Week 2

Lesson 2: Cyber Security

Cyber security and cyber safety are closely linked; both deal with protecting yourself online, but in different situations. Cyber safety focus on protecting, you, the individual. Cyber security is concerned about protecting those things that belong to you, such as your bank account information and social security number. In the last lesson, which focused on cyber safety, you learned about how to protect yourself against cyber-predators.This lesson will focus on how to ensure you don't become a victim of financial crimes.

Activity:

1. Read the USA TODAY article *Identity theft's a big pain, but protecting yourself needn't be*.

2. As a class, discuss the following questions: According to the article, young adults (ages 18 to 24) are at higher risk of identity theft than other adults, why do you think this is? If steps to protect oneself are so simple, why don't more people safeguard themselves against cyber crime? Do you personally have anti-virus software or firewalls on your computer, and do you know when they were last updated? Why or why not?

3. Find a partner. Adopt the role of cyber security specialists with Mastercard. Your job is to create a flyer, designed to convince people your age to protect themselves against identity theft and cyber crime.

4. Trade flyers with another set of partners. Give feedback on what is and isn't effective about their flyer. Did their flyer convince you to follow the steps to cyber security? Why or why not?

5. Have each set of partners present their flyer to the class. Then, take a vote on which flyer is most effective and why.

Discussion:

The article outlines five easy steps for protecting oneself against financial crimes; are you likely to begin doing any of those steps? One-third of students between the ages of 10-17 regularly post their real names, phone numbers or home address, is this something you do? Why is posting this kind of information on your MySpace page (or anywhere on the Internet, for that matter) a bad idea?

Week 2

Cyber Security

Identity theft's a big pain, but protecting yourself needn't be

By Sandra Block
USA TODAY

You've chronicled your dating history on your MySpace page. You've posted a video of your wild weekend in Tijuana on YouTube. Still, even if you're young and uninhibited, there are some things you shouldn't share with the world. We're not talking about those photos of your hot tub party. We're talking about financial information — your Social Security number, for example, or your credit card statement.

Sharing this kind of information makes you vulnerable to identify theft, an insidious crime that can haunt you for months, even years. Young adults are particularly at risk. About 5.3% of adults from 18 to 24 said they were victims of identity theft during the past 12 months, up from 4.5% a year earlier, according to a new survey by Javelin Strategy and Research.

The study found that 3.7% of all adults were victimized, down from 4% a year earlier. Overall identity theft has been declining since 2003, when 4.7% of adults said they were victimized, Javelin said.

Not everyone agrees that identity theft is declining. Linda Foley, director of the Identity Theft Resource Center, a non-profit based in San Diego, said she's seen no evidence of a decline -- or even a leveling off -- of complaints.

Javelin President James Van Dyke, says identity theft is "still a significant problem." But consumers are doing more to protect themselves, such as using online financial sites to check for suspicious activity, he says. "You have people monitoring their accounts more frequently, using new electronic methods," he says. "Ten years ago, you couldn't do that unless you went to an ATM constantly."

Yet even though young adults are more cyber-savvy than their parents, they're less likely to take basic precautions, Van Dyke says. For example, the survey found that young adults were less likely than other adults to use anti-virus software and firewalls in their computers.

How to protect yourself

Concerns about identity theft have fueled a billion-dollar market for credit-monitoring services, identity theft insurance and other products. But some of the most effective steps you can take to protect yourself are inexpensive or free. Among them:

▶ Monitor bank and credit card accounts regularly by phone, ATM or over the Internet.

▶ Reduce the amount of paper in your life. Mailboxes containing credit card bills and other sensitive financial information are prime targets for thieves, Van Dyke says.

Shredding sensitive documents is a good idea, but "it's not enough just to shred," Van Dyke says. "Most criminals go to your mailbox, not your trash." His advice: Arrange for electronic delivery of bank statements and bills.

▶ Lighten your wallet. Nearly 40% of identity theft stems from lost or stolen wallets, checkbooks or credit cards, according to Javelin's survey of victims who know how their information was stolen (see box). Rid your billfold of credit cards you don't use, along with other documents, such as your Social Security card, that you don't need on a regular basis.

▶ Secure online accounts with difficult-to-guess personal identification numbers and passwords. Keep PINs and passwords in a safe place and change them often. Update your anti-virus programs and firewalls frequently.

Online accounts are "a safe way to do business as long as you take the necessary precautions," Foley says. That includes working with a reputable company that will safeguard your information, she says.

▶ Take advantage of your right to obtain free credit reports. The major credit-reporting agencies offer credit-monitoring services that alert you to any changes in your account. But you can create your own credit-monitoring system at no cost. You're legally entitled to order a free credit report once a year from each of the three

AS SEEN IN USA TODAY FEBRUARY 6, 2007

Week 2

credit-reporting agencies through www.annualcreditreport.com. By staggering your requests, you can receive a different credit report every four months, enabling you to check your reports for any suspicious activity.

While free credit reports provide enough protection for most people, those who believe their personal information may have been stolen should consider subscribing to a credit-monitoring service. If you think you're at high risk of identity theft, checking your credit reports every four months "may not be enough," Van Dyke says.

Another option is to freeze your credit reports. A credit freeze bars lenders and others from reviewing your credit history, making it almost impossible for criminals to open new accounts in your name. Twenty-six states have adopted laws that let residents freeze their credit reports, according to Consumers Union.

You can find information about your own state's laws at www.consumersunion.org.

National Cyber Security Alliance presents Top 5 Tips to Stay Safe Online

1. **Know who you're dealing with online.** Do not respond to/download attachments from unsolicited emails. If your bank asks for any personal information, always call and confirm before sending any personal information online.

2. **Secure your computer** with anti-virus and anti-spyware software and a firewall. After you install, it's important to keep it updated so you're protected against the latest risks.

3. **Use automatic updates** for your web browser and operating system. This closes any holes in your operating software, helps protect you from hackers and doesn't require any work from you!

4. **Create strong passwords** to protect your personal information. Make it harder for hackers to steal your passwords by using at least eight characters, including numbers, letters and/or symbols.

5. **Know what to do if something goes wrong.** Contact your local law enforcement agency if you think you've become a victim of Internet crime or online identity theft, and then contact the three credit bureaus and have them place a credit freeze on your identity. Moreover, contact your banking institution immediately if your credit card number is stolen.

Get more tips for keeping your computer and identity safe at **http://www.staysafeonline.org**.