



Lesson 10: Protecting Yourself

WHAT IS IDENTITY THEFT

Use with *Learning About Identity Theft Stations* activity. One copy per station.

WHAT IS IDENTITY THEFT?

Identity theft is the crime of using another person's name, credit or debit card number, Social Security number, or another piece of personal information to commit fraud, typically for economic gain.

Identity theft can take many forms. It's important to consider some common scams and take preventive action to protect yourself.



Beware of phishing scams.

Phishers send out text and email messages trying to get you to click on links and share personal information. These might look like they are from companies you recognize.



Protect your passwords.

Don't save your passwords on public computers or share passwords with friends.



Watch out for malware.

It's important not to download programs or open links in strange emails because they may contain computer viruses.

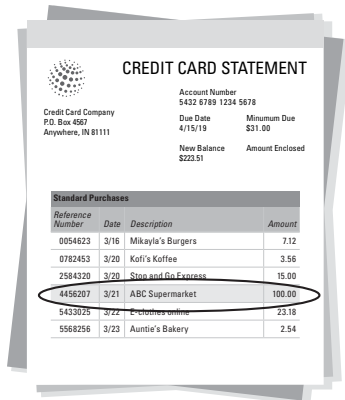
Source: www.common sense media.org/blog/the-bare-minimum-you-should-do-to-protect-your-familys-data



Lesson 10: Protecting Yourself YOU'VE BEEN SCAMMED!

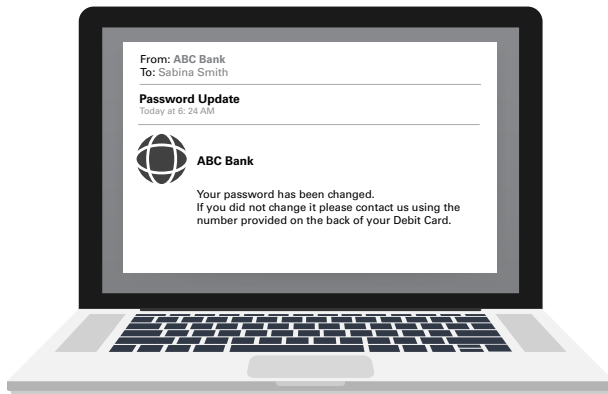
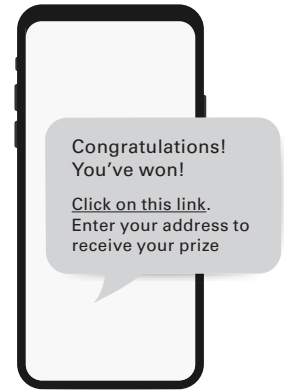
Use with *Learning About Identity Theft Stations* activity. One copy per station.

What Does it Look Like When You've Been Scammed?



Charges on your credit or debit account that you did not authorize:

Responding to online, text, or phone requests for personal information without being sure they are secure:



Receive an email letting you know your password has been changed when you did not change it.

Receive a text message saying your favorite store needs you to update your address



“Phishing” is an attempt to acquire personal information by pretending to be a trusted agency.



Lesson 10: Protecting Yourself

PREVENTING IDENTITY THEFT

Use with *Learning About Identity Theft Stations* activity. One copy per station.

STINGY!

Be stingy about giving out your personal information, both in person and online. If someone from a reputable financial institution or company calls to acquire personal data, ask him or her to send you a written application.

CHECK!

Check your financial information regularly. You should receive monthly statements on all bank and credit card accounts that list your most recent transactions. If you aren't receiving your monthly statements, call the bank right away. Check your statements thoroughly to make sure there are no unauthorized withdrawals or charges.

ASK!

Ask periodically for a copy of your credit report. Your credit report should list all bank and financial accounts under your name, and will provide other indications of whether someone has wrongfully opened or used any accounts in your name. You can obtain one free credit report from each of the credit bureaus once every 12 months. Get your free credit report from each of the three major nationwide credit bureaus at www.annualcreditreport.com.

MAINTAIN!

Maintain careful records of your banking and financial accounts. Financial institutions are required to maintain copies of your checks, debit transactions, and similar transactions for five years, but you should, too, for at least one year. If you need to dispute a transaction, your original records will be accessible and useful when you argue against it.



Lesson 10: Protecting Yourself

I'VE BEEN SCAMMED! NOW WHAT?

Use with *Learning About Identity Theft Stations* activity. One copy per station.

- **If you are receiving texts or emails asking for personal information or that seem fraudulent, tell your parents.**
- **If you notice your social media accounts have posts you did not make, change your password and ask your parent or guardian to help report it on the website.**
- **Contact the credit reporting companies and place a free fraud alert on your credit file.** This can make it harder for an identity thief to open more accounts in your name.
- **Check your bank and other account statements for unusual activity.** Look at your monthly statements to determine fraudulent transactions.
- **Get a free copy of your credit report.** Visit www.annualcreditreport.com.
- **Consider requesting a credit freeze.** This means that potential creditors cannot get your credit report and it makes it less likely that an identity thief can open a new account in your name. This does not affect your credit score.
- **Create an identity theft report.** This helps you get fraudulent information removed from your credit report and stop a company from collecting debts that are a result of identity theft.



Lesson 10: Protecting Yourself

IDENTITY THEFT ROLE-PLAY CARDS

Use with *Learning About Identity Theft Stations* activity. One copy per group.

| | |
|---|---|
| Scenario #1, Role A | Scenario #1, Role B |
| You open up your latest bank statement to discover that there are several transactions on it that you did not authorize. You decide to make a call to the customer service branch of your bank. | You are a customer service representative at the bank. You regularly field calls from customers at your bank who believe that they have been the victims of identity theft. |
| Scenario #2, Role A | Scenario #2, Role B |
| You recently purchased several items from a store that has just suffered a security breach. This means that some identity thieves hacked into the store's credit and debit card readers and stole bank account information. You are unsure about what to do and you seek the advice of a trusted friend. | You are considered trusted and knowledgeable about finances by all of your friends. Offer your friend advice about what to do if he or she feels that she has been the victim of identity theft, and about protecting herself against identity theft in the future. |
| Scenario #3, Role A | Scenario #3, Role B |
| You've just learned about identity theft and how to protect yourself. When you get home from school, you realize that your parent or caretaker has thrown away unopened bills, responded to an unknown email address requesting personal information, and left computer passwords out on the table. Talk to your parent or caregiver about taking precautions against identity theft. | You are a busy parent or caretaker who doesn't have time to make sure that everything is perfect in life. Sometimes you forget to save your bills, or shred personal information before throwing it away. Nothing bad has ever happened in the past and you're not worried about anything bad happening in the future. |
| Scenario #4, Role A | Scenario #4, Role B |
| You are at the grocery store, shopping for some items for dinner, when another person strikes up a conversation with you about some financial trouble that he or she has been having. Give financial advice to this person. | This is a special role. Person A thinks that you are just a regular person looking for advice about some financial trouble that you've been having, but in reality, you are an identity thief trying to steal their personal information. See if you can talk Person A into giving you personal information, but be sneaky! |