# LESSON PLAN

*Foiling Identity Theft*

## - IT'S A - MONEY THING®

### INCLUDED IN THIS PACKAGE

- **LESSON PLAN** *(2 pages)*
- **ACTIVITY** *(2 pages)*
- **QUIZ** *(1 page)*
- **ACTIVITY ANSWER KEY** *(2 pages)*
- **QUIZ ANSWER KEY** *(1 page)*

### COLLECT FROM YOUR LIBRARY

- **VIDEO 03** *(Foiling Identity Theft)*
- **HANDOUT 03** *(Foiling Identity Theft)*
- **PRESENTATION 03** *(Foiling Identity Theft)*

BROUGHT TO YOU BY

Chilliwack Learning Society

# LESSON PLAN
*Foiling Identity Theft*

**GRADES**
*7 to 12*

**TIME**
*45 minutes*

## OVERVIEW

In today's connected world, staying safe online is more important than ever. This lesson plan focuses on educating students about the importance of protecting personal information and understanding the risks associated with oversharing on social media.

## GOALS

- Help students understand the importance of keeping personal information secure
- Help students recognize the risks associated with oversharing on social media
- Equip students with practical strategies to protect their identity and personal information online

## OBJECTIVES

- Discuss the significance of securing various forms of personal information
- Analyze mockups of social media posts to spot oversharing of personal information
- Develop a set of best practices for maintaining online privacy and security

## MATERIALS

- ☐ **VIDEO 03**—*Foiling Identity Theft*
- ☐ **HANDOUT 03**—*Foiling Identity Theft*
- ☐ **PRESENTATION 03**—*Foiling Identity Theft*
- ☐ **ACTIVITY**—*Spot the Social Media Mistakes and Answer Key*
- ☐ **QUIZ**—*Foiling Identity Theft and Answer Key*

## ASSESSMENT

Use the activity in this lesson plan to assess students' grasp of the topic. An optional quiz is also provided (the quiz is not factored into the lesson's 45-minute runtime).

*Did you know?* This lesson plan explores concepts from Standard 6 (Managing Risk) from the **Council for Economic Education's National Standards for Personal Financial Education.**

## PREPARATION

- *Gather digital materials (video and presentation)*
- *Print **HANDOUT 03** for each student*
- *Print and cut out social media mockups for the **ACTIVITY***
- *Prepare a copy of the **ACTIVITY** for in-class display*
- *(Optional) Print **QUIZ** (Foiling Identity Theft) for each student*

# LESSON PLAN
*Foiling Identity Theft*

## TIMELINE

**5 minutes** — Introduce topic and show **VIDEO 03** *(Foiling Identity Theft)*

**10 minutes** — Go over **PRESENTATION 03**

**25 minutes** — Divide students into small groups and distribute the **ACTIVITY**; go over the correct answers together as a class

**5 minutes** — Wrap up discussion and distribute **HANDOUT 03**

**(Optional)** — Assessment: **QUIZ** *(Foiling Identity Theft)*

## INSTRUCTIONS

1. Begin with a brief discussion on what personal information is and why it is important to keep it secure; ask students to list examples of personal information (e.g., Social Insurance Number, address, phone number, birthdate)

2. Show **VIDEO 03**

3. Go over **PRESENTATION 03**

4. Distribute the **ACTIVITY**

   - Divide students into small groups
   - Distribute one or more social media mockups to each group
   - Instruct students to analyze their mockups and identify any oversharing or privacy risks
   - Bring the class back together and display the social media mockups for everyone to view
   - Have each group present their findings; review and discuss any missing answers

5. Wrap up by sharing the following:

   - Ask students to share common mistakes in social media use that they have observed (either in real life or from the activity)
   - Emphasize the importance of being vigilant about personal information security
   - Ask students to review their own social media profiles at home and identify any information they may need to remove

6. Distribute **HANDOUT 03** for students to take home

7. (Optional) Distribute **QUIZ** for individual assessment, or answer the questions together as a class; decide whether or not students can reference their notes/ handouts during the quiz

