IDENTITY THEFT AND PHISHING SCAMS

Key concepts
Consumer protection of financial records, protection of one's identity through paper and online

Summary
This lesson introduces students to identity theft and phishing, including common methods used in the crime of identity theft. Students also learn about the consumer protection agency (the FTC) that handles this fast-growing financial crime.

Overview & Lesson Objectives
This lesson is intended for high school students in ninth through twelfth grades. The lesson teaches students how to protect their identities while making purchases online and in everyday financial life. The activities rely on a variety of interactive and visual formats designed to be interesting and fun.

Students will be able to:

- List the common techniques used to steal one's identity
- Become aware of electronic phishing ploys
- Describe and evaluate methods to protect financial records
- Explain how to take action if your identity is stolen
- Explain behavior to operate more safely online and with mobile devices

Time Allocation:
15 – 20 Minute Prep
35 – 40 Minutes Engagement

Materials:

- Access to the internet in the classroom or handouts from the Federal Trade Commission website

Lesson Begins: Setting the Stage

State the Objective: Tell the students what they will be able to do upon conclusion of the lesson.

"Today we are going to learn about a fast-growing financial crime: identity theft. You will be able to list the common techniques used to steal one's identity and know how to report that one's identity is stolen. You will be able to list some behaviors to protect your financial records and personal information and to operate more safely online and with mobile devices."

Lesson Continues

If you have ever heard a parent or a relative say when they opened their credit card bill, "Wow, I did not charge all of these items." I did not buy a $500 watch!" it is possible that they were a victim of identity theft. Federal Trade Commission (FTC) surveys show that about 18 million people are victims of identity theft each year. People who are dishonest and unethical (and they are often very smart) will try to make their money by stealing yours. Identity theft is a crime.

Open the lesson with a definition of new terms and phrases, asking students if they know what they are.

Definitions:

Identity theft is when a person acquires and then uses your name, address and Social Security Number in order to apply for a credit card in your name or purchase products in your name.

Phishing occurs with electronic communication such as e-mail or text messaging. It is when someone pretends to be someone or something they are not to acquire your passwords, credit card or bank account information, or other personal information.

FTC: The Federal Trade Commission an independent federal government agency (since 1914) whose mission is to promote consumer protection and help deter anti-competitive and unethical business practices such as deceptive advertising, phishing, and identity theft.

Watch an instructional video by the Federal Trade Commission on identity theft.

- FTC – Identity Theft Deter.Detect.Defend (10 minutes) at: https://www.youtube.com/watch?v=bC8pjXn-sWM&t=9s

Phishing article from the Federal Trade Commission

- https://www.consumer.ftc.gov/articles/0003-phishing

Review the major points of the video and article. If your classroom does not have access to the internet, the major points are:

The top methods for stealing a person's identity are:

1. "Dumpster Diving": going through a person's or household's trash to look for credit card offers, bills, bank account numbers, pay stubs, anything with Social Security numbers, birth dates, bank or credit account number, or other personal information.
2. Skimming: stealing credit card numbers with a small hand-held unit that can store your credit card number with a quick swipe of your card.
3. Phishing: pretending to be a legitimate financial institution, government agency, or company though an e-mail, a pop-up message, a text message, etc.
4. Changing your address: Completing a change of address card at the Post Office to defer your mail to another location other than your home. Or hacking into your e-mail or online accounts to change your address or steal your personal information.
5. Stealing: stealing mail from a person's U.S. postal service mailbox, or stealing your mailed Income Tax Return; stealing wallets or purses; bribing employees who have access to employee personnel records.
6. Unsecured Websites: online purchase sites where the URL does not start with "https", indicating it is not secure and opens you to the chance that identify theft occurring.

Ask students if they can think of other, unscrupulous methods for attempting to steal one's identity or cleverly disguise phishing. Ask them if they have ever received a spam text message (it is likely that they have).

Ask students to come up with a list of the harmful things that could occur if your identity is stolen, for example:

- Someone could withdraw money from your bank account using a debit card or credit card in your name.
- Your credit score could drop if you exceed your credit limit.
- You have to take the time and go through the expense of cancelling accounts, getting new accounts and account numbers, etc.

