Identity Theft: Risks and Recovery

LESSON DESCRIPTION (Background for the Instructor)

In this lesson, students will learn about reasons for the increase in identity theft worldwide and personal identity theft risk factors that they have some control over. They will also learn about the impacts of identity theft on individuals and the arduous process that victims must go through to restore their pre-theft identity including repairing their credit history and restoring bank account balances and tax refunds.

The lesson includes five activities that instructors can select from. In these activities, students will:

- View the video *Secrets of an Identity Thief* and answer debriefing questions
- Play the 10-question game *True or Trick?* to identify myths about identity theft
- Take the online quiz *Are You at Risk for Identity Theft?* and answer debriefing questions
- Analyze the case study *What Would You Do?* to identify action steps to reduce identity theft risks
- Conduct a *Web Quest* to learn about steps that fraud victims should take to restore their identity

The lesson also contains 10 assessment questions (5 multiple choice and 5 True-False), learning extensions (i.e., suggested learning activities beyond the scope of the lesson plan), and references and resources.

INTRODUCTION (Background for the Instructor)

A century ago, when criminals wanted to steal money, they often robbed banks. While some bank robbers achieved fame and notoriety, robbing banks was a very hazardous "occupation." Bonnie Parker, Clyde Barrow, and John Dillinger were shot to death by police at young ages as shown in the movies *Bonnie and Clyde* and *Public Enemies*. Willie Sutton lived to age 79 but spent more than half his adult life in prison.

Today, identity theft is a leading cause of financial theft. Identity theft is the stealing of another person's personal identification information (e.g., Social Security number) and using it for personal gain. Identity theft is not typically a "stand-alone" crime but, rather, part of another crime such as credit card fraud. There is no need for thieves to use guns or physical violence to steal money from others. Rather, a victim's personal information is used to commit a fraud. Identity theft can affect credit card accounts, cell phone service, bank and brokerage accounts (e.g., withdrawal of account funds), tax refunds, and health insurance. A Social Security card and a driver's license are the two most commonly misused forms of identification.

Some thieves even take out loans in a victim's name, often to buy expensive items such as a car. Criminals also steal victims' health insurance data and have medical services performed in victims' names. Some identity theft uses "low tech" methods (e.g., stealing wallets and "dumpster diving" for papers with sensitive data) while other cases are committed online or by hacking computer databases.

With identity theft, criminals act as if they were another person (the victim) and use the victim's data to commit fraud in the victim's name. Men can "be" women or women can "be" men as shown in a series of humorous television commercials about identity theft (e.g., a woman talking in a man's voice and a man claiming to be a woman named "Peggy"). Identity thieves often capitalize on a topic or event in the news and use these events to create a sense of urgency to encourage victims to divulge personal data.

Unfortunately, many potential sources of identity theft are beyond an individual's control such as personal data in databases and at workplaces, government agencies, medical service providers, and companies that consumers do business with. Anyone can be a target of this crime. For example, during the 2017 Equifax hack, cyber thieves stole the personal information of 145.5 million people, which is more than two-thirds of the U.S. working population. Therefore, almost everyone is (or will be) a victim. While we can't control every possible risk for identity theft, it is still important to control what we can.

Following are suggested steps to reduce the risk of becoming an identity theft victim:

- Never click on unsolicited pop-up ads which are often associated with phishing scams or spyware. Use strong computer passwords in a string of at least 10 characters with numbers and characters.
- Consider following a personal policy to never hand over a credit card to others to swipe outside of your view. This reduces the risk of having your credit account data "skimmed" and misused by others.
- Use a crosscut shredder to shred documents with sensitive data. A crosscut shredder is better than a straight line one because paper is cut into small pieces instead of strips that could be pieced together.
- Avoid divulging your Social Security number. When absolutely necessary (e.g., to receive expense reimbursement), never type it in an e-mail. Give it to the person in authority who is requesting it.
- Take precautions to secure incoming and outgoing mail. Use locked mail boxes or post office boxes for incoming mail and place outgoing mail in mail boxes and not in open mail trays.
- Avoid carrying around a lot of identifying information. Never provide personal data over the phone to people who call you for it and to be careful not to leave personal data out in the open at home.
- Regularly review credit reports to check for suspicious charges or other evidence of fraud (e.g., new credit accounts that you did not open).
- Regularly review bank and credit card account transactions online to look for evidence of fraud.
- Never give personal information over the phone to "cold callers" wanting to "verify numbers."
- Save all credit card receipts and match them against monthly bills.
- Be conscious of routine financial statement due dates and follow up with creditors if bills are late.
- Use caution when posting personal information on social media and use secured websites for purchases.
- Consider using multifactor authentication. This means that at least two forms of identification are required to access an account (e.g., a password or PIN and a challenge question).
- Consider using a password manager program to store, organize, and encrypt multiple passwords.

