CyberSmart! 21st century skills for education

SAFEGUARDING YOUR STUFF, MY STUFF, OUR STUFF

Crime File: High School Hacker

An 18-year-old high school senior enters the school building after school hours. He uses passwords stolen from teachers to hack into the school network, changing his grades and changing the grades of some of his friends as well. He installs *malware*, or malicious code, that allows him to re-enter the network from any computer outside school. Instead of attending his high school graduation, he sits consulting with his lawyer, charged with crimes that, added up, could possibly result in a 38-year prison sentence.

What's the Problem? What actions did the young man take that were wrong, broke school rules, and may have been illegal? Who was affected by these actions? What if you were a student at that school—how might his actions affect you?

Notes:

Crime File: Malicious IMs

A 19-year-old hacker creates malware that spreads itself through instant messages. The messages, which look like they are from a buddy, invite the victim to look at a photo on a social networking profile. In reality, the link leads to a phony Web site that installs the malicious code on the victim's computer. As a result, all the information stored on the computer, including credit card numbers, can be viewed and copied by the hacker.

What's the Problem? What could be the consequences for the victims of this young hacker's actions?

Notes:

Crime File: Roaming Robots

An American employee of a company that sells kitchenware turns his company's computers into a network of virtual robots that earn him extra money while he sleeps. He uses his *botnet* to infect personal computers all over Europe with malware that displays pop-up ads on command. A second company, an advertising company in the Netherlands, pays him for each software installation. His trial results in a sentence of three and a half years in prison.

What's the Problem? How did this person's actions affect his employer? How could they affect the people who owned the computers he infected?

Notes:

CyberSmart! 21st century skills for education

SAFEGUARDING YOUR STUFF, MY STUFF, OUR STUFF

Think About It

Every day, different parts of the Internet are routinely scanned. There are many reasons people do these scans: Some do it to understand the Internet better, some to invent ways to make it work more efficiently for their business, and others to look for computers to attack.

The attacks can come from lone teenage hackers, organized crime rings, or political organizations. Some do it for the bragging rights, while others do it to promote a cause, attack others' homeland networks, make money, or steal money from others.

The Internet is a two-way street: Information passes into computers and out of computers. So when you connect to the Internet, the computer you use may be open to damage or trickery from anywhere in the world—from viruses, worms, Trojans, *phishing*, and *pharming* attacks. And because the technology is constantly changing, new threats are constantly being invented. That's why using the Internet means accepting responsibility to help protect your home computers, school computers, public computers, and even your country's computers from attacks.

Find Solutions

How can you defend your personal computers and the stuff on them against viruses, hackers, identity thieves, and botnet schemes? The best way is to stay informed about the latest security methods and use them regularly. Use critical thinking to evaluate online situations such as unsolicited e-mails and IMs, file sharing, free downloads, and all the other temptations on the Web.

Start at the place where your computer meets the network. All Internet connections require a modem. If your computer is connected directly to the modem, you need firewall software to keep the bad guys out. If you have more than one computer in your home or you use a wireless network, it is likely that you also have a *router*. Routers keep bad guys from scanning your computer. But there are still plenty of other ways for them to get to what they want from you. For example, phishing attacks try to trick you into connecting to a phony Web site and willingly giving out your private identity information.

Take Action

Have you and your parents had "the talk"? No, not *that* one, the one about cyber security. In this case, it's likely that you know more than your parents. So plan to talk to your family frankly about preventing cyber crimes on your personal computers and the public computers they use in the community. In class, do a role play to practice getting your talk just right. At home, answer your family's questions at their level of interest and knowledge. Together, create a list of actions to take to make the computers you routinely use and your information more secure.

Be CyberSmart!

Don't wait until something bad happens to your computer (slowdowns, crashes, corrupted files, stolen identity information). Make a cyber security plan and stick to it!

CyberSmart! 21st century skills for education

SAFEGUARDING YOUR STUFF, MY STUFF, OUR STUFF

Use the following checklist when planning your discussion with your family.

Personal Computers

- ☐ Install antivirus software and update it regularly.
- ☐ Beware of files attached to e-mails. They may be viruses. Don't open them unless you know what's in the file.
- ☐ Make sure you have a firewall on your computer or a router.
- ☐ If you have a wireless network, secure it with a password.
- ☐ Be very careful about the settings you choose when using file-sharing software. If you're not, you could accidentally give others access to private identity information.
- ☐ Disconnect from the Internet when you leave your computer.
- ☐ Back up your files onto external devices, CDs, or Internet servers.
- ☐ Download security and operating system upgrades regularly.
- ☐ Set up different accounts for each family member so that each person will have access only to the things he or she needs.
- ☐ Follow secure password management tips, including changing passwords often.

Public Computers

- ☐ Make sure the browser, messaging software, and other programs are not set to remember login names and passwords.
- ☐ Never leave a public computer while you are signed in to one of your accounts.
- ☐ Beware of over-the-shoulder snoops who watch you key in your passwords.
- ☐ When finished, always click "log out." Don't just close the browser window.
- ☐ When you are finished, clear the browser history, cookies, and any temporary files created as a result of your browsing.
- ☐ Don't do online banking or use a credit card.
- ☐ Check with owners of the public computers to find out what security precautions they have taken. If they don't have good answers, don't use the computer to log into personal accounts.