To Catch A Hacker. The true story of John Maxfield, electronic private eye. Appeared in August 1990 issue of PC Computing Magazine, by Rick Manning.

The computer crackers and phone phreaks who visited Cable Pair's cluttered office one August evening in 1983 must have thought they were in heaven.

Cable Pair was a sysop for a hacker forum on the Twilight Phone, a Detroit area computer bulletin board. The forum had become a meeting place for members of the Inner Circle, a nationwide hacker group that used words and swap tips on phone phreaking--getting free use of long-distance phone systems.

Cable Pair's visitors that evening were some of the Inner Circle's most active members, highly placed in the hacker pecking order. They had come in response to messages that Cable Pair had posted on the board, inviting them to take a guided tour of his headquarters, and they were suitably impressed. Computer equipment was everywhere. The sysop's console consisted of several terminals connected to a remote Hewlett-Packard minicomputer.

In a back room was a bank of electromechanical telephone switches--old stuff, but enough to run a phone system for a small town. Cable Pair even had an official Bell version of the infamous "Blue Box," a device that sends out the precisely calibrated tones that unlock long distance telephone circuits. To
demonstrate the magic box, he keyed in a 2600 cycle per second tone and was rewarded with the clear whisper of AT&T's long distance circuit.

Then like jazz players in a jam session, group members took turns showing what they could do. One tapped into AT&T's teleconfrencing system. Another bragged about how he once nearly had Ron Reagan, Queen Elizabeth, and the pope on the same conference call.

One hacker's specialty was getting into Arpanet, the advanced research network that links universities and government agencies, including defense research centers. "The Wizard of Arpanet sat right there at that keyboard and hacked into the system," says Cable Pair smiling at the memory. "And we captured every keystroke."

It was probable Cable Pair's finest hour. He was not, after all just another hacker. The gathering that evening was the culmination of an elaborate sting operation.

Outside the office, FBI agents watched everyone who entered and left the building. A few months after the jam session, police raided homes across the country. The confiscated computers and disks and charged about a dozen adults and teenagers with various counts of computer abuse and wire fraud.

Cable Pair was John Maxfield, whose career as an FBI informant had started a year earlier. Now approaching the age of 50, he is still chasing hackers, phone phreaks, and computer pirates. When his cover was blown in a hacker newsletter soon after the office party, he attracted a network of double agents, people who found it more convenient and safer to work with him than against him. Some continue to maintain their status in the hacker underground and pass information to Maxfield.

The nature of Maxfield's calling depends on your frame of reference. If you've read enough cheap fiction, you might see him as a private dick in a digital overcoat. Or a stagecoach guard sitting on the strongbox, eyes scanning the horizon, electron gun across his knees. He refers to the hacker phenomenon in the nebulous language of Cold War espionage, casting himself in a spy novel role as a warrior fighting battles that both sides will deny ever happened.

"He's very good at getting hackers together on one thing," says Eric Corley, editor of 2600, the hacker publication that fingered Maxfield more than six years ago. "I can think of nothing that hackers agree on except that John Maxfield is evil!"

Maxfield responds in kind "Hackers are like electronic cockroaches," he says. "You can't see them, but they're there, and at night they raid the refrigerator." Although a lot of hackers are what Maxfield calls "tourists"--young people who go into a system to simply look around--more sinister influences often lurk behind them.

"The tourist may go into a system and look around, but when he leaves, he's got a password and he'll share it with others because he's got an ego and wants to show how good he is," says Maxfield.

"It's my experience that ever hacker gang has one or more adult members who direct activities and manipulate the younger ones. What could be better than to have the naifs doing your dirty work for you? They can open all the doors and unlock the systems and then you go in and steal space shuttle plans."

The hackers are one step away from the shadowy world of spies." says Maxfield. "Some have deliberately sought out and made contact with the KGB." Maxfield wasn't suprised at all when West German police announced in March 1988 that they had arrested a group of computer hackers who used overseas links to U.S. computer networks to steal sensitive data. And he thinks computer companies and corporations haven't learned much about securing their systems. "There are more interconnections," he says "and that leads to more vulnerability."

A good example was the worm that Robert T. Morris Jr., unleashed in Nov 1988 through the Unix based Internet research and defense network that shut down more than 6000 computers.