Below are some "red flag" warnings that someone may be a victim of identity theft:

- Calls or letters from creditors or collection agencies demanding payment for items you never bought.
- Information in your credit file about accounts that you never opened.
- Calls from creditors, or potential creditors, about suspicious new accounts or credit card activity.
- Unauthorized withdrawals from bank accounts.
- A wallet, purse, paycheck stub, or cell phone that is lost or stolen.
- Credit card or phone bills do not arrive on time as regularly scheduled (mail may have been diverted).

Below are recommended steps for victims to clear their good name with creditors and others:

- **Freeze Your Credit-** A credit freeze prevents potential creditors from accessing a credit file, thereby preventing identity thieves from opening accounts in an identity theft victim's name. Credit freeze requests can be made online, by phone, or certified U.S. mail.
- **Change Your Passwords**- Change passwords so identity thieves cannot access accounts for which they have stolen account numbers and other personal identification information.
- **File an Identity Theft Report**- Resources are available at https://www.identitytheft.gov/. The Federal Trade Commission has created an easy system for people to create and update identity theft reports.
- **File a Police Report-** A police report will document that a crime has taken place and may help identity theft victims communicate with credit bureaus, banks, and creditors.
- **Remove Fraudulent Charges-** The Federal Trade Commission (FTC) web site (above) has a sample letter to dispute fraudulent charges made in a victim's name.
- **Close Fraudulent Accounts-** The FTC web site also has sample letters to request that accounts opened in the name of an identity theft victim be closed.
- **Consider Hiring a Credit Monitoring Company**- Monitoring companies use algorithms to scan the entire Internet, including the dark web, for evidence of fraudulent use of victims' personal identification information. Many also provide identity recovery services. Services generally cost $6 to $20 per month.
- **Regularly Monitor Credit Reports**- According to Identity Force (an identity theft monitoring company), most identity theft victims find out that they have been scammed within 3 months but 16% don't find out for three years.
- **Stay on Top of Things and be Persistent-** Cleaning up your credit file will take time and, at times, it will "feel like a full time job." According to the Privacy Rights Clearinghouse, average identity theft victims will spend about 175 hours recovering losses and cleaning up their credit history.

OBJECTIVES

Students will be able to:

- Define identity theft and describe how it occurs.
- Describe strategies they people can take to reduce their risk of becoming an identity theft victim.
- Describe steps that people can take to cope with identity theft and restore their identity.

NEW JERSEY PERSONAL FINANCIAL LITERACY STANDARD

- Standard 9.1.12.E.9: Determine reasons for the increase of identity theft worldwide and evaluate the extent to which victims of identity theft are successful in fully restoring their personal identities. See http://www.state.nj.us/education/aps/cccs/career/FLFAQ.htm#gradcredit and http://www.state.nj.us/education/cccs/2014/career/91.pdf for information about Standard 9.1

TIME REQUIRED

45 to 180 minutes (depending upon student progress and content depth and number of activities used)

MATERIALS

- YouTube Video (6:04): *Secrets of An Identity Thief* https://www.youtube.com/watch?v=WmdyXcfNF2g&t=113s and debriefing questions
- *True or Trick?* activity handout
- Online Quiz: *Are You at Risk for Identity Theft?:* http://www.testq.com/education/quizzes/206-are-you-at-risk-for-identity-theft and debriefing questions
- *What Would You Do?* case study activity handout
- *Web Quest: How to Restore a Stolen Identity* activity handout
- *Identity Theft Quiz* (ASSESSMENT)

Teachers are encouraged to use as many of the student learning activities as time permits to provide a fuller understanding of identity theft. The activities can also be used for extra credit assignments, homework, or after-school activities.

PROCEDURE

1. Ask students to explain what identity theft is and what they know about it. Conclude by telling students that identity theft is an increasingly common white collar crime (i.e., a nonviolent crime without the use of guns, knives, or physical injury to victims), worldwide, and a difficult crime to prosecute.

   Answers will vary. Students will likely note that identity theft is the stealing of personal identification information such as a driver's license, Social Security number, or credit card. They might also tell stories about people they know (e.g., parents) who have been identity theft victims or stories in the news about data hacks (e.g., Equifax in 2017) and the impact of identity theft on victims.

2. **Activity 1:** Show the video *Secrets of an Identity Thief* (ABC News) and debrief the following questions (based on video content) with students:

What are some steps that people can take to avoid exposing their personal data to thieves?

Actions mentioned in the video include not leaving a PIN number in your wallet, avoiding public wifi to transmit sensitive data (e.g., banking transactions), and not leaving valuable items or bags and backpacks that contain valuable items in open view in a car.

