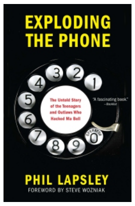

Title	**Raiders Proliferate With Computers**
Publication	*Los Angeles Times*
Date	1981-12-06
Author(s)	Perlman, Jeffrey, and Hastings, Debi A.
Abstract	Computer phreaks break into computer systems for fun. Article describes their methods and crimes.
Keywords	Kevin Mitnick (suspect); Lewis DePayne (suspect); Mark Ross (suspect); Pacific Telephone and Telegraph Co. (PTT); Los Angeles; The Ark (DEC's main computer; Digital Equipment Co. (DEC); Pasadena, CA; CA Dept. of Motor Vehicles (DMV); phone phreaks; blue box; Apple Cider (bulletin board); Donn Parker (computer crimes specialist); CRANK (British computer hacker group); computer hackers; National Computer Crime Data Center; TRW Credit Data; Bruce Goldstein (computer system security consultant); NCIC (national criminal intelligence network); Bruce Patton (computer hacker); Bruce of Irvine (alias, computer hacker); phone phreak; Starcom (bulletin board); COSMOS (PTT computer system); U.S. Leasing; Monroe High School (Sepulveda, CA)
Source	ProQuest

Raiders Proliferate With Computers
JEFFREY PERLMAN; DEBI A HASTINGS
Los Angeles Times (1886-Current File); Dec 6, 1981; ProQuest Historical Newspapers Los Angeles Times (1881 - 1985)
pg. B1

Raiders Proliferate With Computers

Computer pranking "is a serious, widespread, international problem."
—Donn Parker
Computer crimes specialist

'Pranksters' Try to Crack Complicated Systems

By JEFFREY PERLMAN
and DEBI A. HASTINGS,
Times Staff Writers

During a party at a Hollywood pizza parlor one Saturday night last May, Kevin Mitnick, 17, Lewis De-Payne, 21, and Mark Ross, 25, decided to drive to Pacific Telephone and Telegraph Co.'s downtown Los Angeles computer center and paw through trash.

They were looking for discarded correspondence and computer printouts bearing confidential codes and account numbers. With them, the trio could wreak havoc on the telephone company and its computer systems. Such search missions had worked before, Mitnick later told authorities.

They did not stop at rummaging through trash.

Court records quoting Mitnick in statements to the FBI say they pretended to be on a phone company tour, entered the center and stole several important computer manuals. The three were arrested last summer and charged with a variety of crimes. Through their attorneys, all three declined comment.

What seems especially noteworthy to authorities is that these young men say they were doing it for kicks. And what happened at PT&T appears to be only a sample of what those who understand complex telephone and computer systems can do.

Mitnick, for example, also was charged with gaining access to a private San Francisco firm's computer. The company initially estimated that it would cost $250,000 to reprogram information that had been lost or altered.

'These are technological trespassers. They often do it for the sheer joy of destruction.'

And Mitnick told the FBI that he had obtained sensitve data from "The Ark," Digital Equipment Co.'s main computer in Maynard, Mass.

Indeed, what emerges from court records and interviews is a subculture of about 150 people in California, many of them teen-agers, who have used telephones and computers in illegal ways. Computer pranksters are suspected—or have claimed credit—in:

—Shutting down Pacific Telephone's directory assistance service in the Pasadena area twice in recent weeks.

—Obtaining records from the computer of the state Department of Motor Vehicles.

—Obtaining confidential credit information from a major Southern California credit bureau's computer.

Theft of PT&T's computer manuals could have enabled Mitnick and his friends to shut down much of the phone service in the Los Angeles area, a district attorney's investigator recently speculated, and PT&T has fired the security firm that had been guarding some of its offices.

What's more, by Mitnick's account to the FBI, Mitnick and his friends had gained unauthorized access to computers all over the United States—computers supposedly impenetrable to all but selected people who know the codes and passwords to make the computers respond, like keys that unlock doors.

Computer pranksters obtain those "keys" by posing as company employees, by rummaging through company trash or simply by trial and error, using likely combinations of words and numbers. Companies using computers, it seems, have a limited imagination when it comes to codes and passwords, and few firms bother to pay the $50,000 and more that it costs to install special scramblers to protect computerized data.

In the 1960s, there were "phone phreaks" who used tone-emitting "blue boxes" to make long-distance telephone calls without paying. The new generation of "phreaks" uses computers to arrange sexual encounters, trade equipment and information about the latest computer games, and to share electronic espionage and sabotage techniques.

There are clubs, newsletters and electronic bulletin boards, and the participants often adopt nickname identities, much like citizens band radio users. Computer play is a hobby to many, but it occasionally crosses into more serious pranks.

A computer bulletin board called "Apple Cider" was used to transmit a death threat to a San Gabriel woman, who is expected to testify in the trial of one of Mitnick's co-defendants. The source of the threat could not be traced, authorities said.

