Around
$1.00

CYBER'ZINE

Issue #6
Volume #2

Originally The Black Book, now even better.

The following article was reprinted from Business Week, July 13, 1992, page 134

Telephone companies are cracking down on long-distance telephone fraud. AT&T, MCI Communications, Inc., and US Sprint are among several corporations that have taken steps to monitor long-distance usage and have implemented systems that will cut off access to certain numbers when a suspicious pattern is noticed. The Christian Broadcasting Network lost $40,000 to a hacker who had broken into the phone system and used the system to make calls to Pakistan. (editor note: see Hacking Voice Mail Systems elsewhere in this issue. That's the method he used). Phone fraud losses are estimated to range from $500 million to $4 billion. AT&T utilizes a computer program that looks for unusual patterns. Sprint collects data about phones usage daily. MCI has focused on crime in New York, where the company estimates 70 percent of the fraud comes from. Hackers have recently turned to cellular phone networks and are infiltrating corporate voice mail systems

---

```
 DFS2002 18:06:16 TERMINAL CONNECTED TO IMS     AIMSPI17
 10/26/93 18:06:09                                                PAGE     1
 ORD C3352990815    DD 10-29-93 PTD          PCN 000    TYP FR TKT 060150 SEQ 3884
 ITEM NUM 0001  REVISION 0  PURPOSE CODE            SERV CATG            POTS
 MSG A676 ORDER/ITEM CANCELLED

I TN [redacted]
I OE     02-421-109  /SWITCH 414494/TRANS CD 0  /OE TYPE L/
      /DF GNBYWI11 F92/ 009L/ 06021
I F1 /CA 00000021/PR 0250/BP 0250/CI NONLOAD /WC 414494
      /TEA SAI 937 DOUSMAN ST ;PXJ;SAI/TPR 213202/WC 414494
      /DF GNBYWI11 F92/ 008R/ 06 07 2
      /RMTE BP 351-400 & 451-600 DD

I F2 /CA      937D/PR 0155/BP 0005/CI BISDN    /WC 414494
      /TEA F 109 ALLARD ;PDW;FC/TPR 213202/WC 414494
      /D1
      /RMTE 105A1,

I FA AUX GNBY  / 109  ALLARD AV
      /RT 2131 /RZ 13

B F1 /CA 00000021/PR 0250/BP 0250/CI NONLOAD /WC 414494
      /TEA SAI 937 DOUSMAN ST ;RXJ;SAI/TPR 213202/WC 414494
      /DF GNBYWI11 F92/ 008R/ 06 07 2
      /RMTE BP 351-400 & 451-600 DD

B F2 /CA      937D/PR 1434/BP 0009/CI BISDN    /WC 414494
      /TEA R 968 DOUSMAN ;CDW;RGT25/TPR 213202/WC 414494
      /D1
```

If you ever go dumpster diving at a CO, or office and find this kind of stuff all linked together, grab it. This is the switch-network documentation that we were talking about.

Opening newspaper machines

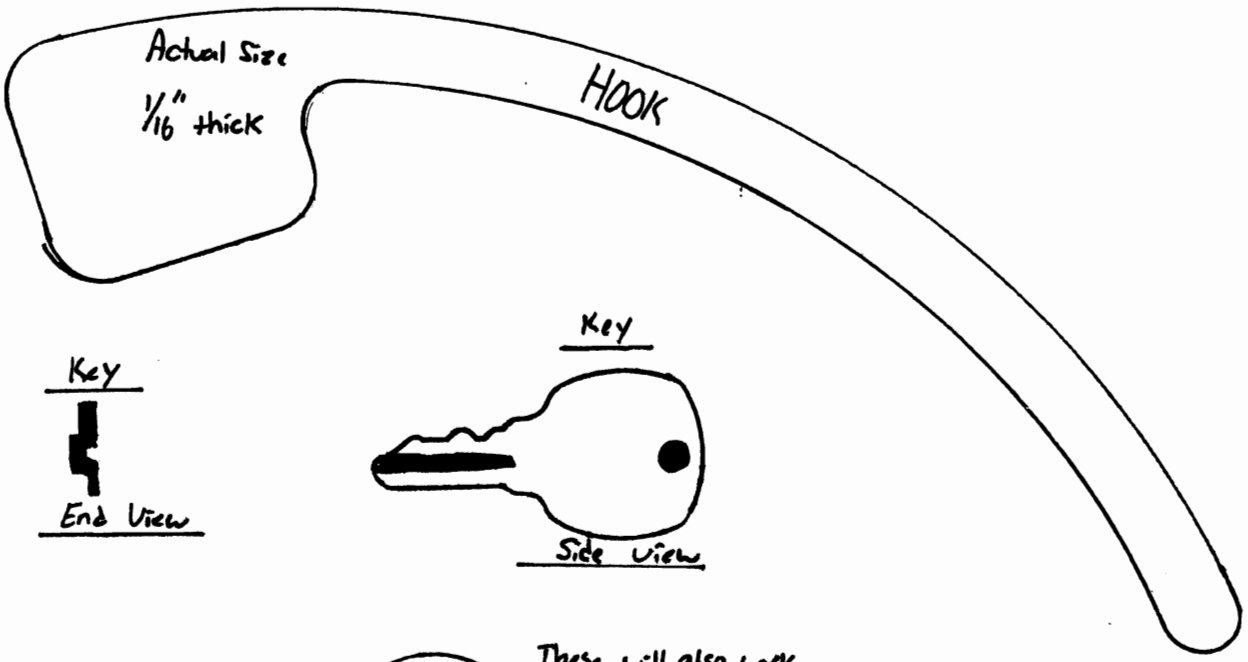
Everyone knows that in order to get more than one newspaper for the price of one, all you have to do is take more. But, in order to get the machine open, you had to deposit the amount of money a paper cost. Having to pay money really got to people. Here are so methods for opening paper machines. (NOT the part were money is, that involves freon, a hammer and the next issue)

