning something not government regulated, etc.) has been deleted. In fact this morning over 1000 newsgroups have been screened out from our system. Is there any way for a person to get around sysadmin control 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 trust his own computer science students.

Any help would be greatly appreciated.

Concerned

As explained in a letter in our Winter 1991-92 issue, that particular modification will always produce tones of 1721.0 Hz and 2208.1 Hz and the timing will always be 54.62 mS on and off. The concern is that theoretically it would not be difficult for those unique traits to be looked for by the phone companies. We’re unaware of this ever actually 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 wannabe logged in to the network as sysop with a valid password when, lo and behold, 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
Bethesda, MD

Dear 2600:

I just read the review of NTPASS 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 Phrack #40) which will create a temporary SUPERVISOR equivalent account with a name that you specify.

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

The advantages to this are obvious over NTPASS... 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!

Erreth Akbe

A Way Around Caller ID?

Dear 2600:

Your story is not unique, unfortunately. Oftentimes, people in charge feel the need to restrict or cut off access. Apart from making sure we never turn into 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 telnet out to another site that isn’t as restrictive. Perhaps you could trade accounts with a student at another school or subscribe to a cheap public UNIX system. With the Internet in its present form, anything is possible.

Lost and regulated in
NB, Canada

Your story is not unique, unfortunately. Oftentimes, people in charge feel the need to restrict or cut off access. Apart from making sure we never turn into 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 telnet out to another site that isn’t as restrictive. Perhaps you could trade accounts with a student at another school or subscribe to a cheap public UNIX system. With the Internet in its present form, anything is 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 ring through to the called party, prompting their CID unit to answer, provided CID uses a normal modem hookup. 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 autodialer 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 telco. This would allow a quick and easy way around Caller ID, especially if *67 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 right switch yet.)

Levendis

Sorry. It doesn’t work. The Caller ID box is in 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 special 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 dorms you dial 3-xxxx, and offices can be had by dialing 4-xxxx and 5-xxxx.

What’s interesting is that this town also has other phone exchanges, such as 257 and 256. However, to dial these exchanges you need to hit “9” first, and then dial the full number. To dial toll free numbers, you hit “7” and then the full number - “9” also works for this.

I’m fairly sure the school has its own switching 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.

lexis
cyberspace

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 acts differently. Your room phone has a different class of service as a public hall phone so the restriction level is not the same. No doubt there are other restriction 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.

BG
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 asked to (and took) one of the very honesty tests you described in your latest issue.

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 “test” 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 choosing the lowest denomination on the question referring to the approximate value of all monies or properties taken from a non-job location.) On a better note, the job wasn’t all that important to begin with, and it fazes me not that an honesty test might have lost me a job with this company. Incidentally, the manager of the arcade “Tilt”, 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 out pops one’s rating as an honest individual. There was also a free-form written part of the test where the testmakers asked if there were any inconsistencies and/or confusing questions on the test that we would like to comment on. Needless to say, I wrote them an essay....

The Vampire Gabrielle
<table>
<thead>
<tr>
<th>Location</th>
<th>Phone Numbers</th>
</tr>
</thead>
</table>
| Eindhoven University, Netherlands | +31 40 430032 300-9600  
+31 40 435049 300-2400  
+31 40 455215 2400 | 219-980-6866 300-2400  
Purdue University, IN | 219-989-2900 VAX |
| University of Manitoba         | 204-275-6100 2400 or less  
204-275-6132 9600 & 14.4 | University of Maryland, College Park, MD |
| University of Washington       | 206-685-7724 2400  
206-685-7796 9600 and above | 301-403-4444 v.32 bis  
Illinois State University |
| Columbia University, New York, NY | 212-854-1812 1200-2400  
212-854-1824 1200-2400  
309-438-8200 9600 N81 - LANACS |
| New York University            | 212-995-3600 2400 and lower  
212-995-4343 2400 and up | Depaul University, IL |
| Southern Methodist University, TX | 214-368-1721  
214-368-3131 | 312-362-1061 9600 E71  
Cisco Terminal Servers, Chicago |
| University of Pennsylvania     | 215-898-0834 9600+  
215-898-4781 1200  
215-898-6184 2400 | 312-413-3200 7 bits mark parity  
312-413-3212 8 bits no parity |
| University of Central Florida  | 407-823-2020 | Ball State University, IN |
| University of Maryland, Baltimore, MD | 410-333-7447 v.32 bis  
410-788-7854 2400 | 317-285-1000  
317-285-1108  
Kokomo, IN |
| Purdue University, IN          | 317-494-6106 | Indiana University East |
| University of Pennsylvania, Oakland | 412-621-2582 300-2400  
412-621-5954 300-2400 | 317-973-8265 300-1200 |
| University of Pennsylvania, Greensburg | 412-836-7123 300-2400 | 407-823-2020 |
Southeast, IN
812-944-8725 300-2400
812-944-9820 300-2400
812-945-6114 300-1200
University of Pennsylvania, Johnstown
814-269-7950 300-2400
814-269-7970 300-2400
University of Pennsylvania, Bradford
814-362-7558 300-2400
814-362-7597 300-2400
University of Pennsylvania, Titusville
814-827-4486 300-2400
Sherbrooke University, QUE
819-569-9041 2400
819-821-8025 Zyxell
Bishop University, QUE
819-822-9723 2400
Michigan Tech
906-487-1530
Pomona/Pitzer College, CA
909-621-8455
Sacramento State, CA
916-456-1441
Wake Forest University, NC
919-759-5814