Donn Parker, an author and computer crimes specialist at Stanford Research Institute in Palo Alto, calls computer pranking part of a "serious, widespread, international problem."

RANDY McBRIDE/Los Angeles Times

For instance, a British group known as CRANK reportedly obtained data from university, government and business computers whose security was previously unbroken, to demonstrate the need for better computer security.

Parker said the phenomenon hit home for him when his 14-year-old son was victimized by fellow students who were able to "talk" to their school computer and change grade transcripts.

"These are technological trespassers," Parker said. "They often do it just for the sheer joy of destruction. It looks fairly benign at first, but then some of them go on to more serious crime."

Jay BloomBecker is a former Los Angeles deputy district attorney who two years ago helped create the National Computer Crime Data Center in Los Angeles. It is a reservoir of case histories involving fraud committed via electronic data processing.

The public perception of computer pranksters as "geniuses and whiz kids" is inaccurate, Bloom-Becker said. The equipment is so easy to use, he said, that virtually anyone can learn how.

"Where one type of computer criminal will see the computer environment as a cookie jar—the source of enough money to meet personal needs—another might see it as a playpen—simply a place to play computer games for as long as he likes," BloomBecker said.

" . . . Unfortunately, there is no computer industry standard to define precisely when playing has gotten out of hand. Thus, if a student uses an hour of computer time without permission, one university computer department considers it criminal theft of services and another views it as commendable ingenuity."

Authorities say there was no law specifically making it illegal to gain access to someone else's computer until 1980, when a law sought by business and prosecutors took effect.

The new law, Penal Code section 502-C, states:

"Any person who maliciously accesses, alters, deletes, damages or destroys any computer system, computer network, computer program or data shall be guilty of a public offense."

Some lawyers say the new felony statute covers any computer access gained without permission. But others say it applies only to efforts to "vex, harass or destroy," not to unauthorized look-sees.

With or without the new statute, prosecutors have charged some suspects with theft, a legal strategy available only if something of value has been taken from a victim's computer. But such prosecutions are difficult, partly because judges have been reluctant to accept expert testimony about the dollar value of claimed losses. For example, prosecutors say there is no agreement about how much an hour of "stolen" computer time is worth, and computer time is often the only provable loss. This has led to dismissals of some criminal cases.

"Most cities (police departments) don't know how to deal with the problem (computer crime)," according to Randy McMahon, a fraud detective at the City of Orange Police Department. "My partner and I are the only ones in our department who have an active interest in it, so we went to a Radio Shack store to learn how to deal with it."

But McMahon and dozens of other police officers in the state also have been attending computer crime seminars held periodically by the state Department of Justice in Sacramento.

Some companies previously victimized by computer fraud, such as TRW Credit Data, have increased security by changing their operating procedures and by installing sophisticated equipment, McMahon said, but many others seem not to care.

Pranksters seem bent on proving they can do almost anything with computers and phone lines, and engage in one-upmanship.

"These are people who are experiment prone," said Bruce Goldstein, a computer system security consultant in San Francisco.

Patton said they can '...clean out your bank records and even have your front lawn removed.'

"To me it's an ethical issue. It stems from what students in high schools and universities are being trained to do.

"It's the mentality that pervades the universities and their computer 'crash' clubs, where the students are actually taught how to crash (destroy) a computer program. Instead of teaching them how to crash a computer, they should teach them a lot more about how to prevent it."

Public court records quote Mitnick, now 18, of Panorama City, telling authorities that he and other pranksters discussed trying to gain access to the national computer network known as NCIC, which processes criminal intelligence information for law enforcement agencies.

"I called the police station and they gave me their code, but I never tried to get into it," Mitnick said according to court documents.

However, Bruce Patton, a friend of Mitnick, told The Times that computer "phreaks" have obtained access to NCIC, and have run names through it without destroying or modifying data.

"I was there when they did it," Patton said.

Known as "Bruce of Irvine" on electronic bulletin boards, Patton, 28, is a self-described "phone phreak."

He called a Times reporter late one night and asked "What would you say if I told you I knew a format to type someone's phone service out of existence?"

The tall, lanky, long-haired Patton wears scuffed cowboy boots and talks in a high-pitched voice of acquaintances who can "disconnect your phone, repossess your car, clean out your bank records and even have your front lawn removed," all of which can be done by anyone with the right numbers, a home computer and telephone coupling device.

Aware that his claims were hard to believe, Patton volunteered to demonstrate his abilities. Patton said he is cooperating with phone company officials.

Patton—with a Times reporter listening in—used a law firm's computer to communicate with a Pacific Telephone computer and read back supposedly private information about The Times' telephones.

On another occasion, using a computer terminal in Newport Beach, Patton showed a reporter seated at a Times computer terminal in Santa Ana how to connect the two machines telephonically; then he caused private financial data from a Newport Beach law firm's computer to appear on and then vanish from the screen of the reporter's terminal.