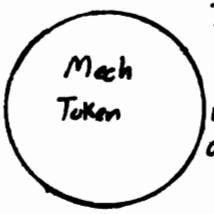
First you should know that most of the paper machines are made by Kasper wire in Texas. The model of machines are Sho-Racks. The best part of these machines is their parts are inter-changeable. This means the key used to open one machine will open the others. In Green Bay, the key that opens the Press-Monopoly machine, ALSO changes the price from $.35 to $1.50 on Sundays.

The locks on these are very easy to pick. They are only 3-pin tumblers with a relatively large shear line. On the Press-Monopoly machines, the lock on the lower left opens the machine. Just turn the cylinder, and at the same time pull on the handle. The other lock, located to the left of the handle, changes the price to a $1.50, or reverse. Just turn it to the S (if it's a weekday). That sets the price for Sunday papers. After you do that, hit the coin return button a few times to set the machine. Now you can sit back and watch people put money into the machine, and wonder why it's not opening.

The USA Today, and other two slot machines are a lot easier. All you have to do is make the object shown below. It will open all machines that have two slots (one for quarters, the other for dimes and nickels).

All you have to do is stick it down the quarter slot until it stops. You'll feel a metal bar. Push down on this with the hook, while at the same time pulling on the handle. The door should pop open. If it doesn't, just wiggle the hook around inside the machine while pulling on the handle. This will usually help.





These will also work.

They are magnetic so won't work in payphones, change machines or other devices that check for iron.

This is a reprint of an article that was in the spring '89 issue of 2600, the hackers quarterly. It is very interesting and was written by Eric Corley.

By now you have probably all heard about Kevin Mitnick. Mitnick, 25, is an overweight, bespectacled computer junkie known as a "dark side" hacker for his willingness to use a computer as a weapon. He allegedly used a computer to break into Defense Department computer systems, sabotage business computers, and electronically harass anyone -including a probation officer and FBI agents-who got in his way. He was arrested in late 1988, after being turned in by a friend who said Mitnick was "a menace to society."

Mitnick has an amazing history, to say the least. He and a friend logged into a North American Air Defense Command computer in Colorado Springs in 1979. The friend said they did not interfere with any defense operation. They just "got in. looked around, and got out."

Investigators believe that Mitnick also may have disseminated a false report, carried by a news service in April 1988, that Security Pacific National Bank lost $40 million. The report appears four days after Mitnick had been turned down for a job at Security Pacific. He also learned how to disrupt telephone company operations and disconnected the phones of celebrities such as Kristy McNichol.

In February 1988, Herbert Zinn Jr.., an 18 year old hacker broke into U.S. military and AT&T computers, was sentenced to nine months in federal prison. A dropout from Mather High School in Chicago, Zinn (a.k.a. Shadow Hawk) was sixteen at the time he committed the intrusions, using his home computer and a modem. Zinn penetrated a Bell Labs computer in Burlington, North Carolina, and another AT&T computer at Robbins Air Force base in Georgia. He copied fifty-five programs,including complex software relating to computer design and artificial intelligence. Although no classified material was involved, the government claims that the programs he copied from a NATO computer liked with the U.S. missile command are "highly sensitive."

During his trial in January '89, Zinn spoke in his own defense, saying that he copied the programs to educate himself and not to sell them or share them, Zinn is still in jail.

When people actually start going to jail for playing with computers, it's time to ask some very serious questions.