HACKERS FOR "BOB"
"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 peaceably 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. What does this mean to us dedicated 2600ers?

When you are attending a 2600 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 these points: You chose this area because of a) its successful reputation, b) its great location, c) the fine merchants, 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 them of your research into the local laws and ordinances of.

Winter 1993-94  2600 Magazine  Page 35
trespassing. 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 so! 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 meet 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 them 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 arrests 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 basis 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.
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)
Review 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. Which, I suppose, does pretty well describe what happens on the latest frontier in computer technology. About a month ago, I had the opportunity to observe virtual reality in action at a display at the Calgary Stampede. There were three enclosed cockpits with the participants wearing headsets that cut them off from their surroundings. TV monitors depicted the scenes transmitted into the headsets that cut them off from their surroundings. TV monitors depicted the scenes transmitted into the headsets, which in this instance involved a game with a lot of stairways. One participant became so enthralled in attempting to zap his opponent that he totally forgot there was an audience “outside” and his language left a lot to be desired. Such is the power of this ultra-futuristic technology.

We are still a long way from the real-time graphics of the holodeck depicted on TV’s Star Trek: The Next Generation, but at the present rate, it won’t be long before we see extraordinary developments. After all, 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 this 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 dawn of the new era back to the Cinerama/Cinemascope/3D movies of the 1950’s. A man named Morton Helig actually made plans for an “Experience Theatre” back in 1955, and patented a head-mounted stereophonic television display in 1960. Helig is still alive, in his sixties, 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 Neuromancer), which is now used widely to describe the internal 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 where you could touch the screen to choose an option. This in turn led to glove-mounted sensors. The author was one of the first to try a NASA prototype in 1988 that demonstrated the amazing potential capabilities of the system - the major 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 chemical research, and even simulated sex! There are currently moves underway to bring the dimension of tactile sensation to the simulations, 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 perceptions 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 time there instead of in the so-called “normal” reality? Addiction in other words. Then there is the weapons potential - it has always been easier to kill people if you are distanced from them by machines, as any bomber pilot from World War II will tell you. A dictator could zap rebels with a laser-mounted cannon combined with a virtual/robotic system, without ever leaving the comfort of his presidential palace many miles away. However, we must not fall into the trap of arbitrarily rejecting new technology just because of the possibility of misuse. There is a huge potential for paralyzed 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. Huxley’s Brave New World 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 stunning insight into just how far along the road to a science fiction reality we are. Ironically, it uses the very earliest virtual reality device to do so - i.e., the printed word. Well, everyone has used reading at one time or another to turn off the annoyances of the “outside”. The difference 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!
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 hacked 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.