How many Americans are affected by identity theft annually?

More than 16 million people are affected by identity theft annually. In a country of 325.7 million people (2017), that is about 5% of Americans annually. Even young children can have their identities stolen. An increasing number of data breaches is a major cause. Identity theft is a common consequence of hackings.

What is the estimated annual cost of the value of identity theft losses?

$24.7 billion

What are some well-known companies whose data was hacked by criminals?

The video mentioned 3 stores: Target, Home Depot, and Saks Fifth Avenue. Other companies that have been hacked include Equifax (credit reporting agency), Anthem (health insurance provider), Sony PlayStation Network (gaming), eBay (online auctions), and Yahoo (website and e-mail provider).

What are some ways that identity theft occurs?

Four specific strategies were mentioned in the video:

- Fake wifi hot spots that people log into for Internet access
- Skimming devices that swipe credit card information onto a card reader
- Stealing wallets and backpacks with wallets or electronic devices from cars (either unlocked cars or cars where windows are smashed when thieves see valuable items inside)
- Stealing mail with sensitive information (e.g., account numbers) from mailboxes

What do identity thieves do with stolen information?

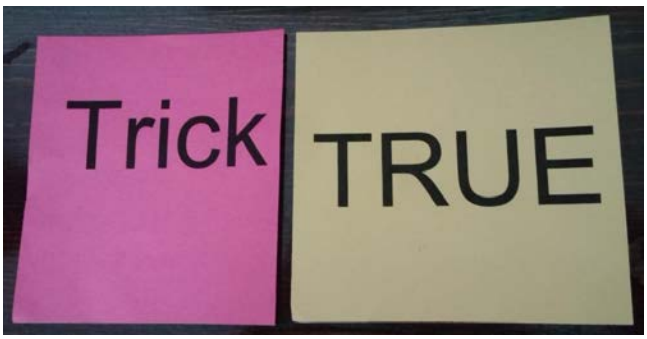
Identity thieves use a victim's good credit history to enrich themselves, They may clean out bank accounts with stolen account numbers and passwords or take over existing credit card accounts to buy items that they subsequently fence (i.e., making transactions with stolen or fraudulently obtained items) or sell.

What can people do to reduce their risk of becoming an identity theft victim?

Four specific strategies were mentioned in the video:

- Get a lock on their mailbox
- Shred important documents
- Get online access for bank and credit card accounts to monitor them frequently
- Protect data on laptops and cell phone with strong passwords

3. **Activity 2:** Distribute the 10-Question *True or Trick?* activity handout to identify myths and incorrect information about identity theft. Read each question and have students decide whether the statement is correct (hold up the *True* card) or false (hold up the *Trick* card). The *True* or *Trick* cards should be printed on different colors of paper or on colored index cards. Debrief each question using descriptions of the correct answers below.



Someone who is diligent about personal security issues can avoid becoming an identity theft victim.
TRICK
Anyone can become an identity theft victim. While it is possible to reduce the risk of becoming victimized by taking proactive measures (e.g., locked mailboxes, multifactor authentication, and shredded documents with sensitive information), everyone is at risk. One reason is data breaches that steal personal information (e.g., full names and Social Security numbers) from company, government, or other organization's records.

There is a good chance that you will become a victim of identity theft during your lifetime.
TRUE
With more than 16 million people affected by some type of identity theft (e.g., *account takeover* where a thief uses an existing credit or debit account or *identity takeover* where a thief opens new accounts in a victim's name), some experts say that many people will experience identity theft at least once.

For many victims of identity theft, their biggest loss is time spent "cleaning up the mess."
TRUE
Many victims spend over 100 hours on identity theft-related tasks including filing a police report, requesting and checking credit reports, sending and replying to e-mails, calling banks and credit card companies, changing passwords, and disputing bogus charges on credit cards. This is not fair but it is reality. Not surprisingly, victims often feel a great deal of stress from both the identity theft itself and its aftermath. Time losses and emotional stress are often more damaging to people than monetary losses.

The least effective method of preventing identity theft is a credit freeze.
TRICK
A credit freeze is a very aggressive strategy to avoid becoming an identity theft victim. Many people decided to freeze their credit after the 2017 Equifax hack exposed the personal information of 145.5 million people. This information included names, addresses, credit card numbers, and Social Security numbers. A credit freeze prevents potential creditors from accessing a credit file, thereby preventing identity thieves from opening accounts in an identity theft victim's name. It is considered one of the best things that people who have had their information hacked can do to protect their identity.

