Phishing for Some Information

TOPIC: SOCIAL ENGINEERING

GRADES: 3-5

LESSON DURATION: 45 MINUTES

SOFT SKILLS: COMMUNICATION, CRITICAL THINKING

Introduction:

- This activity should be done with students who have access to devices. The topic is abbreviated and simplified for this age group. It is best coupled with the activity on P.I.I.

Learning Outcomes:

- Students will have a basic understanding of what the term social engineering means.
- Students will recognize “phishing” attempts versus reliable emails/texts.

Materials:

- Presentation
- Worksheet
- Video from Google Education: Stay Safe from Phishing
- Optional worksheet for students to complete

Activities:

1. The teacher should explain that today students will learn more about being safe online. Sometime things on the internet are not what they seem. Today’s topic will be social engineering.
2. The teacher can begin with a breakdown of the term: social=people; engineering=to build/make. Therefore social engineering is the attempt to trick people into doing something that you want. In this case, give away private information online so it can be used for bad.
3. At this stage, the teacher can review the information learned during the PII lesson.
4. The teacher should ask students why someone would want their information? What would they use it for? What information is valuable to others?
5. The teacher can then explain in a basic fashion, how this information might be taken if social engineering is used. It’s a tactic called phishing. A presentation is available here and the teacher can modify as needed.
6. As a wrap-up the students should complete the worksheet in the Materials section. Question 3 is especially important for this topic as students have to decide which email is okay to respond. The left graphic is a great example of phishing. The teacher may also choose to show students concrete examples of phishing emails that he/she has received.

7. End the activity by showing the phishing video from Google Education. The video is 3:15 minutes long.
8. It is important to note, that in today's world social engineers are going "old school" again. Their attempts don't just come through email or text. Phone calls are now a jackpot for social engineers. The reason it works=humans are innately good, trustworthy people. Therefore we fall for these attempts even though we know it exists. Sometimes we are in a hurry, sometimes we fall for the story, etc. The tactics are also always changing. As long as students know that social engineering is a threat and learn the basic skills to combat it (don't click, slow down, open or trust things that you cannot verify, look for the warning signs (nothing is free, time sent, spelling errors, etc.), the chances of being a victim decrease.