"The hackers will tell you that this kind of thing is just a practical joke, a harmless prank. But in can do some very serious damage," says Maxfield. Computer systems experts who testified at Morris's trial last Jan. estimated that the cost of cleaning up after the chaos wreaked by the Unix worm was $15 million!.

The information that Maxfield collects about these computer pranksters and criminals goes into a database that he maintains to help him identify hackers and monitor their activities. Maxfield tracks the phone phreaks' identities and aliases to help his clients, who are managers at large corporations, credit card companies, and telephone companies--business people who feel the need to protect their electronic goods and services.

What can Maxfield do for them? If a corporation's phone system is abused

by unauthorized users or if its computer system is invaded by hackers, he can conduct an investigation and advise the company on how to contain the problem. He can also tell them where their system is vulnerable and what to do about it.

Most of the hackers whose names and aliases are in Maxfield's database probably are pranksters, teenagers attracted by the danger and excitement of electronic lock-picking. Their activities would remain mostly benign, Maxfield says, if it weren't for the organized online groups and the criminally-minded adults that urge them on.

"That's the real threat," he says. "It's not the pranksters so much as the
people they're associated with. The people who don't run bulletin boards, who don't brag openly about what they can do.

Maxfield could easily have become one of the hackers he now fights against .
As a teenager growing up in Ann Arbor, Michigan, in the late 1950's he had a comsuming passion for telephones and computers. During the summer he worked for an independent phone equipment manufacturer and spent time hanging around the offices of Michigan Bell. He also made some friends within Bell.

Naturally curious, Maxfield experimented with his telephone at home and learned how to blow fuses at distant switching stations and even how to shut down whole portions of an exchange. By studying AT&T technical journals used on his job and by picking up technical information from his contacts at Bell, he learned how to make his own blue box. In 1961, when dirrect dial service reached Ann Arbor, Maxfield was finally able to test his discovery.

Maxfield was shocked when he realized he could make long-distance phone calls for free. He called a friend at the phone company, and he mentioned his triumph to other friends. Maxfield's discovery attracted the attention of some people who offered to pay him $350 each for 1000 blue boxes.

Word also got back to AT&T special audit inspectors through the friend at Michigan Bell. After paying Maxfield a visit, the inspectors let him off with a warning, but not before suggesting that it was probably the Mafia that wanted to buy the boxes.

"They said the records of the bookmakers' long distance calls get them convicted in court," Maxfield recalls. If bookmakers manage to evade the telephone company's billing equipment, of course, they not only avoid having to
pay for the long-distance calls they make, there are no records that federal prosecutors can use against them.

Maxfield's prototype blue box took a midnight swim of a Huron bridge, and the kid stayed out of trouble after that. For the next 20 years he channeled his electronic expertise into fixing and installing phone equipment.

In fact, Maxfield's career as a counterhacker began quite innocently, in

1978, when he helped a local computer club start one of the nations first electronic bulletin boards. Four years later, the FBI cam looking for pirated software.

"I knew the pirated software wasn't in the clubs, but I also knew about pirate bulletin boards that had sprung up in the area," Maxfield recalls. So he printed out some of the messages from the pirate boards and took them to the local FBI office in 1982.

The FBI scarcely knew what to make of all of the information that Maxfield handed them. "They were still keeping records on 3X5 index cards!" he says.

But the bureau offered to compensate Maxfield for his expenses if he would monitor the hacker bulletin boards and report to them.

Maxfield accepted. The arrangement gave him what every hacker and phone phreak would love to have...a license to hack. He could call anywhere in the world or attack any computer and not worry about the consequences.

Maxfield might still be undercover for the FBI today if he and his contact at the bureau had kept their mouths shut and not underestimated the resourcefulness of the hackers.

Following the success of his 1983 office party and the resulting raids, Maxfield, still undercover, got involved with a New York hacker group that had take control of a corporate voice-mail system.

Against the FBI's advice, Maxfield tipped off the voice-mail system administrator, leaving a message urging him to contact the FBI. "What I didn't know as that the hackers also had access to the system administrator's account so they got the message first." Maxfield says.

One of the gang members, posing as the system administrator, called the FBI and learned enough to identify Maxfield. A story about Cable Pair's involvement with he government appeared in the first issue of 2600 in January 1984.

"We thought Cable Pair would be a promising contributor to this publication," the story concluded. "Instead we learned a valuable lesson: Don't trust ANYBODY."

