Activity 11-1: Phishing Detective

Big Idea

This "Phishing Detective" activity empowers students to become savvy digital citizens, teaching them to critically analyze emails and identify phishing attempts. This hands-on approach not only enhances their cybersecurity awareness but also fosters important critical thinking skills essential in the digital age.

Materials

- Sample Email Examples (the two provided and/or others you find)
- Computer/Tablet with Internet Access

Vocabulary

Phishing
Email address
Domain
Cybercriminal
BCC (Blind Carbon Copy)
Spoofing
File extension
Link preview
Misspelled Domain
Attachment

Background

Let's talk about something super important: phishing messages. These sneaky messages are designed to trick you into clicking on a link, which can then let a cybercriminal sneak into your device or steal your personal info. You might get these through emails, texts, or even phone calls.

These messages can look super legit, like they're from a real company, with all the right logos and colors. Sometimes, they even sound like they know you, using urgent language or making it seem like you need to act fast.

It's not always easy to spot these phishing attempts, but here are some smart tips to help you out:

- **Check the Sender:** Is the email address weird or misspelled? Be wary, even if it's from a popular email service.

- **How Did You Get the Message?** If you're BCCed or it's a mass email you didn't sign up for, be cautious.
- **Personal Greeting:** Legit messages should know your name, not just a generic "hey there."
- **Does it Sound Right?** If it's a company email, does it sound professional? If it's from a friend, does it actually sound like them?
- **Look Out for Errors:** Watch for misspelled words, bad grammar, or strange formatting. These can be red flags.
- **Do Your Research:** If you're not sure, look up the sender online to see if they're the real deal.

And if you get a message that seems fishy (pun intended):

- **Don't Click Links:** Unless you're 100% sure it's safe, don't click on any links. Hover over them to see where they lead.
- **Beware of Spoofing:** This is when someone pretends to be someone important, like your bank or a company, and asks for urgent action. Always double-check by calling them on a trusted number (not the one in the email!).
- **Check the Headers:** Learn how to see the full path of an email in your email program. This can give you clues about where it really came from.
- **Be Careful with Attachments:** Watch out for weird file extensions like .exe or .jsp. If you weren't expecting an attachment, it's better not to open it.

Activity Directions

Alright, let's dive into some cool activities to become super sleuths in spotting phishing emails!

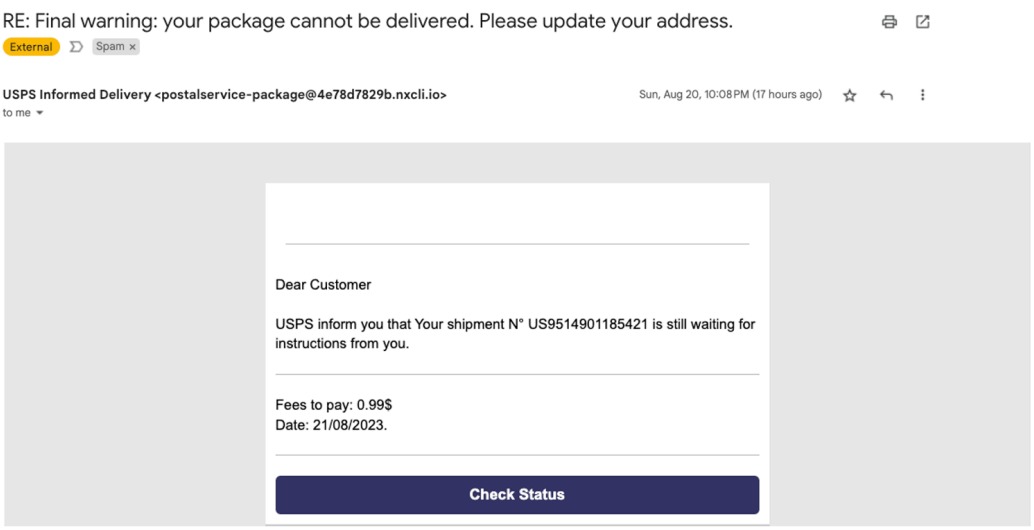
1. **Phishing Detective Challenge:** Take a look at a bunch of different email examples. (see below) Your mission? Figure out which ones are sneaky phishing attempts and which ones are safe. Are they trying to trick you into giving up your personal info, or are they just regular emails?

2. **Make a "Phish or No Phish" List:** Once you've played detective, create a list for each email. Why do you think it's a phishing attempt? Or, if it seems legit, why do you trust it? Look for clues like weird email addresses, strange links, or urgent language. Share your findings with your classmates or friends. This is like being a digital detective!

