OPINION

Is hacking ethical?

By Marcia J. Wilson
Computerworld | MAR 24, 2004 12:00 AM PST

The definition of *hacker* has changed radically over the years. With the aid of the mass media, the word has developed a negative connotation rather than the positive one it used to have. Add *ethical* in front of *hacker*, and it's even more confusing.

For the purposes of this article, I'll define those hackers with malicious intent as "crackers." Hackers can be categorized into the following three buckets:

1. Hacktivists: Those who hack as a form of political activism.
2. Hobbyist hackers: Those who hack to learn, for fun or to share with other hobbyists.
3. Research and security hackers: Those concerned with discovering security vulnerabilities and writing the code fixes.

Since The Hacker Manifesto was published in 1986, computer security has become a national concern, especially after the terrorist attacks of Sept. 11, 2001. The casual hacker no longer has the freedom to poke around public or private networks without raising the concerns of law enforcement agencies.

Laws have been passed or refined that make it a crime to hack. Many hacktivists and hobbyists are more careful when pursuing their activities to avoid being arrested, fined or jailed for their activities. Many have legitimized their activities and hobbies by taking jobs in the computer security profession, starting their own security consulting companies, working in the open-source community or through other openly public and cooperative ways.

The Computer Security Act of 1987 has received more notice since the Sept. 11 attacks. The act is a declaration by Congress that improving the security and privacy of sensitive information in federal computer systems is in the public interest. The threat of cyberterrorism has increased focus on this piece of legislation, as well as the more recent USA Patriot Act.

As a result of increased anxiety over terrorist threats, federal and state laws have changed to make it an offense to "break and enter" a private or public network without permission. Federal law has required companies to comply with privacy requirements, business controls and corporate governance standards. These laws have brought pressure to bear on our increasing responsibility to secure the infrastructure and have made it more difficult for hackers to practice their hacktivism, hobbies or research.

Technology has also affected hacking activities. In response to legislation about privacy, business controls and terrorism, companies interested in capitalizing on the opportunities that exist have developed and manufactured sophisticated security hardware and software. The increased sophistication of these products has made the job of the hacker more difficult, and the casual hacker may stupidly get caught when attempting to circumvent a complex security system.

Education and awareness campaigns have also made an impact on hacking activities. Companies and government agencies have become more aware of security issues. Some train their employees on security-conscious use of their computers. The famous hacker Kevin Mitnick declared that social engineering was his primary tool.

Where have all the hackers gone? Have they gone more underground or taken "real" jobs? There is continuing debate over the ethics of hiring a former cracker, especially one with a criminal record, and placing him in a position of responsibility in a security capacity. I suspect that this is going to continue to be a difficult debate. Since the laws have become stricter, hacktivists and hobbyists are at risk of being labeled crackers.

What should our response be to crackers, who focus on hacking for personal gain and whose intent is to steal, threaten and destroy? Throw them in jail and throw away the key! What should our response be to the three categories of hackers? Do the First and Fourth Amendments of the U.S. Constitution protect hacktivism? Is there a way that hobbyists can work with the community to serve their interests, maintain their integrity and gain the trust of the public and private sector? Can we embrace the hobbyists and separate the crackers from the mix and treat the two groups differently? Can we educate our children on the differences, emphasizing *right* from wrong while supporting and promoting passion, creativity and freedom?

Is hacking ethical? It is if viewed within the context of the three definitions offered: hacktivist, hobbyist and researcher. We have the right in this country to protest, and if our activism takes a digital or electronic form, we have the right to do so. But don't take my word for it, explore this excellent article by Dorothy E. Denning at Georgetown University, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." It will make you think.

We have the right to peaceably assemble, and that may mean "sitting in" on a Web site or physically locking arms side by side with others in a large city's downtown intersection.

We have the right to free speech. Researching vulnerabilities and reporting those vulnerabilities is also our right, even if big companies like Oracle Corp., Apache Digital Corp., Microsoft Corp. or Hewlett-Packard Co. get angry and threaten us with lawsuits. That's par for the course.

I would like to see citizens better protected against big business and government. I don't want a huge company with lots of money to snuff out the fire, passion or interests in my life, and I don't want the federal or state government telling me what I can and can't do by broadening their powers via the Patriot Act.

I believe hackers have a lot to offer. They provide a balance of power by virtue of their creativity and technical skills. I think we need to protect and recognize them and find ways of working together.

Yes, I do believe that hacking -- when properly defined -- is an ethical activity. And yes, I do believe that understanding our freedoms and rights and protecting all that's good in our society while preventing all that's bad is the right approach.

Related: Security

YOU MAY ALSO LIKE

Recommended by Outbrain

Memory-Lane Monday: Did they say anything about an offer you couldn't refuse?

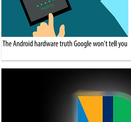
Ready or not, we're on our way to the Windows Virtual Desktop

The best way to write Messages on Apple Watch?

The HP example: How to do collaboration and remote work right

Windows 10 cheat sheet

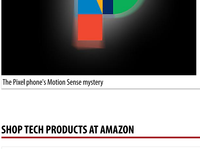
Google's grand Chrome OS plan is finally coming into focus



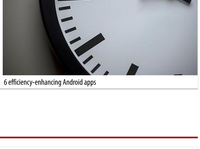
The Android hardware truth Google won't tell you

The Galaxy Chromebook and the problem with promises

It's time to squirrel away a clean copy of Win10 version 1909



The Pixel phone's Motion Sense mystery



6 efficiency-enhancing Android apps