Lesson Plan 17: Staying Safe in a Digital World

Lesson Overview: In this lesson, students will learn how to identify and deal with scams in the form of email, text messages, and online pop-up windows and advertisements.

Lesson Objectives

Students will:

- identify scams in the form of email, text messages, and online pop-up windows and advertisements.
- explain what they should and should not do once they identify a scam.

Materials and Setup

Technology /Equipment

- An Internet- and audio-enabled computer, projector, and screen
- Student devices (laptops, tablets, desktop computers)
- The teacher needs to send an email to herself/himself to demonstrate live in class. See the text for the email in the Teacher Materials 17.1: Mary's Email Scam.

Supplies/Teacher Materials

- Whiteboard and markers
- Teacher Materials 17.1: Mary's Email Scam
- Teacher Materials 17.2: Is It Safe or Is It a Scam? Powerpoint
- Teacher Materials 17.3: Is It Safe or Is It a Scam? Slide Notes

Student Handouts

- Handout 1: Mary's Email Scam
- Handout 2: Checking Links on your Phone
- Handout 3: Digital Safety Basics
- Handout 4: Is It Safe or Is It a Scam?

Online Resources

- Google Form: tinyurl.com/dartdigsafety

Instructional Tips

- ***Key Vocabulary:*** You may want to ask students to label a page in their notebooks for this lesson's key vocabulary and have them write down each of the words as you explain them as they are used in the context of the lesson. Ask students to write down the meaning of the word in their own language.
- ***Keyboarding Practice:*** Students will practice keyboarding when they complete the online quiz on digital safety in the evaluation section of this lesson.

Standards

Adult English Language Proficiency Content Standard(s)

Lesson 17: Staying Safe in a Digital World

- 2.1. Participate in level-appropriate oral and written exchanges of information

CASAS Content Standard(s)

- L2.9: Comprehend specialized vocabulary (e.g., technical, academic)
- S2.9: Use specialized vocabulary (e.g., technical, academic)
- R1.1: Identify the letters of the English alphabet (upper and lower case)
- R2.1: Interpret common symbols
- W1.1: Write the letters of the English alphabet (upper and lower case)
- W4.5: Use specialized vocabulary (e.g., consumer, work, field of interest)

Seattle Digital Equity Initiative Skill(s)

- EF.10: Create Safe Passwords / Password basics: creation, safe storage, resetting
- PS.2: Verify Secure Websites
- PS.3: Limit Sharing of Personal Data
- PS.6 Recognize Online Threats

Northstar Digital Literacy Standards for Essential Computer Skill(s)

- Internet Basics 7: Demonstrate understanding of when it's safe and appropriate to share personal, private, or financial information (e.g., recognizing phishing attempts, identifying unsecured websites).
- Internet Basics 10: Identify address bar and demonstrate understanding of its functionality.
- Internet Basics 14: Identify and make use of common website interactions (e.g., play buttons, hyperlinks)

Key Vocabulary

- scam
- victim
- shop online
- pop-up window
- computer virus
- hover
- urgent / immediate
- win/won/winner
- prize / gift
- schedule/reschedule a delivery

Reinforced vocabulary: address bar, web page, link, email, email address, text/text message, delete, verify , account, click, press, hold down, scroll

ENGAGEMENT

Notes

- Write the word 'scam' on the board. Ask students what the word means. If they do not know the word, ask them to look it up on their phones in their own language. (Scribe student answers – possible responses are something that is not true, a trick, a lie, stealing, etc.)
- Write the word 'victim' on the board and do the same.
- **Ask**: Has anyone been a victim of a scam? (Take responses; prompt students to tell their experiences as a victim of a scam if they want to do so. Share your own experiences if you have any.)
- **Say**: Many people get text messages on their phone that are scams. Many people get emails that are scams. You can click on advertisements on web pages that are scams. You can also be scammed when you shop online. You can also be scammed when someone calls you on the phone.