Multifactor authentication is not necessary to use unless you are an identity theft victim.
TRICK
Multifactor authentication can help prevent identity theft because it requires at least two forms of identification to access an account. Typically, a password is the first form of identification and the second form of identification can be a challenge question, thumbprint, PIN number, or digital PIN number that is sent to an account owner's phone via text messaging. Everyone with information that can be hacked online should consider using multifactor authentication to enhance the security of their accounts.

Identity thieves can steal information from a victim's garbage can.
TRUE
Stealing documents with sensitive information (or anything) from a garbage can is known as "dumpster diving." This is a low-tech method of identity theft (vs. hacking online databases), but it still occurs. This is why it is important to shred bank and brokerage account statements, old tax returns, and old checkbooks.

The easiest way to avoid tax refund identity theft is to file your taxes early.
TRUE
Tax refund identity theft occurs when a thief files a fraudulent tax return in a victim's name using stolen information. While filing a tax return early can't prevent criminals from filing a fraudulent tax return in a victim's name, it may enable victims to beat criminals to their money. Otherwise, months of delays are likely while the IRS investigates why two people filed with the same name and Social Security number.

Account takeover is a more common form of identity theft than identity takeover.
TRUE
Account takeover means that an existing bank or credit card account that is owned by a victim is taken over by a thief. For example, a checking account can be depleted with a stolen debit card and fraudulent purchases can be made on a stolen credit card. The other form of identity theft, *identity takeover*, is where criminals open a new account fraudulently in a victim's name.

The Consumer Financial Protection Bureau is the government agency that has sample victim letters.
TRICK
The Federal government agency that is leading the development of identity theft recovery resources, including sample letters to dispute fraudulent charges and close fraudulent accounts, is the Federal Trade Commission (FTC). Consumers can access these materials at www.identitytheft.gov. This web site also includes detailed information about steps to take for victims of fraud.

Identity theft can have a lasting effect on a victim's financial, physical, and emotional well-being.
TRUE
It is not uncommon for victims to say that they feel "violated" whether identity theft occurs through low-tech (e.g., dumpster diving) or high-tech (e.g., online data breach) methods. In some instances, the thief is even a parent, friend, or co-worker that the victim knows. Victims may experience fear, anxiety, insomnia, and other physical effects of stress and become withdrawn and isolated.

4. **Activity 3:** Ask students to take the *Are You at Risk for Identity Theft?* online quiz, which consists of 10 questions and classifies respondents into three categories: Guard Tower (people who take some security measures), Iron Fortress (people who have very secure practices), and Open Door (people with very poor security practices). If some questions do not apply to students' lives now, tell them to indicate what they would do in each situation. Debrief the activity (e.g., areas of strength and weakness; e.g., a locked mail box), using the handout, and discuss students' identity theft risk classification categories.

5. **Activity 4:** Distribute the *What Would You Do?* case study activity handout. Ask students to read the case study and work together to answer the questions that follow. Debrief the activity.

Sarah Coats just received her first credit card. It is a retail store card with a $200 limit. Should she carry it around with her on a daily basis or just when she goes shopping and might use it?

Since the credit card likely can't be used anywhere else but the retail store, there is no need to carry it around on a daily basis. Rather, she can leave it at home in a secure location (e.g., locked desk drawer) to reduce the risk of having it be lost or stolen. Another benefit is reduced temptation to overspend.

A year later, after handling her retail store credit card responsibly, Sarah applies for, and receives, a Visa bankcard. Should she carry this credit card around with her on a daily basis?

Yes. The credit card will be useful in the event of emergencies (e.g., a flat tire). In addition, if she wants to earn rewards for purchases, she will need to have the credit card with her for everyday purchases (e.g., collecting rewards for purchases such as groceries and gas). The credit card should be kept securely in a wallet, purse, or other place where Sarah carries important personal items.

Sarah gets a roommate to help cover her expenses. They will share some common living areas and there will be times when the roommate will be there without Sarah. She does not know the roommate very well. What can Sarah do to secure her personal identification information?

Sarah should place all of her personal information under lock and key. This may include a locked door to her private living area, a locked desk drawer, a locked file box, and/or a home safe. She should also put strong passwords on her computer, tablet, cell phone, and other electronics and make sure that she does not leave mail with sensitive information lying around. She might also want to discontinue mailed statements for bank accounts and credit cards and receive all of her account information online.

Sarah stops by the retail store and finds a bargain, but her credit card is at home. The store clerk says that her account number can be accessed with her Social Security number. Three people are standing in line behind her within earshot. How can she safely provide the required information?

Under no circumstance should Sarah say her Social Security number out loud where other people in line can hear it. Some stores have shielded keypads where customers can securely type in their credit card number. Another option is to write it on a slip of paper, hand it discretely to the store clerk, and immediately rip it up when the clerk has entered her data. Other options are to simply not buy the item or to ask the store clerk to hold the planned purchases until she can return to the store with her credit card.

