Don't Feed the Phish

How can you protect yourself from phishing?

OVERVIEW

Internet scams are part of being online today, but many kids might not be aware of them. How do we help our students avoid being tricked into clicking malicious links or giving out private information? Use this lesson to help kids avoid online identity theft and phishing schemes.

Learning Objectives:

- Compare and contrast identity theft with other kinds of theft.
- Describe different ways that identity theft can occur online.
- Use message clues to identify examples of phishing.

Key Vocabulary:

identity theft
a type of crime in which your private information is stolen and used for criminal activity

internet scam
an attempt to trick someone, usually with the intention of stealing money or private information

phishing
when someone poses as an institution, like a bank or school, and sends you a personalized message asking you to provide private information

private information
information about you that can be used to identify you because it is unique to you (e.g. your full name or your address)

shortened URL
a web address that has been condensed and which could mislead an user into going into a risky website

Classroom resources

- Colored markers or highlighters
- Pencils
- Blank paper
- Lesson Slides
- Trick Questions! Practice Quiz (Google Form) Handout
- Trick Questions! Practice Quiz (Printable) Handout
- How to Catch A Phish Handout Teacher Version

- Lesson Quiz

Lesson Plan

Warm Up: **Safe or Unsafe?** 7 mins.

1. **Project Slide 4** and read it aloud: *What's something you own that someone else might want to steal? Why? What would they do with it? Take turns sharing your idea with your partner.*

   After students pair-share, call on a few of them to share out with the class. Students may respond by naming things of value that they own (clothing items, electronics, etc.) and how they might be used.

2. **Say**: *In reality, the thing you own that might be most valuable -- and most likely to get stolen -- is not a thing at all: It is your identity. What do you think that means? How could someone steal your identity?*

   Call on students to respond. Students may say: *It means that someone can pretend to be you* or *Someone can get your information*. Follow up by asking students to explain more and clarify any misconceptions. For example, identity theft might mean that one or more pieces of information about you has been stolen, not that everything about you has been. It also doesn't mean you no longer have what's been stolen (as in the case of a stolen object); you are still you and your identity hasn't changed.

3. **Project Slide 6** and define **identity theft** as *a type of crime in which your private information is stolen and used for criminal activity*.

   Ask: *What do you think is meant by "private information"? What would an example of that be?*

   Call on students to respond and provide examples. Dene **private information** as *information about you that can be used to identify you because it is unique to you (e.g., your full name, phone number, or address)*. (**Slide 7**)

4. **Say**: *Identity theft is important to know about, because if your identity is stolen, it can lead to some pretty bad consequences. And you may not even know about those consequences until far into the future. If your identity is stolen, it could potentially enable someone to:* (**Slide 8**)

   - *steal money from you.*
   - *apply for credit cards in your name and buy things.*
   - *cyberbully someone while pretending to be you.*
   - *create false identification documents.*
   - *apply for loans (to buy a car or house).*
   - *get a driver's license or a job under your name.*

5. **Say**: *Now that we know what identity theft is, let's talk about how it happens and what you can do.*

Explore: **How Identity Theft Happens** 5 mins.

1. **Say**: *One way that someone can try to steal your identity on the internet is by getting you to click a link or enter information about yourself. This is called an internet scam* (**Slide 10**), *which is an attempt to trick someone, usually with the intention of stealing money or private information. Let's see how this can happen.*

2. **Explain** that one of the most common ways identity thieves get your private information is through something called **phishing** (*when someone poses as an institution, such as a bank or school, and sends you a personalized message asking you to provide private information*). Students might think of phishing as similar to shing -- someone trying to "catch" people's private financial information like trying to catch a fish. (**Slide 11**) .

3. Inform students that they have been phished! Slides 12-13. Look at the data for how many students open the phishing email. Maybe some students will go check their email right now.

4. **Project** the samples messages on **Slide 15**. Have students share whether to click on or skip the various links shown and why. Encourage them to pinpoint which details helped them decide.

They should identify only the Mari_Tellez example as one that is likely OK to click.

Explain that some links, or URLS, are not what they seem. Ask: *Why do you think the links might trick someone?* Dene **shortened URL** (**Slide 16**) as *a web address that has been condensed and which could potentially mislead a user into going into a risky website*. Explain that such a website may:

- install malware on your device.
- steal your information.
- charge you money.

Say: *In the next activity, you'll learn strategies for protecting yourself against phishing and identity theft.*

Analyze: **How to Catch a Phish** 10 mins.

1. **Distribute** the How to Catch a Phish Student Handout and focus students' attention on the list of clues. Allow one minute for students to read the list of clues and answer any questions they have.

2. **Tell** students that they will work in pairs to analyze examples of messages that use tricks to phish for your information. (**Slide 17**) Model how to highlight a clue in the message, and list the type of clue in the empty box. You may wish to have students color-code the clues.
3. **Allow** pairs five minutes to complete the activity on the handout.

Call on students to share out their answers. Use the **Teacher Version** to support students in using specific details from each example.

4. **Summarize** how checking for clues that indicate phishing can help protect you from identity theft.

Wrap Up: **Stay Safe from Scams** 5 mins.

1. **Say**: *You have learned about the importance of protecting your information from identity theft. You also have learned strategies for guarding against phishing scams. Now use what you have learned to show how others can protect themselves against identity theft.*

2. **Project Slide 13** and read aloud the questions. Allow students a few minutes to answer and then collect to assess student understanding.

3. **Have** students complete the **Lesson Quiz**. Send home the **Family Activity** and **Family Tips**.