|  |  |
| --- | --- |
|  | **First Steps: Understanding the World of Work through Career Technical Education** is a standard-based, CTE focused, career development curriculum for students in grades 7-8. The First Steps logo indicates instructional resources are aligned to the [First Steps Standards](https://cte.idaho.gov/Resource_Catalog/Program_Areas/Middle_School/TheIdahoMiddleSchoolCTEInitiative.pdf) and IDCTE approved! |

**First Steps Standard(s):** Domain 1: Self-Evaluation (Who am I?) 4. Identify Skills (What am I good at?) C. Information Security iv-v. Demonstrate basic internet and email safety and document a reflection

**Career Activity Curriculum Topic:** Don’t Get Scammed!

**Learning Outcomes:** Students will be able to (SWBAT):

1. Understand the importance of Information Security
2. Demonstrate understanding in email
3. Apply the information security guidelines to their professional internet identifies

**Activity Summary:** This lesson will help students recognize signs to differentiate between a safe and unsafe email. They will define what phishing is, learn the common signs of phishing, and practice identifying red flags in email examples. They will take this process and apply it to their own personal email account.

**Estimated Time:** One45-60-minute class period

**Suggested Grade Level:** 7th or 8th Grade

**Materials Needed:**

* Teacher Materials: Computer/Projector, slide deck, handout (Assignment Sheet (1 per student)), Email Examples (copies dependent on teacher choice)
* Student Materials: Pen/pencil, handout, access to a device (or one to share)

**Academic Vocabulary:**

* **Personally Identifiable Information (PII)**: Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.”
* **Public Information:** information that is associated with a person’s or group’s life that is readily available and known.
* **Identity Theft:** all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain
* **Phishing:**  Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites).

**\*\***Definitions from**:** [(NIST)](https://csrc.nist.gov/glossary/term/personally_identifiable_information).

**Introduction:** One aspect of online safety is being able to identify online scammers and phishing attacks.

This lesson will introduce the signs of phishing attacks in the form of emails and teach you to identify them

in your own inbox. Being able to tell when the information you are consuming, or links you are clicking on, is

trustworthy is an important part of participating in an online community. By the end of the lesson, you will have

the tools to help identify email scams and protect your information online.

**Learning Activities/Procedures:** Use the slide deck.

1. Review the content from the previous lesson (Domain 1.4.C.(iii-v) with students. Then give them 5 - 10 minutes to work with a partner and fill out the “Warm Up” on their assignment sheet, encourage them to place AT LEAST five pieces of information in each category.
2. Do a quick “call-out” or discussion regarding different types of information they listed in each category and the answers to the two review questions on the slide. Try to place five (or more) examples in each category from the class.
3. Go through the three “Defining Terms” slides and have students fill in the blanks in the definitions on their handouts. Play the video for phishing once you have reviewed/discussed all three terms.
4. Discuss the tips provided in the video for avoiding the “bait” in a phishing scam.
5. Review the “Common Signs of Phishing Scams” by having students read them off and discussing how each one might look in context.
6. For the “Catching the Phish” Activity, students will identify “Red Flags” or signs of a phishing scam in five different example emails. The directions ask them to identify the red flags, explain why they identified each one, and determine whether the email is trustworthy or not.
7. This activity can be completed as a whole class (display each email on the board or projector), with a partner or group (each set gets one example to work through), as a “gallery walk” or “station” activity (1 email per station), or individually (though it will require a class set of copies or large packets for each student).
8. After the example emails have been determined as trustworthy or not, students will complete the same process for their own emails. They will choose three messages form their school or personal email inbox, identify and explain the “red flags” and then determine if each one is trustworthy.
9. Discuss the following questions as a closing activity. Have students choose ONE QUESTION to answer for their “Exit Ticket” on the handout.

* What is the difference between private and public information?
* What is phishing, and what are the common signs of a phishing scam?
* Could you identify the trustworthiness of an email?

**Accommodations/Adaptations/Extensions**

**Accommodation:** Have students complete the activities within groups or pairs; provide (simple) examples for students who do not have access or make a simpler version of the “Phishing” activity for those in need; play video with subtitles/captions; provide a template for the “practice email”

**Adaptation:** Virtual: Present each email example by sharing your screen with participants and have them send via chat different red flags; post the emails in a discussion forum and have students comment their answers to the phishing activity; change the evaluation and have virtual students construct a “scam” email and send it to you, to demonstrate understanding of each sign.

**Extension:** Challenge students to create a visual aid to teach younger students about this concept. Prompt them to consider the languages, visuals, and examples that would be helpful for a younger audience.

**Evaluation:** Students will complete and submit the handout.

**Closing:** Now that you’ve applied the common signs of a phishing scam to a variety of different emails, you can better understand why it is important to keep private information private. You are better able to separate a scam from a valid email, whether it is in a work/school setting or in a personal setting. Remember: while we focused specifically on email phishing scams, phishing scams are done in a variety of ways. Keep your eyes open and keep your information safe!

**Resources/References:** [(NIST)](https://csrc.nist.gov/glossary/term/personally_identifiable_information)