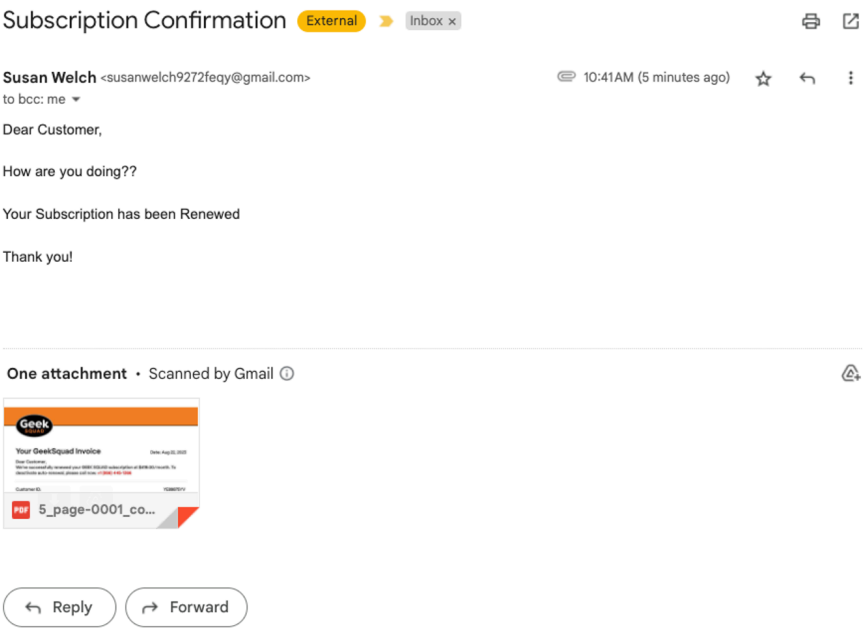
3. **Phishing Awareness Campaign:** Want to take it a step further? Share any phishing attempts you've personally received (make sure to remove any personal info first!). This can help others learn what to look out for. You could even make a cool presentation or a

digital poster warning about the dangers of phishing. Sharing is caring, especially when it comes to staying safe online!

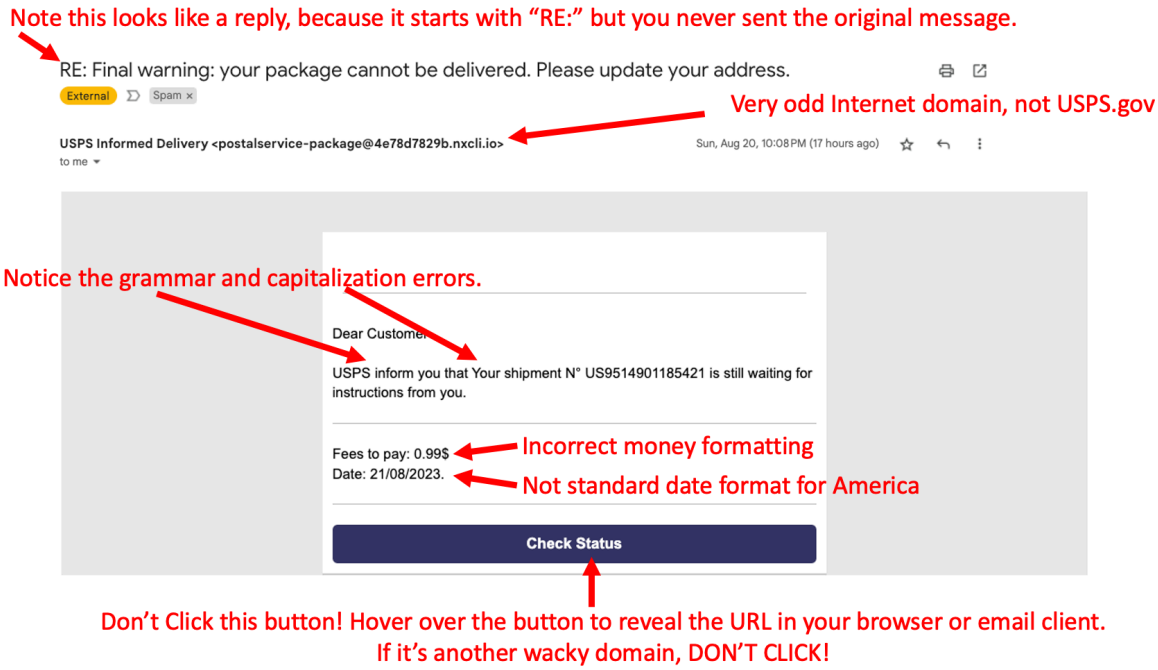
Potential Phishing Email #1



Potential Phishing Email #2



Analysis of Email #1



Analysis of Email #2