01234 012XY 01459 0169Z
01235 012XZ 0145X 015XY
01236 012YZ 0145Y 015XZ
01237 01345 0145Z 015YZ
01238 01346 01467 01678
01239 01347 01468 01679
0123X 01348 01469 0167X
0123Y 01349 0146X 0167Y
0123Z 0134X 0146Y 0167Z
01245 0134Y 0146Z 01689
01246 0134Z 01478 0168X
01247 01356 01479 0168Y
01248 01357 0147X 0168Z
01249 01358 0147Y 0169X
0124X 01359 0147Z 0169Y
0124Y 01365 01489 0169Z
0124Z 01366 0148X 016XZ
01256 0136Z 0148Y 016XZ
01257 0136Y 0148Z 016YZ
01258 01368 0149X 01769
01259 01369 0149Y 0178X
0125X 0136X 0149Z 0178Y
0125Y 0136Y 014XY 0178Z
0125Z 0136Z 014XZ 0179X
01267 01378 014YZ 0179Y
01268 01379 01567 0179Z
01269 0137X 01568 017XY
0126X 0137Y 01569 017XZ
0126Y 0137Z 0156X 017YZ
0126Z 01389 0156Y 0189X
01278 0138X 0156Z 0189Y
01279 0138Y 01578 0189Z
0127X 0138Z 01579 018XY
0127Y 0139X 0157X 018XZ
0127Z 0139Y 0157Y 018YZ
01289 0139Z 0157Z 019XY
0128X 0139Y 01589 019XZ
0128Y 0139X 0158X 019YZ
0128Z 0139Z 0158Y 01XYZ
0129X 01456 0158Z 02345
0129Y 01457 0159X 02346
0129Z 01458 0159Y 02347

Digital locks:
Not as fun as Simplex.
INTERESTED IN ARTICLES and/or technical papers regarding United States phone system routing (Bellcore, AT&T Numbering Plan, etc.). Send mail to killjoy@mindvox.phantom.com. Will trade technical papers.

SNES AND GENESIS BACKUP UNITS, cartridge copiers for backup purposes. Call for more info: 917-462-5071.

LOOKING FOR (FREE) PHONE NUMBERS which use the CCITT (C5) protocol. Any Amiga user interested in blue box programs or other stuff? I also like to swap hack/phreak schematics or other info. Drop a line or disk (IBM, Amiga) at RETORT, Bommelweg 65A, 4014 PV Wadenoyn, The Netherlands.

"THE QUARTER" DEVICE. Complete kit of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $50. Send money order for 2nd day shipping; checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits (foreign add $12 per order, U.S. funds only) for shipping and insurance. Also available: 6.5536 MHz crystals in quantity: 10 for only $35 postpaid. Each additional crystal only $3 postpaid. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

HAVING TROUBLE FINDING THE INFORMATION YOU REALLY NEED? Information on starting and running a home business, blacksmithing, wood working, leatherworking, government surplus, cooking, glass blowing, arc and gas welding, metalworking, open fire cooking, fencing your credit card problems, writing press releases. Special books, unusual projects, hard to find information. Send $1 for a complete catalog - satisfaction guaranteed or your money refunded in full. Cybernetics Design, 88 East Main Street, Suite 457H, Mendham, N.J. 07945-1832.

METROPOLIS BBS. 718-276-0246. A BBS with a better attitude. No rules, no fees, no entrance exam, no elite access, no real names, and no real sysop. The best place to be for exciting discussions about the computer underground. No pirated software please, and no credit card numbers. We would like to remain bust-free. The First Amendment rules!

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

BOOKS AND PROGRAMS of "insiders" phone numbers to all banks, finance companies, retailers, etc.; how to get non-published phone numbers, bank account locates, etc. Call (813) 462-0008 for details. Also - current list of telco CNA numbers wanted.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 603 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-5098.

HACK/VIRUS/PHREAK/ANARCHY/CRACK IBM 3.5" 1.44M disks and books. New Fall 1993 catalog. Lower prices, more products. Send $1 for catalog to: SotMESC, PO Box 573, Long Beach, MS 39560.

THE BLACK BAG TRIVIA QUIZ. On 5.25 360k DOS disk (only). Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining, very educational, and FREE! Just send two 29 cent stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

SPANISH HACKER GROUP named IBERHACKER look for exchange off all types of information about computer insecurity (hacking, cracking, phreaking, computer viruses, etc.) and contact with all interested in computer security. We have thousands of pages with computer security-insecurity information. Contact: IBERHACKER - Peru, 6, 10 - 18600 Motril - Granada - Spain.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KK Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM, and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 2/1/94.
Foulups 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 fire 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 functions take as long as 30 seconds to complete and an unexplained instance of garbage being sent throughout the network. According to County Executive Assistant John Gallagher, “It began to act strangely and started putting information into the records machine that was totally unrelated to the information called in.” All in all, the system has failed nine tests. The county executive has reportedly lost faith and has referred to it as “unstable and unreliable”. The system uses A-16 mainframe computers.

