

LIVING IN THE REAL WORLD

A recent nursing school graduate applied to rent her first apartment and was turned down due to bad credit. Thinking she had no credit history she was mystified – until discovering someone had stolen her identity and left unpaid bills in her name. This theft occurred while she was a student.

She's not alone – the Federal Trade Commission (FTC) estimates nearly 9 million Americans have their identity stolen each year. Here are some tips from the FTC to protect you from this terrible crime.



7 TIPS TO PROTECT YOUR I.D.

1. Shred financial documents and paperwork with personal information.
2. Protect your Social Security number at all times.
3. Don't give out personal information on the phone, through the mail, or over the Internet unless you know exactly who you are dealing with.
4. Never click on links sent in unsolicited emails.
5. Use firewalls, anti-spyware, and anti-virus software to protect your home computer.
6. Don't use obvious passwords like your birth date, address, etc.
7. Keep your personal information in a secure place at home, especially if you have roommates.

For more information visit www.OnGuardOnline.gov.

ON THE HUNT FOR CYBER CRIMINALS!

IN A WORLD OF NEVER-ENDING THREATS FROM NETWORK HACKERS AND CYBER CRIMINALS, TODAY'S SECURITY SPECIALISTS ARE HERE TO SAVE THE DAY.

Individuals and corporations alike are paying a premium for system-wide protection. If you have a technically oriented mind and an old-fashioned instinct for solving mysteries then you may be the perfect candidate for the rapidly growing field of electronic security.

IT'S IN THE NEWS nearly every week: Somewhere somebody with a lot of time, access to the Internet, and malicious intent has cracked the "impenetrable" firewall at a bank, a major corporation, or a government agency. Regardless of whether their objective is to steal private funds or national secrets, cyber criminals are nothing more than thieves or terrorists and their crimes cause devastating and lasting harm to others.

In a recent speech Greg Garcia, United States Assistant Secretary of Cyber Security and Communications, stated, "Cyber crime is big business. The number of hackers attacking banks worldwide jumped 81 percent over the past year . . . surpassing drug trafficking from a monetary perspective. Worst of all, the money obtained through cyber crime can be used to finance terrorism."

Fortunately a dedicated group of men and women are entering security fields and becoming part of an ever expanding workforce that is growing in both the number and types of jobs available. This is very good news, according to Homeland Security Secretary Michael Chertoff: "The Federal government is not going to likely invent the best firewall. But there are things we can do to enable the invention and dissemination of techniques to raise standards, to warn about threats, and to help the private sector respond effectively when those threats occur." In other words, the Federal government is going to make sure qualified specialists will be given the opportunities and the resources to succeed.

Job descriptions and salaries for security careers vary widely according to the type of position and whether

PROTECTING OUR NATION

U.S. Department of Homeland Security offers many different careers among its various divisions. While the following list is not comprehensive, it will give you a sense of the jobs available for those who want to use their security skills to serve and protect our nation and its citizens.

DEPARTMENT	JOB
Transportation and Security Administration	Intelligence Operations Specialist
Citizenship and Immigration Services	Asylum Officer
Federal Emergency Management Agency	Fire Specialist
Immigration and Customs Enforcement	Detention Officer
Information Analysis and Infrastructure Protection Directorate	Telecommunication Specialist
Office of the Inspector General	Auditor
Secretarial Offices	Policy Analyst
Customs and Border Protection	Import Specialist
Science and Technology Directorate	Biological Scientist
U.S. Coast Guard	Engineer
U.S. Secret Service	Criminal Investigator



the investigator is self-employed or works for a government agency or a private corporation. For instance, private detectives who work as high tech security specialists are often called computer forensic investigators. Their work varies but usually includes determining how a system has been breached, analyzing encrypted or erased files, and recovering deleted emails and passwords. Median annual earnings of salaried private detectives, including computer forensic investigators, were \$33,750 in 2006.

Computer support specialists who focus in security are on the front lines of protecting systems by planning and implementing information security programs, installing security software, monitoring networks for security holes, gathering evidence when a crime has been committed, and providing education and protocol programs for their company's other computer users. As cyber attacks have increased, the responsibilities of security specialists have also grown and become more vital.

Median annual earnings of wage-and-

salary computer specialists were \$41,470 in 2006.

Network and computer systems administrators design, install, and



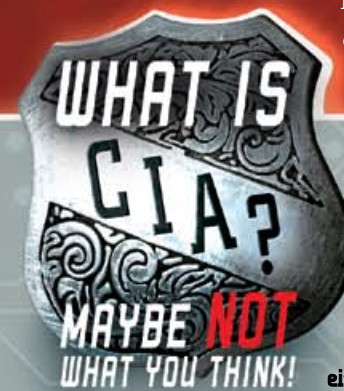
support an organization's computer systems including local-area networks (LAN), wide-area networks (WAN), and Internet and intranet systems. However, today most administrators also plan and execute network security measures as part of their core responsibilities. Median annual earnings of wage-and-salary network and computer systems administrators were \$62,130 in 2006.

Federal Bureau of Investigation (FBI) agents conduct surveillance,

monitor wiretaps, and participate in undercover assignments. Although the FBI investigates many types of criminal activity, cyber crime is becoming an increasing focus of concern. Since Federal law provides special salary rates to employees who serve in law enforcement, in 2007 FBI agents had a wide annual salary range that rose from \$48,000 to more than \$130,000.

For most security degrees, schools require students to take classes in criminal justice, information security, information systems forensics, Internet regulations, and network security and firewalls. These courses provide graduates with the ability to set up protective systems and give them an understanding of the laws that govern electronic fraud. In addition security students should take elective courses in the social sciences including psychology, political science, economics, and sociology; one or more foreign languages; accounting and auditing; and language arts courses like writing and speaking. While a few colleges have bachelor and master degrees in computer forensics, many schools offer certificate programs for law enforcement officers and others involved in investigative work.

To learn more about a career in high tech security, check with a local two-year college. Many programs are available, it just takes someone with a keen investigative sense to find them – and you know who you are! **M**



A common acronym used by cyber security specialists is "CIA." It is a threefold evaluation that designates 1) the limited access available to authorized users only, or **CONFIDENTIALITY**; 2) the assurance of reliable data and the credibility of its source, or **INTEGRITY**; and 3) the functionality of a system and its accessibility to legitimate users, or **AVAILABILITY**. Measures for confidentiality, integrity, and availability can be focused on either detection or prevention of security issues.