How to Avoid Scams

Intro

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.

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: 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 sourced from: National Institute of Standards and Technology*

What comes to mind for you when you think of computer scammers, hackers, or a phishing attack? Have you ever had an experience with something like this? How do these things fit into the experience of being in an online community?

Write any thoughts you have in the space below!

Background Knowledge

Click the link below to learn about phishing attacks.

Watch the Phishing Attacks Video

1) What is the main reason that the video suggests people still fall for "phishing

attacks”?

2) What are some of the tips that the video offers for avoiding becoming a victim of an attack?

How does this relate?

In recent years, both colleges (and college students) as well as many large corporations (and potential jobseekers) have become large targets for spear-phishing or phishing attacks.

Decide which path you want to focus on: **Career-Seeking** or **College-Bound** and click the hyperlink to learn more about that type of phishing attack.

My List of "Tips & Tricks"

When you are finished reading, use the information provided (as well as that from the video) and make yourself a list of 5 “Tips and Tricks” to avoid becoming a victim of a phishing attack.

1
2
3
4
5

Scams in Daily Life

View the sample email below and the list of “Red Flags” that can help to identify an email scammer. See if you can identify some of the “Red Flags” in the email. Explain how you know those are red flags, and whether you would still consider the email trustworthy or not.

Red Flags:

- An unfamiliar greeting.
- Grammar errors and misspelled words.
- Email addresses and domain names that don’t match.
- Unusual content or request – these often involve a transfer of funds or requests for login credentials.
- Urgency – ACT NOW, IMMEDIATE ACTION REQUIRED.

What red flags do you see?

Explain what makes each element you enter below a "red flag."

Is this email trustorwthy?

○ Yes○ No