Sarah receives an e-mail from someone claiming to be from the department store. They are asking Sarah to click on a link to verify her credit card account number. What should she do?

Do not respond to this message. Simply delete it. Stores already have their customers' credit card account information on file so this is a "red flag" indicator of an identity theft scam or a computer malware scam. She may want to call the department store to alert them and to find out if others have received similar e-mails. Some people may also contact their local police department for advice and assistance.

Sarah is meeting friends at a concert hall to go dancing and she is concerned that her purse may not be secure the entire time that she is out with friends. What should she do to reduce the risk of having her personal information stolen?

Leave the purse at home and carry as little personal information as possible (e.g., with a fanny pack or a sweater with big pockets) on her person: an ID card, driver's license, and the credit card for emergencies. Another option would be to take her purse and lock it in her car trunk while she is inside at the venue dancing. It is not smart to leave a purse unattended on the back of a chair. Anyone could come by and steal her credit card, driver's license, or other personal information and misuse it.

Sarah receives her credit card statement and sees three charges for purchases that she did not make. She is very upset and not sure what to do. What steps should Sarah take to deal with the situation?

Step #1 is to immediately contact the credit card company, using their Customer Assistance telephone number, to explain the fraudulent charges. If a credit card is lost or stolen, the highest amount that victims are responsible for paying is $50 of fraudulent charges if someone misuses their credit card before the theft is reported. Many creditors have zero-liability policies, however, and do not hold their customers responsible for any payment. If a loss is reported before a credit card is misused, there is also no financial liability. However, credit card customers, collectively, pay for fraudulent charges through the interest and fees that are charged to everyone. Identity theft fraud is a "cost of doing business" for creditors.

Step #2 is to change the password and/or PIN for online access to the credit card account to avoid additional access by identity thieves. An even better option would be to have the credit card company close the misused account completely and reissue a new credit card with a new account number.

Step #3 is to closely monitor her credit card account for evidence of additional fraudulent purchases. Sarah should also request a free copy of her credit report and review it for evidence of additional identity theft.

Step #4 is to consider placing a fraud alert in her credit report to require creditors to take steps to verify her identity before a new account is opened or an additional card, or a higher credit limit, is issued on an existing credit card. This is done by contacting one of the "Big Three" national credit reporting companies (Experian, Equifax, and TransUnion). Initial fraud alerts expire after 90 days and extended fraud alerts last seven years. Although the main concern in this case is with an existing account, an even more aggressive response would be for Sarah to freeze her credit to prevent new accounts from being opened in her name,

6. **Activity 5:** Distribute the *Web Quest: How to Restore a Stolen Identity* activity handout and ask students to conduct an online search to find information from reputable sources (e.g., the Federal Trade Commission, the Consumer Financial Protection Bureau, newspapers) without a commercial interest (e.g., identity theft monitoring companies) about steps that victims should take to restore a stolen identity. Have students search for three articles and list key take-aways from the articles on the handout.

Answers will vary but students are likely to report the following key pieces of information:

- *There are commercial companies that can help people restore their good credit history, but they are expensive and their quality can vary. "Do-It-Yourselfers" can expect to spend many hours dealing with paperwork, phone calls, and e-mails and the restoration process can be emotionally draining.*
- *Send photocopies of requested documents by certified mail, return receipt requested.*
- *Keep good notes of all contacts with creditors, police, credit reporting agencies, financial institutions, and others including dates, times, phone numbers, and the names of contact persons.*
- *Track how much time and money you spend to clear up the problem in case the thief gets caught and you are able to receive restitution.*

CLOSURE

Ask students if they have any remaining questions about identity theft. Remind them that, given the prevalence of data hacks, they will need to be vigilant about identity theft for the remainder of their lives.

GLOSSARY

Account Takeover- The most common form of identity theft, where a thief misuses an existing credit or debit account belonging to a victim (e.g., making fraudulent purchases with a victim's credit card number).

Credit Freeze- A credit freeze prevents potential creditors from accessing a person's credit file, thereby preventing identity thieves from opening accounts in an identity theft victim's name. This is because most creditors need to see an applicant's credit report before they approve a new account. If they can't access an applicant's credit file, they generally will not extend credit.

Crosscut Shredder- A type of shredder that cuts paper into very fine pieces (as opposed to long strips) that are virtually impossible to reassemble. Shredders are used to destroy documents with confidential information or sensitive personal identification information.

Dark Web- A section of the World Wide Web (Internet) that is only accessible with special software. It is a place where online users and website operators go to remain anonymous and to have their data be untraceable, often for criminal purposes.

