Understanding Social Engineering

TOPIC: SOCIAL ENGINEERING

GRADES: 3-5, 6-8

LESSON DURATION: 30-45 MINUTES

SOFT SKILLS: COMMUNICATION

Introduction:

- This lesson should only be done with students who have access to devices both at school and at home. Teacher discretion is advised.

Learning Outcomes:

- Students will define the term social engineering.
- Students will recognize basic examples of social engineering and develop protections against becoming a victim.

Materials:

- Presentation (editable)
- Worksheet for home practice/outreach

Activities:

1. The teacher should explain to students that today they will learn new vocabulary terms. The terms might be difficult, but it is important that students understand the basic ideas. Teachers may redesign this discussion based on the classroom knowledge base.
2. The teacher should introduce that today students will learn about social engineering. This is an example of unethical behavior. Teacher may choose to review the ethics of computing at this point.
3. In order to introduce social engineering, the teacher might find a current example from the news.
    - A sample current events article can be found at https://wccftech.com/russian-hackers-us-contractors-drone-secrets/ or through a simple google search.
4. The teacher can use the presentation to help students understand. It is also suggested that students be required to define difficult vocabulary terms as the presentation occurs.
5. The teacher may also choose to develop a Kahoot! to monitor students' learning of the concepts.
6. As continued practice, the teacher may require that students complete the worksheet at home with the help of a trusted adult. In this way, students are getting repeat practice and adults can learn/be reminded of online dangers as well.

Other Possible Activities:

1. The teacher can research and find examples of social engineering and place visuals at stations around the room.
2. Each station should be manned by an adult. The station should have a poster of either a legitimate online action/behavior or a social engineering attempt. Certain stations should also have parents that roleplay. For example, 2 separate stations should have phones available. One parent should role play a legitimate phone call attempting to sell something to the student. The other should attempt a vishing attack; trying to get personal information out of the student such as family member's names or location (Sample: Hello, is Judith there? Student: No Judith lives here. You have the wrong number. Hang up---GOOD or Student: No, I'm sorry this is the Smith house and my mom's name is Sandy.——BAD!
3. Students are then given a photo of themselves and should rotate through the stations.
4. Students must go to each individual station, look at the photo or interact with the parent and determine whether it is a safe, legit interaction or a social engineering attempt. If the students identify it correctly, they get to keep their picture and keep moving. If they are incorrect or misidentify the situation, they lose their picture and must sit down.
5. Have the parents keep a tally at each station of the number of students who get their item right versus those that get it wrong.
6. After all students are done, two different things can occur. First students could be required to graph the results from each station for math practice. Secondly, students should participate in a break out session and share what they learned. Which stations proved to be the most difficult? What mistakes did they make and why? Were certain parents good at tricking the students and what behaviors did they use?
7. Sample situations/stations include: picture of a "spoofing" Facebook email that asks you to enter your username and reset your password except the email came from "Facbook; Facbook@spamware.com". (bad) An email from UPS asking for your delivery address so they can deliver a package you ordered. (bad) An email from Pinterest telling you to go to your account and reset your password due to suspect behavior (no link in email). (Legit). An email from your grandma asking you to call or text because she misses you. (Legit) Pop-up chat box while online gaming that asks you to verify your identity (Fake).