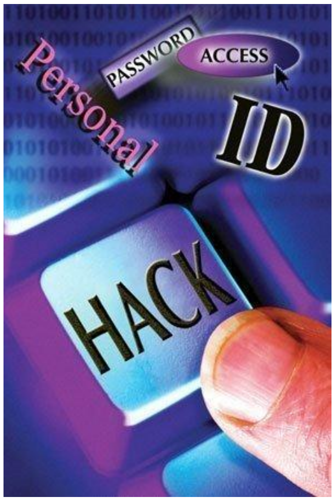
What Are the Effects of Computer Hacking?

Hacking as a Destructive Tool

The common stance on hacking with the average person is that it is morally wrong. There have been several instances where hacking has proven to have caused problems. Hacking can create a variety of damages to people, groups and systems of broad spectrum. Negative Hacking Interactions:

Identity Theft - Some hackers can gain access to sensitive information which could be used to fuel identity theft. This identity theft can cause damages to credit ratings from consumer agencies, run-ins with the law because the person who stole the identity committed a crime, or other damages which may not be repairable at all.
E-mail Access - Hackers have the ability to gain access to personal e-mail accounts. These can have a variety of information and other private files which most people would regard as important. This information could also hold sensitive data which could be used against someone or simply cause ruin for those who are involved in the breach of privacy.
Website Security - Many websites have been victims of hackers. Usually the hackers would simply destroy data and leave the websites in an inoperable state which would leave website owners with the task of rebuilding their sites from scratch if they did not have a backup. This could also pose risks for companies who had their consumer's payment information hosted on their websites. Defacing the websites by leaving tags or "calling cards" stating the unknown group's signature was not uncommon in the early days of hacking websites.

Hacking as a Political Statement



Some hackers are out to get the government and show the vulnerabilities that the government has in trusting their systems too much. This is extremely illegal in the United States and other countries. This has led to some vulnerability in security systems to being fixed and made the government computer systems even stronger. Of course it is difficult to do this kind of hacking without a trace being left behind. Most if not all hackers who get into the government systems around the world are captured by the government and punished for unauthorized access to their systems.

Hacking through Worm Exploits

Worms are nasty pieces of malicious code which are designed to find vulnerabilities in computer systems and exploit them with automated processing. They can be used to destroy data, collect information or simply lie in wait until they are given commands to do something. The worm code self replicates and tries to infect as many systems as possible. The big threat that these worms bring is the knowledge that a system is open.   This can allow the automated response to install a back door into a system which can allow malicious hackers to gain access to computers as well as turning systems into "zombies" which could be used for various purposes including spamming and masking the actions of the original hacker. Creators of catastrophic software such as the author of the first Internet worm, Robbert Tappan Morris Jr. did not mean to do bad at all. Before the Internet, there was ARPANET (Advanced Research Projects Agency Network), which was used by the United States government Department of Defense. Morris created the Morris worm, which was meant to gauge the size of the Internet but had actually gained access to ARPANET by accessing vulnerabilities in Unix based systems which were in use at the time. There was an error in his coding of the worm which caused replication at exponential rates which gained access into NASA and the Air Force systems. It was not intended to harm the computers, but did show that they were vulnerable to attacks. He got off with only community service even though federal guidelines should have given him extensive consequences for his actions. He was hired by MIT and is currently a professor working in the Artificial Intelligence Laboratory.

Hacking as a Learning Tool

Hacking leads several people into the interest of creating newer, better software which can revolutionize the electronic world. Although it is important to remember that hacking is a varied skill and those who have been hacking the longest will have more success because they know how computers work and how they have evolved over time. Ethical hackers use their knowledge to improve the vulnerabilities in systems, their hardware and software. The ethical hackers come from a wide variety of different backgrounds. The best examples are from ex-malicious hackers who decide their purpose is to help prevent damages to companies by holes in their security. These companies pay their ethical hackers handsomely as they are providing a service which could be extremely useful in preventing damages and loss. They can be hired by single companies who need advanced protection while others could be hired by software designers who will reach millions of people around the world.

Possible Protection from Hackers

Protection from hackers is important no matter whether it is for personal use or for large corporations. The following tools are the best defense against hackers:

Firewalls – The firewall is a software barrier which is designed to protect private resources and prevents unauthorized network traffic. They are designed to block off ports of access on the computer and require administrative clearance to access resources.

Routers – All modern routers include firewalls and protective features. You can password protect wireless networks and create useful protection with them.

Updates – Software updates are crucial to ensure the safety and security of any application of the software. It could be the operating system at home or the server software that processes website information and more.

Source: http://www.tech-faq.com/what-are-the-effects-of-computer-hacking.html