Fraud Alert- A notice that is sent to a credit reporting bureau (i.e., Equifax, Experian, and TransUnion) to alert them that a consumer's identity may have been stolen and that requests for new credit in the consumer's name may be fraudulent. Consumers must submit proof of their identity when requesting a fraud alert and are entitled to a free copy of their credit report from each credit bureau.

Hacking- Gaining unauthorized, illegal access to data housed in a single computer or a computer network.

Identity Takeover- A form of identity theft, less common than account takeover, where criminals fraudulently open a new account in a victim's name.

Identity Theft- Stealing another person's personal identification information (e.g., Social Security number and bank account number) and using it for personal gain. Identity theft is not typically a "stand-alone" crime but, rather, part of another crime such as bank account, credit card, or health insurance fraud.

Multifactor Authentication- Two forms of identification required to access an online account. Typically, a password is the first form of identification and the second form of identification can be a challenge question, thumbprint, PIN number, or digital PIN number that is sent to an account owner's phone via text messaging. Multifactor authentication is used to reduce unauthorized access to online accounts.

Phishing- The practice of prompting people to divulge sensitive personal information to commit identity theft by sending fraudulent e-mails that purport to come from reputable companies.

PIN (Number)- An acronym for "personal identification number," a PIN is a combination of numbers, or numbers and letters combined, that is used as a form of identity authentication for online accounts.

Skimming- The practice of fraudulently capturing credit card information using a skimmer (a.k.a., cardreader), which is a device that captures and stores details stored in a credit card's magnetic stripe.

Spear Phishing- A more personalized, targeted form of phishing where requests to divulge personal information are directed at a specific individual or organization about which information is known.

Spyware- Maliciously installed software (i.e., malware) that enables criminals to obtain sensitive data from a victim's computer without the victim's knowledge.

LEARNING EXTENSIONS

If time permits, the following activities can be used to extend the depth of this lesson:

- Invited an identity theft victim or local law enforcement agency representative as a guest speaker to discuss their first-hand experiences with identity theft.

- Show one or more of the following videos about identity theft:

  - *Why Care About Identity Theft?* (Federal Trade Commission): https://www.youtube.com/watch?v=k3yh9hjnE44
  - *Identity Theft* (10-minute *60 Minutes* segment): https://www.youtube.com/watch?v=kQdDKg0N1DE&t=24s
  - *Common Ways Identity Theft Happens* (FTC): http://www.youtube.com/watch?v=-IEBVIh7bzc
  - *Identity Theft* (Victims' Stories): http://www.youtube.com/watch?v=OoPJImjP1ZQ
  - *5 Ways to Protect Your Identity* (Federal Trade Commission): https://www.youtube.com/watch?v=lp_8cvNm_vE
  - *Identity Theft Prevention* (Kaspersky Lab): https://www.youtube.com/watch?v=Fztuohj3Fck
  - *Victims of ID Theft: 5 Steps to Take* (Bank of America): https://www.youtube.com/watch?v=QizfpGI7acE
  - *Medical Identity Theft* (ABC News): https://www.youtube.com/watch?v=EePx7STsnOI
  - *Identity Theft Commercial* (CitiBank): https://www.youtube.com/watch?v=KERwnA8VfFM
  - *How to Spot a Phishing Scam* (Trend Micro): https://www.youtube.com/watch?v=pXp2RvA0SBU
  - *Phishing Scams in Plain English* (Commoncraft): https://www.youtube.com/watch?v=aIBHCUNVm5Y
  - *What is Phishing?* (AARP Academy): https://www.youtube.com/watch?v=WpaLmeHTp3I
  - *Guide to Scary Internet Stuff- Phishing* (Symantec): https://www.youtube.com/watch?v=v3JGY2L8NK4

- Have students take the Rutgers Cooperative Extension *Identity Theft Risk Assessment Quiz* at https://njaes.rutgers.edu/money/assessment-tools/ and debrief their responses.

- Add additional content to your class discussion of identity theft from the following lesson plans:

  - *Identity Theft and Phishing Scams* Lesson (TD Bank): https://www.tdbank.com/wowzone/lessons/Gr9-12Lesson10.pdf
  - *ID Theft and Account Fraud: Prevention and Cleanup* Lesson Plan (Consumer Action): http://www.consumer-action.org/downloads/english/ID_Theft_Lesson_2014.pdf

- Use lessons, activities, projects, case studies, and other interactive materials on identity theft developed by Next Gen Personal Finance: https://www.ngpf.org/curriculum/financial-pitfalls/ (Click on Scams, Fraud, and Identity Theft).

- Have students write a brief reaction paper, blog post, or newspaper article on what they learned about identity theft and how they plan to apply this information in their lives.