What to do if you are a victim of Identity Theft

The FTC's website is a one-stop resource to both learn about identity theft and walk you through the appropriate actions if your identity is stolen. https://www.consumer.ftc.gov/

Some steps include:

- Report the identity theft to the 3 credit bureaus: Experian, TransUnion, and Equifax.
- File a police report with local law enforcement.
- Report the theft to the FTC online at www.ftc.gov/idtheft or by phoning 1-877-FTC-HELP (1-877-382-4357).

Deterring Identity Theft:

Ask students to come up with a list of behaviors to deter thieves from stealing their identity, such as:

- Shred financial documents that are not being kept for safeguarding. [This allows a teacher to cover the kind of information that should be held and for how long (in years). It also allows a teacher to cover what documents are best kept in a safe deposit box, a home safe, regular home files, etc.]
- Do not carry around your Social Security Card in your wallet.
- Do not give out personal information over the phone or over the internet unless you are absolutely sure who you are dealing with.
- Choose computer and electronic passwords with care by avoiding birth dates, your Social Security Number, your mother's last name, etc.
- Try not to have your postal mail pile up in your mailbox for several days; if you are going to be away for a few days, have your mail held at the post office until you return.
- Do not click on suspicious links in e-mail or complete forms with your account number and password. Check the web address.
- Be suspicious about regular bills that do not arrive on time, denials of credit for no apparent reason, calls or letters about purchases you did not make, charges on your financial statements that you do not recognize.
- Use a password to access your mobile devices such as your cell phone, tablet (iPad), etc., just as you would have a password to get access to your e-mail accounts.

Lesson Closes

Review with students the importance of securing their personal information and keeping an eye out for persons trying to steal information through electronic means. See the suggestions page for "Additional Engagement Opportunities/Resources", for additional ideas.

Additional Engagement Opportunities / Resources

Pair and Share
Students (pairs) interview one another about the lesson content. They must summarize the partner's feedback in either written report or verbal format

Sample questions:

- How can you better safeguard your personal information?
- What should you be careful to review online to avoid responding to phishing scams?
- Describe why it is important to protect one's financial documents/identity.
- What can you do to protect your identity from being stolen?
- What steps should you take if your identity is stolen?
- What is the name of the government organization that can assist you if you're a victim of identity theft?

Misinformation: Quote information from the day's lesson purposely erroneous. Call on various students to restate the information correctly.

Samples:

- Phishing is when someone uses your name, address and social security number to open a credit card in your name.
- It is safe to respond to an email asking for personal information
- It is recommended to use your birthdate or mother's maiden name as your password
- Shredding your financial documents guarantees protection from Identity Theft

What's left out? Supply students with statements that have some information missing. This can be done verbally or it can be done on a board. Ask students to provide the missing information.

Samples:

- Stealing credit card numbers with a small hand-held unit that can store your credit card number with a quick swipe of your card is called _____.
    - *Answer is "skimming"*
- Pretending to be a legitimate financial institution, government agency, or company though an e-mail, a pop-up message or a text message is a form of _____>
    - *Answer is "Phishing"*
- If you gave a scammer your personal information, go to_____. You'll learn what to do if the scammer made charges on your accounts
    - *Answer is "Identitytheft.gov".*

Peer Education through Skits, Videos: Often learning is reinforced or students learn best by teaching others. Have students write a script and act it out in class with the objective of teaching each other (their peers) about the lesson. A student skit could show identity theft or phishing in action and/or the proper steps for preventing it or reporting it once it occurs. Students could invent very clever scenarios that will keep them on alert in the future. These should be prepared by students and performed in another class period that follows this lesson.

Educational Standards

NJ Core Curriculum Content Standards for Personal Financial Literacy 2014:
Standard 9.1: 21st Century Life and Careers
Standard 9.1 Personal Financial Literacy
9.1 E. Becoming a Critical Consumer: 9.1.12.E.8, 9.1.12.E.10

National Standards in K – 12 Personal Finance Education (from Jump$tart Coalition) 2017:
Spending and Saving:
Standard 4: "Apply consumer skills to spending and saving decisions."
Financial Decision Making:
Standard 1: "Recognize the responsibilities associated with personal financial decisions."
Standard 7: "Control personal information."