STUDENT LEARNING PLAN

Lesson 2-5: Identity Fraud

OVERVIEW

Everyone needs to take precautions to protect personal information from being used by others without permission. Identity theft and fraud are big business—costing victims, companies, and governments billions of dollars a year. Even if you are able to fix a fraud problem without losing money, it will take you more time than you want to spend to gather evidence and inform others about the issue.

This lesson will help you plan ways to protect yourself from being a victim of identity fraud.

LEARNING OUTCOMES

In this lesson you will take steps to protect yourself from identity fraud. Along the way you will:

- ☑ Give examples of identity fraud.
- ☑ Describe how to address problems of fraud.
- ☑ Identify ways to protect against fraud.

Use what you learn to take action to keep your personal information safe.

LEARNING TASKS These tasks match pages 34-38 in Student Guide 2.	
__ 1.	Participate in a scavenger hunt activity.
__ 2.	Read about what happened to Jesse's dad (page 34). Participate in a discussion about ways people are victims of identity fraud.
__ 3.	Share experiences about how you protect your personal information. Complete **Activity 2.10: Take Preventive Action** to evaluate how you protect your data.
__ 4,	Guess what—Mariah has lost her new credit card! She has confided in you but tells you not to worry—she's sure it will turn up soon. She doesn't want to tell her mom for fear she will freak out and not allow her to ever have a credit card. What would you tell Mariah to do?
__ 5.	Put up your own shield to protect yourself from identity fraud. A. Create a checklist of at least five actions you will take, starting now, to protect your personal data. B. Over the next week, document evidence that you have carried out the actions.

EXTENSION

Host a "Protect Your Identity Day" for parents and community members. Use the Federal Trade Commission's toolkit as a guide to plan and host this event.

TAKING IT HOME

Test your family's ID theft savvy by playing the Identity Theft Face Off game hosted by the Federal Trade Commission. Choose a character whose identity has been stolen—literally!

TAKING IT HOME

How safe are you online or when you use a computer? If you have a computer at home, check your online privacy settings and your systems security with this checklist:

- ❑ Your computer files are backed up on a regular basis.
- ❑ Your Internet security level is set to "High" or "Medium High."
- ❑ Your Internet privacy setting blocks all cookies or blocks cookies from sites that do not have a compact privacy policy.
- ❑ Your Internet privacy settings do not allow websites to request your location.
- ❑ You have checked your privacy settings for all media and social networking websites you use.

Activity 2.10: Take Preventive Action

NAME: **DATE:**

Directions:

1. For each of the suggestions above, evaluate what you do now to deter thieves from stealing your personal information.

2. To the left of each bullet, write your rating as "+" if the advice matches your actions most of the time, "-" if you never carry out the action, or "+/-" if you sometimes do the action but could be more careful.

My Rating + +/- -	Preventive Action
	Stay mum. In your profiles, don't list your real birth date, mailing address, or anything you use as a password or to answer a security question for your financial accounts.
	Become a control freak. Use privacy settings to limit the personal information people outside your network can see.
	Pick a strong password. Hackers pretending to be you can scam your friends. Create a non-obvious password that includes a mix of numbers, symbols, and letters (both capitals and lowercase).
	Stay cautious. Messages sent via social networking sites may be even less secure than typical email when it comes to viruses, malware, and fraudulent links to scam your information.
	Just say "ignore." If you can't bring yourself to reject a stranger's "friend" request, just ignore it. Scammers will quickly move on to someone else.
	Watch your apps. Facebook and other social sites do not screen new apps for security issues and viruses. Search an app's name online before adding to see if there are any reported problems.

INFORMATION SHEET

Action Plan for Fraud

Here's an action plan for two common scenarios—finding unauthorized charges on a credit card or unknown accounts on your credit report and discovering your wallet or purse has been stolen:

<table>
<tr><th>Suspicious Charges or
Fraudulent New Accounts</th><th>Stolen Wallet or Purse</th></tr>
<tr><td>File a dispute.
Tell the creditor or credit agency you found a suspicious transaction. Credit card issuers should give you a credit for the suspicious transaction while they investigate it.</td><td>File a report.
Inform the stolen card department at your credit and debit card companies. The company will make a note on your account and send a new card with a different number.</td></tr>
<tr><td colspan="2">File a police report.
Call the non-emergency number (unless you're in danger) and explain what happened. After asking a few questions, they should give you a case number, which you may need to help remedy the situation later.</td></tr>
<tr><td colspan="2">Place a "fraud alert" on your credit report with all three credit reporting agencies.
For the next 90 days, businesses must try to verify that you're the applicant before opening any new credit accounts in your name.</td></tr>
<tr><td colspan="2">Write your credit card companies.
Follow up your calls with a letter that includes your account number, when you noticed the problem, the date you reported the loss to them and your police case number (if available). The letter helps prove when you contacted the company in case there's an issue later.</td></tr>
<tr><td>Contact the FTC.
Report any fraud to the Federal Trade Commission at www.ftc.gov/idtheft or 1-877-IDTHEFT. They work with police departments across the world to shut down identity theft rings.</td><td>Call your cellphone company.
Neglect a missing cellphone and you may get a bill next month for $1,000 in international calls that you didn't make. Your cellphone provider can lock the phone's service so it can't be used.</td></tr>
<tr><td colspan="2">Document everything.
Record what happened, who you talked to, and what they said for every conversation you have with them about the fraud problem.</td></tr>
<tr><td colspan="2">In a few months, check your credit report to confirm there are no new problems.
Check it again periodically after that. If there are negative items, file a dispute with the credit agency. You may also want to add a statement to your credit reports noting that you're the victim of identity fraud and are working to get your credit restored.</td></tr>
</table>

Task: Safe and Secure

NAME: **DATE:**

Directions:

How safe are you online or when you use a computer? If you have a computer at home, check your online privacy settings and your systems security with this checklist:

☐ Your computer files are backed up on a regular basis.

☐ Your Internet security level is set to "High" or "Medium High."

☐ Your Internet privacy setting blocks all cookies or blocks cookies from sites that do not have a compact privacy policy.

☐ Your Internet privacy settings do not allow websites to request your location.

☐ You have checked your privacy settings for all media and social networking websites you use. List those websites here:

After you check for these items, review your checklist with your family and discuss the level of security and privacy you and your family want. Upgrade your privacy and security as needed.

Don't have a computer at home? Then take similar steps to secure your privacy on any social and networking websites you use. Also, ensure that your cell phone and PDA are password protected. Follow the guidelines on page 36 of your Student Guide to create a strong password.