Touch Tone Registration

Colleges across the country are using a new method of registering students: touch tone phones! We checked out two similar systems operating at each. At Suffolk Community College, students simply dial (516) 696-4910. The only information required by the system is the student’s Social Security number! Armed with this information, anyone can change the poor student’s schedule, adding or dropping courses to their heart’s delight. Of course, you also need a copy of the current academic schedule in order to obtain the proper four digit section 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). It brings new meaning to the words “learning institutions”. Right now, they’re learning pretty slow. Oh yes, the number for that system is (516) 632-9393.

Electronic Mayhem

Earlier this year, motorists were startled 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 claims 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 line 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 ridiculously simple,” he said. “The menu 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 newspaper and the University Health Insurance Office but declined to give his name, fearing disciplinary action. He said he wanted people to know that “technology is a really powerful tool.”

The Latest From The U.K.

According to British Telecom, attacks by “organized and well-equipped criminals” on BT’s 110,000 payphones rose from about 1,000 a month in September 1991 to around 6,500 by January 1993. But, thanks to a “determined campaign”, the number of attacks has since been cut by around 50 percent. Part of this campaign includes payphones that speak, saying “Warning - tamper alarm; police have been informed.” Warbling alarm tones are also being used. They really go all out on these studies, by the way. They have graphs, charts, press 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 attacks and the number of payphones in working order.” Gosh.
In Perth, Scotland, the first tests 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 coercive style as it is in the States. BT claims that 90 percent of its customers enthusiastically 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 .01 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 C7 signalling process.

In more British news, the countdown to Phoneday has begun. On April 16, 1995, the biggest change to 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 will be dialed after the initial 0 of city codes. The extra digit is 1. So London, which only a couple of years ago was 01 and is now 071 or 081, will soon be 0171 or 0181. The toll-free code of 0800, the mobile codes of 0860 and 0850, and the information and entertainment services code of 0891 will remain unchanged. The general idea is for codes beginning with 01 and eventually 02 to be geographical in nature, 03 to be more mobile numbers, 07 to be for "lifeline" numbers (the same idea as AT&T's EasyReach service), and 08 to be for specially tariffed premium services. 04, 05, 06, and 09 are not going to be used right away. Five cities (Leeds, Sheffield, Nottingham, Leicester, and Bristol) will get brand new city codes. Their current codes are 0532, 0742, 0602, 0533, 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. These are traumatic times.

Collect Your Wits

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 0+ with AT&T was $2.20 for the first minute and 26 cents per minute thereafter. By using AT&T's 1-800-OPERATOR service, the rate was $1.73 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 neat way of saying customer service. Anyway, their rate for a 0+ call to the same number was either $3.76 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 $1.73 for the first minute and 24 cents for each additional minute, identical to 1-800-OPERATOR. Things started to get complicated when we asked about intrastate calls. We tried to price a call to the governor's mansion in Albany, NY. AT&T's 0+ 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 0+ 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 daytime call! We knew 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, then 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. Phone trauma in the United States, unlike Great Britain, doesn't center 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 retrieve messages from anywhere in the world, all you have to do is dial (407) 827-1888 (only the last five digits are necessary from within the hotel), then enter your room number and your secret password. You can easily remember your secret
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!
Now that prepaid phone cards are starting to appear in the United States, crazed collectors are hopping up in hot pursuit. Phone companies are encouraging this behavior by producing colorful and unique telephone cards, sometimes centered around special events, like the Democratic Convention in New York City in 1992. On September 25th, Richmond, Virginia hosted the first International Credit Card Collectors’ Convention. Some see this euphoria for cards rivaling the current ecstasy that coin and stamp collectors constantly experience. You can drool over pictures of more than 400 telephone cards by getting the 1993 U.S. Telephone Catalog, available for $5 from Lin Overholt, P.O. Box 8481, Madeira Beach, FL 33738. You can also get information on a publication called International Telephone Cards by writing to 29/35 Manor Road, Colchester, Essex CO3 3LX, 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 stampede) AT&T will cover all fraudulent phone costs above $25,000. This, naturally, doesn’t include the sign-up fee. If AT&T fails to notify the customer of the fraud, the customer only has to pay $12,500. Sprint has a similar program, no doubt designed to provide the best service possible at 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, 711 is being allocated for deaf 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 offer still more pay services. The reasoning is that since many major companies block 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 various 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 most 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 “one 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 to AT&T’s Easyreach service, currently reachable on 0700 numbers, 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 BosniaHercegovina - 387. Don’t expect to get through on that last one for quite some time.

