Scams and Schemes

Do you know someone who has been scammed? What happened? You might know of instances in which someone has been convinced to send someone else money or purchase a fake or bad product.

What is the purpose of a scam? What tricks do people use to carry out a scam? You should understand that the ultimate purpose of a scam is to get someone to give the scammer money, or information that can help the scammer steal money, such as a credit card number, ATM code, or password. To accomplish this, scammers tell lies and often pretend to be someone they are not.

Can people get scammed on the Internet? How? You may know stories of friends or relatives who have been scammed online. Some examples:

- Someone can be tricked into buying a bad or fake product online
- Someone can be lured into sharing information that a scammer can use to steal from them

You will be learning about a variety of online scams, including which kinds of information scammers look for, and how that information can be used. You will also learn how to protect yourself against online scams.

Part 1: What Is Identity Theft?

People who scam others online don't always have to get money from them directly. Instead, they use a variety of strategies to trick people into giving out private information. They then use this information to access their bank and credit card accounts or other personal accounts. They can even "re-create" someone's identity and produce false documents, such as Social Security cards, credit cards, or drivers' licenses in someone else's name.

IDENTITY THEFT: A type of crime in which your private information is stolen and used for criminal activity.

Can you guess what kinds of personal information identity thieves might look for?

Identity thieves look for any information that might help them pretend to be their victims. Below is a list of the types of information identity thieves look for:

- Full name
- Account numbers and the companies
- Date of birth and where you were born
- Current and previous addresses and phone numbers
- Driver's license or passport number where you hold accounts (e.g., Amazon, PayPal, etc.)
- Passwords

- Social Security number

VULNERABLE: In a position that makes it easier for you to be harmed or attacked.

Anyone is vulnerable to an online scam. Although teens might not think they're at risk, there are a few important reasons why they are vulnerable to identity theft – and why it matters:

- Identity thieves look for "clean" Social Security numbers that haven't yet been used to get credit. They target teens and kids, who often have Social Security numbers that have no credit history yet. Identity thieves might sell or use these numbers, which would allow someone else to get a credit card or loan and build up debt under your name.
- Being a victim of identity theft can ruin your financial future and your ability to obtain loans and purchase things. For example, it could affect your ability to get a student loan for college or a loan to buy a car.
- In addition, if you use your parents' accounts and credit cards online, or fill out forms with your parents' information, you are sharing information that could potentially put your parents' identities at risk.

It can take months, even years, to recover your identity if it's stolen. Cleaning up such a mess takes a lot of time and energy, and it can also be expensive.

Part 2: How to Catch a Phish

How do you think identity thieves might try to get your information?

PHISHING (pronounced "fishing"): When people send you phony emails, pop-up messages, social media messages, texts, calls, or links to fake websites in order to hook you into giving out your personal and financial information.

The best way to avoid phishing scams is to be skeptical about any online request for personal information. It's also good to be skeptical of online messages or posts from friends that seem out of character for them, which is a warning sign that their accounts have been hacked. There are clues that can help you spot phishing.

You will learn more about these clues and these types of scams when you complete the assignment called "Spotting Scams".

Part 3: Protect Yourself from Online Scams

SCAM: An attempt to trick someone, usually with the intention of stealing money or private information

If you ever encounter something online that you believe might be a phishing scam, you should observe the following rules:

- Avoid opening the message or email in the first place.
- Don't click on any links or download any attachments; they might contain viruses or spyware.
- Don't reply.
- Mark as "junk mail" or "spam" for your email provider, or report it to your social network site.
- If you are concerned about an account you have with a company, contact its customer service department by phone.
- Make sure you verify the company's contact information elsewhere online first.

You can also protect yourself from Internet scams by learning how identity thieves think.