

Identity Theft Lesson

Grade Level: 9-12

Duration: Two 15 minute sessions

Description: **Objectives**

- Define online identity theft and describe several ways it can occur.
- Research online identity theft and create a tip list for preventing it.
- Communicate good online identity theft prevention practices to family members.

Content Outline

1. Read the following to students (or have students read):

From: Corvallis Woman Loses nearly \$100 in Bank Fraud

http://www.gazettetimes.com/articles/2009/07/08/news/community/5loc02_fraud070809.txt

Corvallis woman loses nearly \$100K in bank fraud

by the Gazette-Times

July 8, 2009

Money transferred out of her account to California bank

Nearly \$100,000 was stolen electronically from a Corvallis woman's banking account late last month, according to a Corvallis Police Department report.

The woman, who is a scientist, called police the afternoon of June 29 to report that she was missing \$96,770. She noticed the money was missing on the evening of June 26 when she received a bank transfer alert on her e-mail account.

According to Capt. Jon Sassaman of the Corvallis Police Department, the FBI is working with local officers to investigate the "unusual" case.

"Someone was able to transfer money from one bank to the other across state lines," Sassaman said.

Few details were available regarding how the fraud occurred. In a telephone interview on condition of anonymity, the victim said police asked her whether her mail had been stopped by someone other than herself.

Tony Green, a spokesman for the Oregon Attorney General's Office, was skeptical about that method of information theft, saying that it seemed an overly elaborate way to steal personal mail.

Sassaman urged bank customers, especially those who do a lot of online banking, to check their statements regularly and to be sure to call their banks if they notice any unusual activity.

Corvallis police initially asked the Gazette-Times not to report on the crime, saying publicity could alert the suspect that police were investigating the theft. However, the authorities later agreed that publicity might prevent or alert people about other online banking fraud and released further details.

Protect yourself from fraud

Online banking is growing rapidly in popularity, and while it's safe in general, there are many things consumers can do to protect themselves, said Linda Navarro, president and CEO of the Oregon Bankers Association.

"A lot of these have to do with your identity in general, not just with online banking," she said. "In general when you are conducting your financial business, you need to be careful, because there are plenty of crooks out there."

Here are some of Navarro's tips.

- Check your bank and other financial statements as soon as they arrive for unauthorized charges.
- People who do online banking can check their accounts often, including between statements.
- Shred your receipts and unused credit card offers before you throw them away.
- Get a yearly credit report, and make sure it is accurate.
- If you suspect fraud or identity theft, notify your bank immediately.
- Don't carry PIN numbers or passwords in your wallet.
- Don't open e-mail from unknown sources, and use virus protection software for your computer.
- Don't provide bank account information, over the phone or online, unless you are positive it is your bank and you have reached out to them. "Your bank isn't going to ask you for your passwords unsolicited," Navarro said.
- Make sure the companies you do business with online are reputable.
- Put your outgoing mail in a secure mailbox, not in a unlocked box with the flag up.

2. Discuss Strategies to Protect Your Identity:

From: Stay Safe Online

<http://www.staysafeonline.info/content/self-assessment-quiz>

- **Back up your computer:**

Even a secure computer can fail, causing you to lose all of your documents, family photos, music and anything else you've stored electronically. If you follow a few simple tips, and make it a habit to make regular backup copies of all critical information on your computer, you can protect yourself from the worst sort of computer disasters.

How to back up your computer:

There are several tools you can use to back up your computer. They vary widely in price, size and ease of use. Some tools, like external hard drives, may provide instructions for how to back up files. In most cases, copying files is as easy as finding the information you want to back up on your computer and copying it onto the media or drive you're using.

Backup devices/tools include:

- Recordable CDs
- Recordable DVDs - DVDs
- USB Flash Drives –
- External Hard Drives -.

Backup Tips:

- Make backups a regular habit. If possible, store your backup device in a different place than where you keep your computer.
- Keep your important files in one place on your computer -- a specific folder perhaps -- to make for easier backups.
- Use your computer's backup tools.

- **Choosing Safe Passwords**

Your passwords are the equivalent of the lock and key to your house on the Internet.

- Passwords should have at least eight characters and include upper case (capital letters) and lowercase letters, numerals and symbols.
- Avoid common words:
- Don't use personal information—name, children's name, birthdates, etc. that someone might already know or easily obtain.
- Change passwords regularly—at least every 90 days.
- Use different passwords for each online account you access (or at least a variety of passwords).
- If you must write down passwords, under no circumstances should you store them in a document on your computer. Keep them in a secure location away from your computer.

One reason people pick passwords that are too easy is because they think they are going to forget them. One way to create a strong easy to remember password is to think of a memorable phrase and use the first letters, upper case and lower case letters, numbers, and maybe an added twist to make it secure. For example, "Only you can prevent forest fires" could become: oYcp4estF

Increasingly, online service providers are implementing new tools to create secure access to accounts. Some involve additional levels of authentication. For example, some sites now offer a small device that attaches to a key chain that gives you a new numeric password every time you log on. Once that password has been used in can never be used a

- **Email Filters**

If you have an email account, you know why you need email filters.

The first thing to do is to enable a junk email (or "spam") filter. Most email programs and online services come with one of these installed. In many cases these are set to "on" by default, but if they're not, you can easily activate by finding your filtering preferences tab, or using your program's "help" tool.

Some junk mail filters -- like the one that comes with Microsoft Outlook -- have multiple junk mail settings. At the highest level these will filter out virtually everything you don't want. Just be aware that at the highest settings, spam filters can sometimes trap emails you want to receive. If you have your junk mail settings cranked up, make sure to take an occasional peek at your junk mail folder.

The next level of email filtering is to block all email from specific addresses. This works differently in different programs, but in Microsoft Outlook, for instance, you just select the message from the sender you wish to block by clicking on it, select "block sender" from the "message" pull-down window then click "yes" and "ok."

IMPORTANT NOTE: No email filter is perfect, so you still want to treat every message you get -- even the ones that appear to come from companies you do business with -- with a certain degree of caution.

- **Keep Your Laptop Safe**
 - Treat your laptop like cash.
 - Keep it locked.
 - Keep it off the floor.
 - Use a non-descript carrying case.
 - Keep your passwords elsewhere.
 - Password protect your system. .
 - Backup important data before traveling.
 - Write it down.
 - Mark it.

Finally, if the worst does happen and your laptop is stolen, report it to local authorities immediately. If it was a business laptop, also notify your employer. You may also wish to review the Consumer Information section of the FTC website at www.ftc.gov for information about data breaches and identity theft.

3. Assessment

Distribute the Identity Theft Self-Assessment Quiz.