Journalistic Integrity
Our local daily paper, Newsday, prides itself on being technologically savvy. All too often, though, their attempts fall flat. For instance, a story this summer screamed “Hacker Heard Plan for Baghdad Attack”. In other words, somebody who can turn on a radio and listen to unencrypted phone calls is seen, in Newsday’s eyes, as a hacker. Also, according to Newsday, “a pen register is a metal 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 Radio Shack CPA-1000 came out ten years ago and could fit in the palm of your hand. We suspect the professional stuff 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
Bergen 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 call a special 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 Jude Del Preore, 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 somehow catch 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 (AND) allows a number unique to the customer and different from his/her phone number to show up on the called 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 on Cable and Wireless 800 numbers. It seems that Caller ID boxes are able to read data from Cable and Wireless long distance calls. In other words, if you have your own 800 number and it terminates on a phone line with Caller ID, you will be able to see phone numbers from around the country show up on your Caller ID box. It appears that ANI information from the calling party is being picked up by Cable and Wireless and translated 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 itemization at the end of the month. The current ability to do this right away through ANI is rather expensive and requires special equipment. With this new method, all that is needed is a Caller ID box. The bad part is that this 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 noticed certain numbers that pass Caller ID data to us would not pass 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 birthdate of a relative or friend, e.g., LISA105; 2) Take the first or last letters from each word of a phrase, e.g., IWADASN (It Was A Dark And Stormy Night) or EDESOEFT (we holD thesE truthS tO bE selF evidenT); 3) Remove all vowels from a common word or words, e.g., TPSCRT (ToP SeCReT); 4) Make it as 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 dumpster divers. Posters are being designed that say “Properly 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 newsletter, ‘2600 Magazine; the Hacker Quarterly,’ based in New York.” Our source goes on to advise us that “a good way to thwart dumpster divers is to either shred sensitive material or seal it in cartons and arrange to have the cartons picked up by the mail center, with instructions to destroy them.” Our corporate source that leaked this company document to us was, incidentally, a dumpster.

**Tidbits**

Here are some fun facts: in 1992, New Jersey Bell disconnected 376,240 accounts, up from 275,855 in 1988. Supposedly, this tells us something about the economy. The number of business accounts disconnected was only 17,291, down from 19,428 in 1991. New Jersey Bell handles three million residential accounts and 524,000 business accounts.

There’s an interesting service operating at (503) 520-2222 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 (ns.speedway.net), you can hook into various systems using telnet or rlogin 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 800-932-2000. AT&T claims that they’ve figured out a way to make callers sound closer and more natural than ever before. To us, it sounds like they’re just turning up the volume a bit. Either way, you can expect this service to spread to your area sometime soon.

AT&T has raised the rates of information yet again. Now it costs 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 which still 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 Pumpcon II (Philadelphia) promised that “any 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 his 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 first.
2600 MEETINGS

Ann Arbor, MI
Galleria on South University.

Austin
Northcross Mall, across the skating rink from the food court, next to Pipe World.

Baton Rouge, LA
In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, food court.

Boise, ID
Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 3, 4, 5.

Buffalo
Eastern Hills Mall (Clarence) by lockers 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

Fort Lauderdale
West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

Houston
Galleria Mall, 2nd story overlooking the skating rink.

Kansas City
Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Madison, WI
Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9814, 9916, 9923.

Memphis

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011, 8927; 212-308-8044, 8162.

Philadelphia

Pittsburgh
Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: 412-928-9926, 9927, 9934.

Poughkeepsie, NY
South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Raleigh, NC
Crabtree Valley Mall, food court.

Rochester, NY
Marketplace Mall food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

San Francisco

Seattle

Washington DC
Pentagon City Mall in the food court.

EUROPE
Granada, Spain
At Kiwi Pub in Pedro Antonio de Alarcon Street.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8 pm.

Munich, Germany

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.
You won't find it in clothing stores. (We did, but that's a long story.) The 2600 hacker t-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 $26. M, L, XL.

The Shirt

Actual footage of Dutch hackers penetrating 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 50 minutes. $10. VHS, NTSC format only.

The Video

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


$25 per year

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(Individual back issues for 1988 to present are $6.25 each, $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

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

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11765

TOTAL AMOUNT:
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.