Let's start with Mitnick. Here we have what appears to be a nasty, vindictive human being. But is this reason enough to lock him up without bail? In normal times in almost any democratic society, the answer would be a resounding no. But there are special circumstances here: computers. Doing nasty things with computers is considered infinitely worse than doing nasty things without computers. As a result, Mitnick had less success seeking bail than he would if he had been charged with murder. Prison authorities wouldn't even let him use the phone for fear of what he might do.

Pretend for a moment that computers don't exist. Mitnick disconnects Kristy McNichol's phone using wire clippers. That's vandalism, maybe trespassing, good for a fine of maybe $100. He and a friend walk into the North American Air Defense Command Center one day. They don't break anything and they soon leave. Had they been caught, they would have been thrown off the grounds or, at worst, arrested for trespassing and held overnight. (The person who left the door open would be fired.)

In our society such a person would be classified as a mischief-maker. Such people exist everywhere. But because Mitnick used a computer to perform his mischief, he's treated as though he's another John Hinckley.

Society is indeed endangered by what's happening here, but that's not Mitnick's fault. He simply demonstrated how vulnerable our

Hacking Voice Mail Systems

Hacking voice mail systems is one of the strongest hacking areas in the underground community. These systems are becoming more popular everyday and their features are increasing.

For those that don't know what these are, they are answering machines that take messages for people in large corporations and businesses. They are usually controlled by computers that store the messages on hard drives instead of tape. Each voice mail system will hold around a thousand "voice mail boxes". The amount of boxes is usually determined by the amount of hard drive space available. You control these boxes through the Touch-Tones on your phone. After you call one up, keep trying different box numbers (they are usually three digits long) until you find one that works. If your lucky, you might get a box that produces a dial-tone. Hit 9, this will get you into the company's personnal phone line. This will allow you to make long-distance phone calls through THEIR phone, not yours, of course they get to flip the bill for your call. Explore them all you want, it's not illegal.
NOTE: Most mail systems turn on after closing hours.

Try some of these numbers-

1-800-525-5000
1-800-325-6397

If it says "Welcome", hack it

It seems that people have been able to get of charges for hacking by noticing that the computer they hacked, "welcomed" them to log on. A computer shouldn't display the word "Welcome", because it is asking you to access the system. By telling the judge this, you can reduce your fine, or even have the charges dropped against you. This also is the same for military systems that say "For offical use only". The "offical use" part will tell the hackers it is military, and will draw alot of attention to the system.

Little bits of information you did not know

The 1004 Hz tone is the official Bell System frequency for measuring channel losses. The 2713 Hz tone allows the user to activate Bell System remote loopback equipment.

---

information-and our way of life-has become. If one person can cause such chaos, then clearly the system is falling apart at the seams.

The Zinn case is equally deplorable. A bright kid is languishing in prison because he didn't know when to curb his intellectual curiosity. The newspapers accused Zinn of stealing software, but all he did was copy some programs. If these programs were so valuable, why in the bell was he able to download them over the phone lines?

The message here is that some of our nation's brightest kids are being imprisoned for being a little too inquisitive, and that's frightening. Much can be learned from what hackers uncover. Hackers may not be knights in shining armor, but the notion that they are dangerous criminals could not be further from the truth. These are kids doing what kids have always done. The only difference is that they've learned how to use a tool that most people have ignored. And until more of us know how to use that tool, there will be many more abuses-not just abuses of the tool but abuses by the tool. That's where the danger lives.

Hacking is not wrong. Hacking is healthy. Hacking is not the same as stealing. hacking uncovers design flaws and security deficiencies. Above all, hacking proves that the ingenuity of a single mind is still the most powerful tool of all.

We are hackers. We will always be. Our spirits will not be crushed by these horrible events. Call us co-conspirators, fellow anarchists, whatever you want. We intend to keep learning. To suppress this desire is contrary to everything that is human.

Like the authors who rose to defend Salman Rushdie from the long arm of hysteria, we must rise to defend those endangered by the hacker witch-hunts. After all, they can't lock us all up. And unless they do, hacking is here to stay.

License Plate Traces

Wisconsin Only

Write to: The cost is $2.10 per record

Vehicle Files
Wisconsin Department of Tranportation
P.O. Box 7909
Madison, WI
53707

Hoped you liked this issue
They will get better.
See you next issue

HOW PHONE COMPANIES ARE CRACKING DOWN ON FRAUD

SPRINT Will monitor overseas calls for suspicious patterns such as heavy calling to unusual destinations. For a fee, will cover losses over $25,000, up to $1 million per year per customer location

AT&T Also monitors overseas calls and, in one program starting in August, will cover losses over $25,000. Will cover customers' losses over $12,500 if customers spot the fraud before AT&T does

MCI No formal program, but monitors calls from the New York and Los Angeles areas, and alerts customers to suspected fraud. Will cover 30% of the first loss suffered by a customer. Recommends ways to stop fraud

FREE THE BABY BELLS

Cyber 'zine