"That's when the shit hit the fan," recalls Maxfield. "I was burned six ways from Sunday.

"My phone was ringing off the hook with death threats," he says. "The hackers were after me, and even the FBI didn't like me for a while."

"It was an ignorminious finish to Maxfield's underground activities for the government, but it launched his career as a consultant and electronic private eye. Several hackers who were worried about how much Maxfield know about their activities offered to become his double agents. "Some were even more highly placed than I was, and a couple of those people are still good sources today."

"Hacker groups are like street gangs," he says: the hierarchy changes all the time, and the organization is very loose.

One way to get to the top of this shifting hierarchy is to be a sysop for a pirate bulletin board, as Cable Pair was. Another way is to boast online about hacking exploits ("Well, I hacked into NASA's network and figured out how to alter the course of the Hubble Space Telescope...") or to post a lot of pirated information on the system.

Maxfield uses the hackers' own techniques to penetrate their private bulletin board systems. "It's a mind game," he explains. "Hackers will seek me out and feed me information about someone they hate or someone higher placed that they are" just to get them out of the way. They're "absolute anarchists," says Maxfield.

While Maxfield is watching the hackers, the hackers are watching him. Says Corley, "We have a nice thick file folder on him."

Maxfield keeps more than file folders. His database which has entries on about 6000 suspected hackers and phone phreaks, is cross-referenced by name, alias, phone number, gang associations, and criminal arrest record for phone fraud. He also tracks the names and numbers of pirate BBS's--and it's all at his fingertips.

Maxfield downloads information from his database directly to some clients. Others receive his periodical, which reports on hacker activities and lists phone numbers of active hackers and pirate bulletin boards. Companies that suspect illegal phone activity can use the list like a reverse phone directory, comparing phone numbers on their bills against the list to isolate the BBS from which the perpetrator is operating. Then they can work on preparing a case for law enforcement. Very often, the same perpetrators tap into the same system over and over, and companies that wish to prosecute must assemble evidence over a considerable period.

Sometimes Maxfield gets involved directly, but he says he is "not a bounty hunter" and claims that he'll tip off corporations or phone companies about security breaches even if they aren't clients.

He'll even help AT&T, although his relations with the company are strained. "They still think I'm one of the bad guys."

Other's in the industry, however, find Maxfield's work helpful and valuable.

"I put a lot of trust in the work he does," says Donn Parker, a computer crime expert at SRI International, in Menlo Park, California, and a regular subscriber to Maxfield's reports. "He does a very good job of keeping track of the malicious hackers and the phone phreak community."

Maxfield often conducts computer security seminars for corporate clients and government agencies. He can alert corporate clients to weak spots in their systems and advise them on how to tighten their electronic security. He tells his clients that networks are particularly vulnerable to invasion because "when you network systems together, it's like a chain, and you need only attack the weakest link. All you need is one site with poor security and you have a loophole."

Data sent over the telephone lines can also be tapped. "Some people sit on a telephone pole or in a car holding a laptop computer wired directly into the phone lines, picking off data and passwords," he says.

"Computer security isn't a computer problem, It's a people problem," says Maxfield. "And people just aren't security-conscious. The leave doors unlocked, and they write their passwords down and tape them to the fronts of their terminals.

"We have the technical knowledge to secure these systems. We know how to

keep the hackers out, but it's a problem of implementation. It's expensive, and it makes the system harder to use."

"Any system that's user-friendly," cautions Maxfield, "is also hacker-friendly."

Maxfield is as addicted to his profession as the hacerks are to their online capers. Even if he wanted to quit the business, he says, he couldn't: "The hackers just won't leave me alone."

Maxfield admits that sometimes it's a little scary to be the Lone Ranger out there. Much of what he's seen and worked on can't be discussed for fear that hackers will be onto what he's doing. But, he says, that problem is dire, and "we've got to wake people up to this. We need to increase corporate awareness, law enforcement awareness, and public awareness. Computer manufacturers need to think about designing systems that are more secure, and the phone system needs to rethink its entire network design."

And so Maxfield feels an obligation to continue his crusade. He knows too much to stop now.

A little info......

This article is one of many controversial articles that is being debated on the Master Control Program BBS. File retyped on 7/19/90 by user #1 of the MCP. Call today! (314)-993-3689.