Another time, he talked the reporter through the steps that would have made it possible to gain access to a Pacific Telephone computer.

On still another night, he told the reporter how to place messages in an electronic bulletin board called "Starcom," based in Westminster, from a Times computer terminal.

Throughout his demonstrations, he showed he could make any telephone call toll-free by dialing into private business firms' long-dis-

Please see 'PRANKS,' Page 3

‘PRANKS’: Computers Proliferate, and So Do Raiders

Continued from First Page

tance systems—systems that require only a four- or five-digit prefix for employee access and that can easily be "invaded" by outsiders using trial and error.

Where did Patton come from? How did he get into phone and computer "phreaking?"

A telephone and computer specialist who maintains data systems for a Newport Beach law firm, Patton said, "Most of us (computer pranksters) started out as bored kids."

"I grew up in Lakeview, Calif., (in Riverside County) and I didn't go to high school or college. I dropped out in the sixth grade . . . . I worked on ranches, took care of horses. I bugged people's telephones and stole equipment from the phone company."

After "playing hippie," he went from one job to another in several telecommunications service firms, taking care of PBX switchboards.

During that time, Patton said, he helped set up a Hollywood-based dial-a-joke, party-arranging and message-sharing phone line.

Patton befriended Mitnick and other "phreaks."

Eventually, Patton said, the group learned of a computer prankster who was a telephone company operator in Orange County. The man said he had a manual for Pacific Telephone's COSMOS (Computer System for Main Frame Operations) units, which lists the company's equipment inventory.

As Patton told it, a woman figured out how to penetrate COSMOS from outside the phone company and traded that information for the COSMOS manual.

The pranksters wanted greater access to the telephone company computers, Patton said, and competition developed over who would be first to get into certain phone company computer systems.

The result: Patton said the woman boasted she could get through security in Pacific Telephone's offices, and one night she proved it by taking her friends on a tour of one office.

"She told security that she worked there and was conducting a tour, and they didn't do anything to stop her," Patton told The Times.

Later, pranksters obtained the combinations to digital locks to phone company computer room doors, and the thefts of company manuals increased.

Court documents quote Mitnick as telling authorities that, after the Hollywood pizza party last May, "We decided to go over to the COSMOS center and look through the garbage cans, 'cause that's how we got most of our information, from the phone company garbage."

However, Mitnick also told law enforcement investigators that he already had obtained a photocopy of a COSMOS manual through a friend of Patton who worked for Pacific Telephone.

Manuals Photocopied

Patton told The Times that his friend gave him PT&T manuals one at a time, and they were returned after being photocopied.

But Patton said he did not know how Mitnick gained access to a private computer at United States Leasing International Inc. in San Francisco, where fouled programming cost $250,000 to repair. Nor did Patton know how Mitnick had hit The Ark, Digital Equipment Co.'s main computer in Maynard, Mass.

According to court records, however, Mitnick told authorities he was first approached about The Ark by a friend at a Culver City computer firm who dared him to do it. Mitnick succeeded, and passed sensitive data to his friend, who wanted it to help complete a problem-stalled computer program.

How was the computer at U.S. Leasing cracked?

Court records quote Mitnick as telling authorities that he used three different computer terminals in the Los Angeles area.

According to John Whipple, U.S. Leasing vice president for data processing, one of their computers was having software problems last December. A repairman came, and the next day Mitnick called and pretended to have the solution to the company's computer problem. A switchboard operator willingly gave Mitnick the password needed to gain access to the firm's computer.

Mitnick told authorities:

"Well, what I really did was I called up and impersonated like a Dutch person and I got the password."

The same court records show Mitnick claiming that he only created his own information account in the computer and blaming DePayne for the destruction of U.S. Leasing data.

Caught by UCLA Police

Mitnick told authorities that a friend at Monroe High School in Sepulveda triggered his interest in computers in the 10th grade. Soon a group of friends started spending all of their spare time playing computer games.

Then in May, 1980, Mitnick and another juvenile were caught by UCLA campus police using campus computers and phone lines to "talk" to computers at USC and elsewhere.

Among the items found on the juveniles:

Computer printouts of their UCLA transactions, a false Pacific Telephone employee identification badge and a homemade black code book showing how to gain access by phone to various computers, including airline ticket sales and reservation systems.

Mitnick's abilities almost allowed him to escape UCLA's campus police the night he and his friend were caught.

According to campus authorities, Mitnick was attempting to find an unrestricted phone line to transmit data from a UCLA terminal to another location and accidentally tapped into a conversation between two undercover campus police officers who had staked out the computer room and were at that very moment discussing Mitnick and his friend.

The two high school students fled, but the officers won the foot race.

Art Longo, a UCLA police detective who worked the case, said of the black code book confiscated from the two juveniles:

"It must have taken years of hard work to collect the numbers and information they had in it."

But Patton said he sees such efforts as fun, not work, and added:

"It's very addictive. Sometimes it's better than sex."