Lesson 17: Staying Safe in a Digital World

EXPLORATION

- Before this activity, the teacher needs to copy and paste the email from **Teacher Materials 17.1: Mary's Email Scam** and send it to herself/himself.
- Distribute the **Handout 1: Mary's Email Scam** to your students.
- Open up your email that you sent to yourself and display it on screen.
- **Say**: Let's read through this email. (Get volunteers to read or read to students as appropriate for their language levels.)
- **Ask**: Who is the email from? (Students should answer the HelpDesk@Loyainc.com.)
- **Say**: We need to check if the email is really from the Help Desk. We need to hover our mouse over the email address.
- **Ask**: Who remembers what "hover" means? (Write hover on the board. Hover was introduced in Lesson 10. If students do not remember, explain that hover means to move the mouse arrow over a link without clicking on the link.)
- **Say**: Let's watch what happens when I hover my mouse over the email address. (Demonstrate and point out to students that the link shows up at the bottom of the screen in a blue bar.) Now I can see that the link is different than the email address. The email link is kramsey@biz5224.com, not HelpDesk@Loyainc.com. (*Refer students to look at their **Handout 1** to see the email links clearly because the link text in the email is very small.*
- **Say**: Now watch when I hover my mouse over the link to reset Mary's password. (Demonstrate.) Are the links the same? (Students might say yes but tell them to look more carefully.) There is one letter different – *loyainc.com* is in the email text, but the link is actually *loyain.com.*
- **Ask**: Should Mary click on the link? (No.) What should Mary do? (Delete the email, contact the Help Desk at her company.)
- **Say**: I can also check links when I look at emails or text messages on my phone.
- **Say**: I have a handout that shows you how to check links on your phone. The handout has 3 steps. (Distribute **Handout 2: Checking Links on a Phone**.)
- **Say**: On the handout, I see an email from UPS. The email says that I can track my package. What do I need to click on? (Wait for a student to say the "Track your package" button.)
- **Say**: I don't know if this is a safe email or if it is a scam. I need to know the link for the button.
- **Say**: Step #1 says to press and hold down on a link or a button. When I do this, a box appears with the link.
- **Say**: Step #2 says to look at the link.
- **Say**: I see the link. I need to ask 2 questions. First, does the link start with https? Second, does the link have the name of the company?
- **Ask**: Does the link start with https? (Students should respond yes.)

- **Ask**: Is the link to the correct company? (Students should respond yes.)
- **Say**: Look at Step #3. It says to Tap on the "Tap to show preview."
- **Say**: After I tap, I see a preview of the web page.
- **Ask**: Does the web page look correct? (Take responses – it does look like the UPS website.)
- **Say**: This link looks safe to open. This email is not a scam.

EXPLANATION

- Distribute **Handout 3: Digital Safety Basics**.
- **Say**: This handout has digital safety basics. Look at the handout. What is the title? (Wait for responses – Digital Safety Basics.)
- **Say**: There are 5 parts in the handout. The 5 parts have headings. What are the names of the 5 headings? (Scribe them as students call them out – Password Safety, Email and Text Message Safety, Web Page Pop-Up Window Safety, Web Page Advertisement Safety, and Online Shopping.)
- Read through the activity with students.
- Start by having them read along as you read through the handout one section at a time. After each section, ask students to circle any words they do not know.
- Ask for the words and write them on the board. Explain the words in simple English. Ask if students in the class know the words in their native languages. Students can also look up what the words mean in their own language.
- When you complete all four sections of the handout, pair students and have them read to each other.

ELABORATION

- **Say:** Now we are going to look at some emails, text messages, and pop-up windows.
- Distribute **Handout 4: Is It Safe or Is It a Scam?**
- Display **Teacher Materials 17.2: Is It Safe or Is It a Scam? Powerpoint**. Present the PowerPoint in Presentation Mode so you can see the slide notes. Alternatively, print out **Teacher Materials: 17.3: Is It Safe or Is It a Scam? Slide Notes** so you can view the notes as you present the slides.
- Go through the PowerPoint presentation. Use the notes to help you prompt students why each example is a scam. You may want students to work in pairs or groups of 3 to talk about each example using their handouts before they give you their responses.

EVALUATION

- Ask students to get a computer, sign in, and open up Google Chrome, and go to the following web address: tinyurl.com/dartdigsafety.
- Allow students to work alone or with a partner to complete the Digital Safety Quiz. Students will receive their scores and right and wrong responses immediately after the quiz.

- Go over the answers with students either immediately after they complete the quiz or at the beginning of the next class.

Differentiation Resources to Meet Diverse Learner Needs

For more advanced students:

- Pull up the following web page and go through the examples of text spams: https://blog.textedly.com/spam-text-message-examples

- Access Skillblox.org and use access code **YCFK6U** to view additional information and examples of online scams