Departments

Commentary

CONFESSIONS OF A HACKER

By Simson L. Garfinkel

Last July, a front-page article in *The New York Times* ran with this headline: "Computer 'Hackers' Viewed as a Threat to Phone Security."

A phone call to an editor of the paper, who asked that her name not be used, told me that *The Times* lexicon defines "hacker" as "computer enthusiast" or "computer hobbyist." So I pointed out to the editor that *The Times* uses the word "hacker" only when it describes people who commit illegal acts. What will a person who has never heard the word before think it means after reading this paragraph:

"Some personal computer enthusiasts, often called 'hackers,' view the task of breaking into the telephone system as a test of their skills and only infrequently inflict damage, industry officials and consultants say. But others act with criminal intent." (July 22, 1988.)

After people read many articles like this, they quickly begin to equate "hackers" with "computer pirates." Such is the case today. Even in the computer press, we're seeing articles all too often that use the word "hacker" for "pirate." Take this article that ran in a September issue of *Network World*:

"*Los Angeles*—A wholesale grocer here recently fell victim to a small band of hackers that commandeered the firm's voice-messaging system and used it to run prostitution rings and pass information about drugs."

Is it too late for us to reclaim the word "hacker"?

Let me retrace my steps...

I first learned of the word "hacker" the week I arrived at MIT, the birthplace of hacking. That weekend, I heard of an unofficial tour of the Institute's subterranean tunnels and roofs that was being led by a band of "hackers." Years later, I become one of these hackers myself, setting out late at night to find steam tunnels, bricked-off rooms, sub-subbasements—out-of-the-way places deep within the heart of MIT.

The thrill is to find a place that you've never been before and to sign your name or initials in some innocuous place: behind a high-voltage box or underneath a ventilation duct. This isn't graffiti; it's a "sign-in," your signature left for other hackers to see and admire. The ultimate thrill is to find a place that nobody has never been before and to be the first hacker to leave your mark.

Then there's computer hacking. Since the 1950s at MIT and other places fortunate enough to have "electronic brains," there have always been cores of people whose hands seemed permanently attached to the computer's keyboards. Joseph Weizenbaum, a professor of computer science at MIT, called these people "compulsive computer programmers."

These people would often stay up all night—sometimes for days on end—trying to fix the last bug in a computer program, trying to get the highest score in a computer game, or trying to wring 20 milliseconds from an inner loop of a device driver. Working alone, they could write programs faster than "software development" teams of five or ten people—software that was better than anything that ever came out of IBM or DEC. These were the people who made the computer revolution happen:

Hackers.

A hacker is responsible for nearly every program used on personal computers today: MS-DOS, Unix, *Visicalc*, BASIC, a whole slew of wordprocessors—all of these were originally written by hackers. The hackers' primary directive is that computers should be used: An idle computer is a sin. The glory is to have people use your program, the more the better.

As I spent more time with the building hackers and the computer hackers, I learned that they were really one and the same group of people. When I met hackers from other universities, again I found the commonality of interests. With a little reflection, it wasn't so surprising.

Today's hacker is the high-tech counterpart of yesteryear's explorer. The hacker has a thirst to go to the places where others cannot go or have not been, to do the things that others have not done. It's that desire to leave one's mark, be it a flag on the North Pole, a name on a wall or a computer program that everybody uses, that drives the hacker onward.

For many—most, in fact—it ends there.

In recent years, hackers have gotten a bad name. Invariably, whenever the stories of computer crime have surfaced ("high school students break into top-secret military computer and destroy missile data..."), the perpetrators are self-described "hackers." The media loved the term.

But by calling themselves "hackers"—a word unfamiliar to most people —these juvenile computer junkies gave the impression that all hackers were similarly inclined toward such mischief. And the rest of us, the silent majority of hackers, did little publicly to prevent the tarnishing of the name.

It's not as if these vandals had misused skills that had been foolishly entrusted to them by older, wiser hackers. Most hackers develop their skills by themselves, without outside help; all a hacker needs to bloom is a computer and time.

The problem is that these punks used their skills in ways that weren't socially acceptable. It's as if they had found the key to the candy store and, after being told all their lives never to go in there, decided to have a look. Some of them took things. Some of them put razors in the chocolate bars, thinking that nobody could be so stupid as not to see the trap before taking a byte.

Malicious hackers have hurt a lot of people.

I have a friend who broke into his high school's computer and wrote a program that created tens of thousands of files, all with names like "FILE00001," "FILE00002," "FILE00003." On this computer, it wasn't possible to type "DELETE FILE" to delete all of these files. At first look to the computer's administrators, it must have seemed as if the files had to be deleted one at a time.

My friend knew this. To make things easier for his victims, each file that he created was a copy of a program that would, if run, automatically delete all of the files. But the people he had played his prank on never thought to look inside the files. Instead, they followed their initial instincts and set about the time-consuming process of typing the commands to delete the files one by one. It took two days.

Other malicious hackers have deleted medical records, thinking that nobody could be so stupid as not to have a backup tape. They've written computer viruses to see if it was possible, then let the programs loose to see how far they could get. These pranksters see computer security as a game: Passwords are challenges to find, call-back modems are something to learn how to defeat. Many lose sight of the real damage they do.

When I called John Gallant, the editor of *Network World*, and asked him why he had called the people who had terrorized the wholesale grocer "hackers," he said:

"Certainly, I agree originally the term had a more romantic meaning than it might have today. In usage, the term has come to describe someone who gains unauthorized entry into a computer system, whether it be for entertainment or illegal purposes. That's the way it's used in the trade press, and that's the way we use the word."

Indeed, that's what most people today think the word means. And so I do not call myself "a hacker" in polite company, even though, in my heart, I know that I am one. And while I'll try to protect the name, I know that I'm fighting a losing cause. In retrospect, it's difficult to imagine how it could have been any different. ◻

Simson L. Garfinkel is a freelance journalist and computer consultant living in Somerville, MA.