## NOTES

# ACTIVITY
*Foiling Identity Theft*

## SPOT THE SOCIAL MEDIA MISTAKES

**Directions:** Identify the potential problems with each social media post.

**1**

**Eddie** ✔ PUBLIC PROFILE
@EddieMarcusMitchell07

Location: Seattle Airport

Counting down the hours until I'm in Hawaii! Two whole weeks of sun, sand and surf! #Aloha #VacationMode
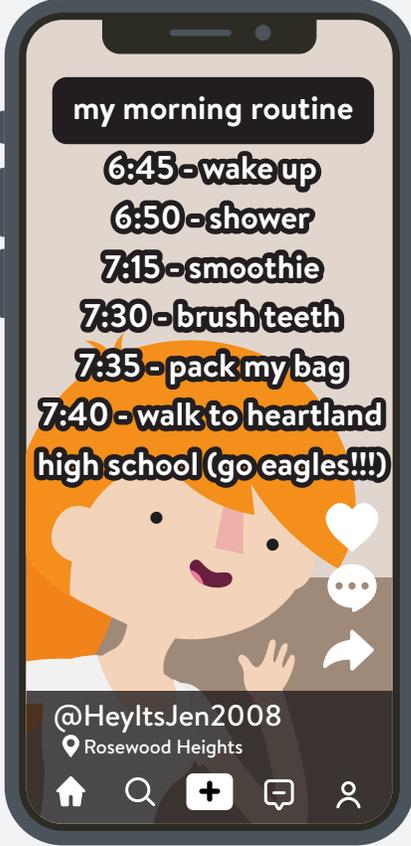
Today, 3:39PM

**2**

**Joy** ✔
@Joy9558

Loving my new place! I'll be here all weekend unpacking, come visit!
203 Main St, Unit 5. #BoxesEverywhere #NewHomeWhoDis

Today, 9:23 AM

**3**

my morning routine

6:45 - wake up
6:50 - shower
7:15 - smoothie
7:30 - brush teeth
7:35 - pack my bag
7:40 - walk to heartland high school (go eagles!!!)

@HeyItsJen2008
📍 Rosewood Heights

**4**

@MacNation 📺LIVE

OAK ST

Comment

# ACTIVITY
*Foiling Identity Theft*

## SPOT THE SOCIAL MEDIA MISTAKES

**Directions:** Identify the potential problems with each social media post.

---

**5**

### Friend Requests

**John B**
Hey! I noticed we have mutual friends, let's connect!

**Sophia Davis**
Omg it's been ages! I found some old photos of us.
DOWNLOAD them here: pm4/xy/link49824

---

**Real_PrizeWin9958**



$1

1,052 likes

**Real_PrizeWin9958** Get a brand new PHONE for just $1! Reply with your address to claim.

**Comments**

**Kat_8457923** Just got mine yesterday! 100% legit #BestDealEver

**Eddie** Seriously? That's awesome!!! 2829 Elm Road in Riverton

**6**

---

**grannylife**
PRIVATE PROFILE

| 2,742 Posts | 15k Followers | 1,304 Following |

**Granny**
Blogger
🌸 Gardening, Knitting and Baking
⭐ Sagittarius ⭐ Dec 5 | 80 years young
🐾 Proud cat mom
💗 Love my grandkids Ava, Jen, Oliver, Harper
📞 (555) 408-4567

**7**

---

**Lucy**
What's your secret nickname? Take your birth month + the street you live on. I'm January Sunnyside! 😀 Share yours in the comments!

**Jen**
July Franklin! Haha **@Lucy** I think you will LOVE the quizzes on PersonaPop. Just search for it and give it access to your account so we can compare scores!

**8**

---

# QUIZ
## *Foiling Identity Theft*

**NAME:**

TOTAL
/ 5 pts

## MULTIPLE CHOICE

**Directions: CIRCLE the best possible answer from the given options.**

1. Which of the following items should you shred before discarding?
   a. Bank statements
   b. Junk mail with your address
   c. School schedules
   d. All of the above

2. Which of these is a good practice for protecting your personal information online?
   a. Using the same password for all accounts
   b. Storing passwords in note-taking apps
   c. Setting strong, unique passwords
   d. Posting your location frequently

3. What should you do if you receive a suspicious message asking for personal information?
   a. Ignore it
   b. Report it as spam and block the sender
   c. Reply with a funny response
   d. Forward it to your friends

4. Which of the following is NOT a recommended way to protect your computer from security threats?
   a. Keeping your operating system up to date
   b. Disabling your firewall
   c. Installing antivirus software
   d. Enabling automatic updates

