LESSON SIX: IDENTITY THEFT

PROTECTING YOUR IDENTITY

Lesson 6: Identity Theft
PROTECTING YOUR IDENTITY

- Students will learn the dangers of ID theft, and what to do if your ID has been stolen
- We'll talk about simple and easy ways to protect your ID and sensitive information

Protecting Your Identity

Identity theft occurs when a person's financial or personal information is taken for the sole purpose of assuming that person's identity to make transactions or purchases. In the USA alone, there are approximately 15 million identity fraud victims every year.

The states with the highest rate of identity theft complaints in 2015, per 100,000 victims, are:

Missouri: 364.3	Connecticut: 225	Florida: 217.4
Maryland: 183.2	Illinois: 158.7	

Identity Theft Can Happen to Anyone, Anywhere

Identity theft can happen in person and over social media, to the young and old. It occurs in any industry and can even happen to the deceased! Some ways your identity can be stolen include:

Skimming: Stealing credit card or debit card numbers with a special device when processing your card.

Phishing: Pretending to be banks, the IRS or some other organization and sending emails or a letter asking for personal information.

Changing Your Address: Completing a change of address card/form and creating a new address for you so they can receive your billing statements. Once they have the statements, they can access your account.

Stealing: Stealing money, purses, or even mail with bank or credit card statements or tax information.

Pretexting: Using false information to get your personal information from financial institutions, telephone companies, and other sources. Criminals pretend to be you to get the information, then use it against you or sell it to someone else to use.

Hacking: Accessing your computer or a financial institution's computer system to get personal information.

Litchfield Bancorp ACADEMY

Common Forms of Identity Theft Include:

- Credit card fraud
- False applications for new credit
- Fraudulent withdrawals from a bank account
- Fraudulent use of telephone calling cards
- Fraudulent use of an IP address to engage in illegal acts online
- Fraudulent use of medical care
- Social security fraud (for tax and employment fraud)

Cost of Identity Theft

Unfortunately, identity theft carries a heavier weight than just someone using your name. Identity theft can result in difficulty in applying for a credit card or a loan, getting a job, clearing negative information on records, or an inability to trust other people.

What to do if you think your Identity has been stolen

1. Put a Fraud Alert on Your Credit Reports

A fraud alert puts a red flag on your credit report and notifies lenders and creditors that they should take extra steps to verify your identity before extending credit. To place a 90-day fraud alert on all three of your credit reports, you only need to contact one of the three credit reporting agencies (Experian, Equifax, or TransUnion). When you place the initial alert, they will automatically notify the other two agencies for you.

2. Contact Any Institution Directly Affected

For example, if you know your credit card was stolen, report the theft to the credit card issuer. If your checkbook was stolen, contact your bank.

For this step, it's helpful if you've prepared a list of institutions and phone numbers in advance. You don't have to write account numbers down on the list - that would be just one more way for a thief to gain access to your personal information. But do keep a list of what's in your wallet, along with the contact information for each item.

Contact the Federal Trade Commission (FTC)

File an Identity Theft Affidavit and create an Identity Theft Report. You can file your report online, by phone (toll-free): 1-877-ID THEFT (877-438-4338). The FTC will provide you with information about what to do next, depending on what type of fraud was, or may have been, committed.

4. File a Police Report

To complete the Identity Theft Report, you'll need to contact your local law enforcement office and report the theft. Be sure to get a copy of the police report and/or the report number. Both your police report and the FTC Identity Theft Affidavit are combined to create your Identity Theft Report. Your Identity Theft Report will help you when working with the credit reporting agencies or any other companies the identity thief may have used to open accounts in your name.

5. Protect Your Social Security Number

If your social security number was or may have been compromised, contact the Social Security Administration (SSA, 800-269-0271) and the Internal Revenue Service (IRS, 800-829-0433).

It's important to talk to the SSA if you have reason to believe your social security number has been compromised, even if you don't yet see any evidence of financial fraud. A thief could be planning to swipe your tax refund or to obtain employment in your name.

Simple Ways to Protect Yourself from Identity Theft

Guard Important Personal Documents

Never carry your social security card in your wallet or give this information out freely. Those nine personalized digits can mean a bad case of identity theft if they fall into the wrong hands. Keep any documents or statements with your personal information in a safe place. If you no longer need them, shred them.

Beware of "Shoulder Surfers"

Keep watch over your debit or credit cards whenever making a transaction. Even at the most seemingly secure location, you never know who might be looking over your shoulder. Thieves have even been known to install tiny cameras, credit card skimmers, and even use binoculars from afar to catch a glimpse of your card.

Protect Your Digital Presence

Your home computer or laptop might just be the most vulnerable to identity thieves. Make sure you have firewalls, anti-virus software, and/or an anti-spyware programs installed on your devices to protect it while you're online. Even If your computer has never been compromised, it's also good to frequently change your passwords, whether they're for your bank account, social media, or another site. Use a password that's hard to guess that contains letters, numbers, and symbols. AND NEVER SHARE YOUR PASSWORDS WITH FRIENDS OR FAMILY!

Be Wary of Fishy Phishing Scams

Open your emails and text messages carefully. Many that look harmless and legitimate are scams in disguise, out to fool people into giving up their personal information. several phishing scams look real, posing as scholarship offers, discount deals, correspondence from fictitious organizations, or even communications from your own bank. Never give out account information over email – that is a sure sign of a scam.

Check Your Credit Report

If you don't already, start checking your credit report at least once a year to see where you stand financially - especially if you're thinking about taking out a loan, buying a car, or opening a new credit card. Look for any fraudulent activity in your accounts, or for open accounts you may not recognize. If people have been racking up debt on your dime, you need to know.

IDENTITY THEFT ACTIVITY

Based on the information you learn today, please answer the following questions.

1. Explain three methods used to steal your identity.

2. List five different steps you should take to protect your identity.

   1. _____

   2. _____

   3. _____

   4. _____

   5. _____

3. What should you do if you become a victim of identity theft?

Match the following terms to the scenarios. Place the letter of the correct term in the blank in front of the scenario.

A. Changing your address B. Skimming C. Stealing D. Hacking E. Phishing

____ 1. Janet has not received a credit card statement for three months, even though she has been using her credit card. She calls the company and is told that her bill was sent to her and now her account is overdue. What term describes why Janet did not receive her bill?

____ 2.Karen received an email telling her that her PayPal account may have been compromised and that she needs to confirm her login and password via email to make sure her account is safe. She clicked on the link in the email and is directed to a site that looks legitimate so she complied with the request. Soon after she supplied the information, she received several emails from PayPal confirming several purchases she had not made. What term describes what happened to Karen?

____ 3. Angie's grandmother paid for dinner with a credit card. The waitress brought her back the card and she signed the receipt. Angie notices on her grandmother's next statement several charges that her grandmother had not made. What term describes what the waitperson did?

____ 4. Charlie wants a new skateboard but doesn't have the money to buy it. He decided to take his father's credit card and order one online, thinking that he will pay his father back when he has the money. What term describes what Charlie did?

____ 5. Brandy is a computer geek with very advanced skills. She can access computers across the internet that belong to other people. She can log in and obtain Mrs. Smith's bank and credit card account numbers and uses them to order items from Ebay. What term describes what Brandy is doing?