Identity theft can be one of the most life-altering experiences a person can have forced onto them. It attacks not just your sense of safety but can leave you on an unending cycle of trying to prove your innocence and rehabilitate the damage done to your standing. But what could you have done to stop it?

Learn more about preventing financial fraud by watching this video and then expand your knowledge by completing this worksheet by yourself or with an adult!

**Try It Yourself!**

Complete the matrix below. Then answer the four questions at the bottom.

<table>
<thead>
<tr>
<th>Preventing Financial Fraud</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>What do you think of when you hear the term identity thief? How about identity theft?</td>
<td></td>
</tr>
<tr>
<td>You get a call from someone saying they are from the Internal Revenue Service and that you owe money for taxes. What should you do?</td>
<td></td>
</tr>
<tr>
<td>Your friend bought an event ticket from a stranger online that turned out to be fake. What mistake did your friend make?</td>
<td></td>
</tr>
<tr>
<td>As a group, children are one of the fastest-growing victims of identity theft. Why do you think this is happening?</td>
<td></td>
</tr>
<tr>
<td>Have you ever heard of scholarship scams?</td>
<td></td>
</tr>
<tr>
<td>What do you think they are?</td>
<td></td>
</tr>
<tr>
<td>When do you think people should start checking their credit history for signs of identity theft?</td>
<td></td>
</tr>
</tbody>
</table>
Vocabulary:

- **Fraud**: Using dishonesty, deception, or other tricks in order to take something of value from another person or party
- **Identity theft**: A crime in which someone acquires and wrongly uses another person's personal information
- **Phishing**: Use of email that represents communication from a familiar and trusted organization to persuade people into revealing personal or financial information
- **Scam**: Fraud; an attempt to deceive another person
- **Social Security number**: A nine-digit number assigned by the federal government to track people’s income and benefit eligibilities

Please select the correct answer for each of the following questions.

1. A high-tech scam that uses spam or pop-up messages to deceive consumers into disclosing their card numbers, bank account info, Social Security number, passwords, or other personal information is called
   a. Soliciting
   b. Phishing
   c. Scamming
   d. Consuming

2. A scholarship or financial aid scam may require a student to share his/her
   a. Teacher’s name
   b. Transcript
   c. College application
   d. Credit card or bank account number

3. An identity thief may want
   a. To use your personal information for their own gain
   b. To steal your money
   c. To open a credit line in your name
   d. All of the above

4. You just signed up for your first credit card and want to protect yourself against credit card fraud. What is the best way to do this?
   a. Leave your credit card at home when you travel
   b. Reconcile your account every month and immediately notify your bank of discrepancies
   c. Throw away all credit card statements
   d. Never use your credit card for online purchases
Answer key

Student answers will vary. The information below should be used to debrief the exercise and clarify student responses.

#1
What do you think of when you hear the term identity thief? How about identity theft?

**Identity thief:** A person who acquires and wrongly uses another person’s personal information

**Identity theft:** A crime in which someone acquires and wrongly uses another person’s personal information

Examples: An identity thief gets a person’s name, Social Security number, and address and opens a credit card or loan. Then the identity thief doesn’t pay the bills. Some identity thieves steal the information themselves. Others buy the information online (often called the “dark web”) and use the information for their own financial gain.

#2
You get a call from someone saying they are from the Internal Revenue Service and that you owe money for taxes. What should you do?

This is an example of an **imposter scam**. People pose as someone else in order to obtain information or get money from the victim.

Examples include people posing as:
- A representative of a bank or other financial company
- A government employee
- A religious official

If the scam happens by email, it is referred to as **phishing**.

Victims should report the crime to local law enforcement as well as the **Federal Trade Commission** or FTC.

#3
Your friend bought an event ticket from a stranger online that turned out to be fake. What mistake did your friend make?

This is an example of a **ticket scam**. Thieves often create counterfeit tickets with forged barcodes and logos of real ticket companies. Other examples include:
- Charging prices much higher than the face value of a ticket
- Selling duplicates of a legitimate ticket and emailing it to several buyers
- Pretending to sell tickets online to steal your credit card information

To avoid becoming a victim, a person could:
- Purchase tickets from the venue whenever possible.
- Avoid buying tickets from strangers.
- Use payment methods that come with protection such as a credit card.

#4
As a group, children are one of the fastest-growing victims of identity theft. Why do you think this is happening?

Identity thieves like using the Social Security numbers of children because they can often go unnoticed for a long time.

Warning signs include:
- Being turned down for government benefits
- Getting a notice from the IRS saying the child didn’t pay income taxes or that the child’s Social Security number was used on another tax return
- Receiving collection calls or bills for products or services you didn’t order or receive
#5
Have you ever heard of scholarship scams? What do you think they are?
Scholarship scams happen when unethical companies guarantee or promise scholarships, grants, or fantastic financial aid packages.
Examples include:
- High-pressure sales pitches and the need to pay immediately or risk losing out on the "opportunity"
- A "money-back" guarantee that a student will get a scholarship (When they try to get a refund, they are unsuccessful.)
- Getting a student's checking account information to "confirm eligibility," then debiting the account without the student's consent
- Other companies quote only a relatively small "monthly" or "weekly" fee and then ask for authorization to debit your checking account – for an undetermined length of time
- Charging a processing fee to file the Free Application for Federal Student Aid (FAFSA) – a form students can complete and submit for free

#6
When do you think people should start checking their credit history for signs of identity theft?
The Federal Trade Commission recommends that parents help their child check for the existence of a credit history around age 16.
Doing so can help them identify a problem and correct it before the child needs to apply for a job, credit card, or loan.
To check for a credit history, the parent or guardian will need to contact each of the three nationwide credit reporting companies (Equifax, Experian, and Transunion) and ask them to conduct a manual search. Children in foster care should request assistance from a case manager.

Answer key
1. B - Phishing
2. D - Credit card or bank account number
3. A - To use your personal information for their own gain
4. B - Reconcile your account every month and immediately notify your bank of discrepancies


© 2021 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.