- Have students work in small groups to create skits about identity theft involving victims and thieves.

ASSESSMENT: *Identity Theft Quiz*

Instructors are encouraged to use the questions below for content review or as a pre-and/or post-test to determine gains in student knowledge about identity theft after teaching this lesson.

Correct answers to the multiple choice and True-False questions are shown in boldface type.

Multiple Choice Questions

1. For many victims of identity theft, their biggest loss comes from
   a. Time spent resolving fraudulent transactions made in their name
   b. Money stolen from bank accounts
   c. Credit card penalties
   d. Debit card fees

2. Which of the following is *not* a form of identification used for multifactor authentication?
   a. PIN number
   b. Code number texted to a cell phone
   c. Signature
   d. Challenge question

3. The low-tech strategy of stealing personal identification information from garbage cans is known as
   a. Garbage picking
   b. Dumpster diving
   c. Trash sorting
   d. Refuse rummaging

4. The process of not allowing potential creditors to access your credit file is known as a
   a. Credit lock
   b. Fraud alert
   c. Identity shield
   d. Credit freeze

5. What federal government agency has a comprehensive web site with multiple resources to assist identity theft victims?
   a. Consumer Financial Protection Bureau (CFPB)
   b. Federal Trade Commission (FTC)
   c. U.S. Treasury Department
   d. U.S. Department of Commerce

True-False Questions

1. An initial fraud alert that is sent to a credit reporting company lasts for 30 days.
   (FALSE: Initial fraud alerts sent to credit reporting companies remain on file for 90 days. An extended alert that lasts for seven years can also be requested by identity theft victims)

2. Multifactor authentication means that an account requires at least two forms of identification to access **(TRUE: Typically, the first form of identification is a password and the second form could be a PIN number, a digital PIN sent by texting to a cell phone, or one or more challenge questions. The challenge questions should not be about information that someone has been shared online)**

3. Identity theft is one of the most common consequences of data breaches **(TRUE: According to the identity theft monitoring company, Identity Force, 31% of data breach victims experienced some type of identity theft. Therefore, the chances of being a victim of this crime are very high once your personal data is hacked. This warrants proactive action to be vigilant about reducing your risk of loss and monitoring for possible instances of identity theft)**

4. Identity theft can impact victims long after the actual theft incident occurred **(TRUE: Some identity thieves steal large amounts of data and may "lie in wait" and take years to misuse a specific individual's personal data. In addition, the emotional trauma aspects of identity theft- feeling violated-may take a long time for victims to overcome)**

5. People need to pay a fee to check their credit report to look for evidence of identity theft **(FALSE: Under federal law, Americans are entitled to request a free credit report annually (i.e., every 365 days) from each of the "Big Three" credit reporting agencies: Experian, Equifax, and TransUnion. In addition, when identity theft victims file a fraud alert, they can also request a free copy of their full credit report to check for fraudulent accounts. This free report is in addition to the free report available annually to all consumers from the web site** www.annualcreditreport.com**)**

REFERENCES AND RESOURCES

How Long Does It Take to Recover from Identity Theft? (Identity Hawk): http://www.identityhawk.com/identity-theft-recovery-time/

How Much Time Does Identity Theft Recovery Take? (Identity Force): https://www.identityforce.com/blog/how-much-time-does-identity-theft-recovery-take

Identitytheft.gov (Federal Trade Commission): https://www.identitytheft.gov/

Identity Theft: A Recovery Plan (Federal Trade Commission): https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf

Recovering from Identity Theft (Consumer.gov): https://www.consumer.gov/articles/1016-recovering-identity-theft

The Ultimate Guide to Identity Theft Protection (CentSai): https://centsai.com/ultimate-guides/the-ultimate-guide-to-protecting-against-identity-theft/

What Do I Do if I Think I Have Been a Victim of Identity Theft? (Consumer Financial Protection Bureau): https://www.consumerfinance.gov/ask-cfpb/what-do-i-do-if-i-think-i-have-been-a-victim-of-identity-theft-en-31/

What to Do Right Away (Federal Trade Commission): https://www.identitytheft.gov/steps

Secrets of an Identity Thief
Debriefing Questions

After watching the video *Secrets of an Identity Thief*, answer the following questions:

What are some steps that people can take to avoid exposing their personal data to thieves?

How many Americans are affected by identity theft annually?

What is the estimated annual cost of the value of identity theft losses?

What are some well-known companies whose data was hacked by criminals?

What are some ways that identity theft occurs?

What do identity thieves do with stolen information?

What can people do to reduce their risk of becoming an identity theft victim?

True or Trick?

Instructions:

Answer the questions below and be prepared to defend your responses during the class discussion.