*/4 pts*

## TRUE OR FALSE

**Directions: CIRCLE either true or false.**

5. TRUE or FALSE      Public Wi-Fi networks are safe to use for online banking and shopping.

*/1 pt*

# ACTIVITY ANSWER KEY
## *Foiling Identity Theft*

- IT'S A -
MONEY
THING®

## SPOT THE SOCIAL MEDIA MISTAKES

**Directions: Display each social media mockup for the class. Ask student groups to share the problems they identified with their assigned post(s). Fill in any missing points based on the provided answers.**

| POST | PROBLEMS |
|------|----------|
| 1 | • Posting about your travel plans, whether on social media or through automated out-of-office email replies, is a classic example of oversharing. This information can signal to potential intruders that your home is unoccupied.<br>• Keeping your social media profile public exposes you to more online risks. To enhance your security, opt for privacy settings that limit who can see your information.<br>• Including your full name and birth year in your username can make it easier for cybercriminals to steal your identity or access your accounts.<br>• Sharing your location through check-ins on social media can reveal your whereabouts to a wide audience. Consider waiting until after you've left a place to post about it. |
| 2 | • Never share your full address on social media. This can expose you to significant risks, including burglary and identity theft.<br>• Using a sequence of numbers like '9558' could hint at a PIN for your bank card or cellphone. Never incorporate digits from your PIN into your username. If numbers are necessary to create a unique username, opt for random digits that aren't related to any PINs or passwords. |
| 3 | • Posting detailed aspects of your daily activities, including the time you walk to school, can put your safety at risk. Before following a trend, consider what information you are sharing.<br>• Tagging any specific locations in your social media posts can reveal too much about your whereabouts.<br>• Including a reference to your age or birth year in your username can make you more susceptible to identity theft. Choose usernames that don't contain personal information. |
| 4 | • During a livestream, ensure that no identifiable street signs or landmarks are visible in the background, as this can reveal your location and compromise your safety.<br>• Before you post, make sure personal items like your credit card or paperwork with sensitive information are out of sight. |
| 5 | • Before accepting friend requests, especially from profiles with limited information, take a moment to verify their identity through mutual friends or other means. Remember that scammers can even impersonate people you know to gain your trust.<br>• If a friend request includes a link or claims to have information about you, avoid clicking on unfamiliar links. These could lead to malicious websites. |

# ACTIVITY ANSWER KEY
## *Foiling Identity Theft*

**- IT'S A -
MONEY
THING®**

### SPOT THE SOCIAL MEDIA MISTAKES

**Directions: Display each social media mockup for the class. Ask student groups to share the problems they identified with their assigned post(s). Fill in any missing points based on the provided answers.**

| POST | PROBLEMS |
|------|----------|
| 6 | • Offers that seem unbelievably good, especially from newly created or suspicious-looking accounts, are often scams. Avoid engaging with these accounts and never share your personal information with them.<br>• Be cautious of comments from others claiming an offer is legitimate. Scammers frequently use fake accounts to create a false sense of trust and mislead users.<br>• Even if a post appears legitimate, never share your personal information in the comments. These are often public and can be viewed by anyone. |
| 7 | • Each social media site has unique privacy settings, and even private accounts can sometimes display certain information publicly. Regularly review and adjust your privacy settings to keep your personal information secure.<br>• Information in your profile, such as your birth year, family names or contact details, can be used by scammers to impersonate you and deceive your friends.<br>• Keeping your account private is a good step, but it's equally important to be cautious about who you allow to follow you. |
| 8 | • Nickname games often ask for personal information that can be used to guess your passwords or answer security questions.<br>• Many social media games and quizzes request access to your profile information, friends list and other personal data. Be aware that the data you share can be collected and used by third parties. |

# QUIZ ANSWER KEY
## *Foiling Identity Theft*

**- IT'S A -
MONEY THING®**

## MULTIPLE CHOICE

**Directions: CIRCLE the best possible answer from the given options.**

1. Which of the following items should you shred before discarding?
   a. Bank statements
   b. Junk mail with your address
   c. School schedules
   **(d.) All of the above**

2. Which of these is a good practice for protecting your personal information online?
   a. Using the same password for all accounts
   b. Storing passwords in note-taking apps
   **(c.) Setting strong, unique passwords**
   d. Posting your location frequently

3. What should you do if you receive a suspicious message asking for personal information?
   a. Ignore it
   **(b.) Report it as spam and block the sender**
   c. Reply with a funny response
   d. Forward it to your friends

4. Which of the following is NOT a recommended way to protect your computer from security threats?
   a. Keeping your operating system up to date
   **(b.) Disabling your firewall**
   c. Installing antivirus software
   d. Enabling automatic updates

*/4 pts*

## TRUE OR FALSE

**Directions: CIRCLE either true or false.**

5. TRUE or **(FALSE)**     Public Wi-Fi networks are safe to use for online banking and shopping.

*/1 pt*