Someone who is diligent about personal security issues can avoid becoming an identity theft victim.

There is a good chance that you will become a victim of identity theft during your lifetime.

For many victims of identity theft, their biggest loss is time spent "cleaning up the mess."

The least effective method of preventing identity theft is a credit freeze.

Multifactor authentication is not necessary to use unless you are an identity theft victim.

Identity thieves can steal information from a victim's garbage can.

The easiest way to avoid tax refund identity theft is to file your taxes early.

Account takeover is a more common form of identity theft than identity takeover.

The Consumer Financial Protection Bureau is the government agency that has sample victim letters.

Identity theft can have a lasting effect on a victim's financial, physical, and emotional well-being.

Are You at Risk for Identity Theft?
Debriefing Questions

Instructions:

Take the online quiz at http://www.testq.com/education/quizzes/206-are-you-at-risk-for-identity-theft and answer the following questions.

What was the rating of your identity theft risk reduction practices on the online quiz: Open Door, Guard Tower, or Iron Fortress?

Why do you think you received this rating?

List five identity theft risk reduction actions that you could take to reduce your chances of becoming a victim.

1.

2.

3.

4.

5.

Case Study: What Would You Do?

Sarah Coats just received her first credit card. It is a retail store card with a $200 limit. Should she carry it around with her on a daily basis or just when she goes shopping and might use it?

A year later, after handling her retail store credit card responsibly, Sarah applies for, and receives, a Visa bankcard. Should she carry this credit card around with her on a daily basis?

Sarah gets a roommate to help cover her expenses. They will share some common living areas and there will be times when the roommate will be there without Sarah. She does not know the roommate very well. What can Sarah do to secure her personal identification information?

Sarah stops by the retail store and finds a bargain, but her credit card is at home. The store clerk says that her account number can be accessed with her Social Security number. Three people are standing in line behind her within earshot. How can she safely provide the required information?

Sarah receives an e-mail from someone claiming to be from the department store. They are asking Sarah to click on a link to verify her credit card account number. What should she do?

Sarah is meeting friends at a concert hall to go dancing and she is concerned that her purse may not be secure the entire time that she is out with friends. What should she do to reduce the risk of having her personal information stolen?

Sarah receives her credit card statement and sees three charges for purchases that she did not make. She is very upset and not sure what to do. What steps should Sarah take to deal with the situation?

Web Quest: How to Restore a Stolen Identity

Use an online search engine (e.g., Google, Bing) to search for words like “identity theft recovery” and “identity theft victim.” Find three articles from government agencies or non-profit-organizations without a commercial interest (e.g., identity theft monitoring companies) about steps that people should take to restore a stolen identity. List key take-aways from each of the articles in the spaces below.

Information Source	**Information About Identity Theft Recovery**

Identity Theft Quiz

Multiple Choice Questions:

Circle the correct answer from among the four answers provided.

1. For many victims of identity theft, their biggest loss comes from
   a. Time spent resolving fraudulent transactions made in their name
   b. Money stolen from bank accounts
   c. Credit card penalties
   d. Debit card fees

2. Which of the following is not a form of identification used for multifactor authentication?
   a. PIN number
   b. Code number texted to a cell phone
   c. Signature
   d. Challenge question

3. The low-tech strategy of stealing personal identification from garbage cans is known as
   a. Garbage picking
   b. Dumpster diving
   c. Trash sorting
   d. Refuse rummaging

4. The process of not allowing potential creditors to access your credit file is known as a
   a. Credit lock
   b. Fraud alert
   c. Identity shield
   d. Credit freeze

5. What federal government agency has a comprehensive web site with multiple resources to assist identity theft victims?
   a. Consumer Financial Protection Bureau (CFPB)
   b. Federal Trade Commission (FTC)
   c. U.S. Treasury Department
   d. U.S. Department of Commerce

True-False Questions:

Mark "T" for True or "F' for False in the space before each question.

____1. An initial fraud alert that is sent to a credit reporting company lasts for 30 days.

____2. Multifactor authentication means that an account requires at least two forms of identification to access.

____3. Identity theft is one of the most common consequences of data breaches.

____4. Identity theft can impact victims long after the actual theft incident occurred.

____5. People need to pay a fee to check their credit report to look for evidence of identity theft.

The *Identity Theft:Risks and Recovery* lesson plan was written by Dr. Barbara O'Neill, CFP®, Extension Specialist in Financial Resource Management for Rutgers Cooperative Extension (boneill@njaes.rutgers.edu).

Publication Date: June 2018

This publication was supported with funding provided via August 2011 legislation, (N.J.S.A. 17:9-43.2.D) that authorizes New Jersey credit unions to serve as public depositories for the purpose of promoting personal financial literacy education.