Cyber Security Lesson Plan

Lesson Title: "Catching Phish"
+Level: Middle School / High School

Summary: Students will practice evaluating messages to determine if they represent phishing attempts.

Learning Objectives/Outcomes: Upon completion of the activity, the student will be able to estimate the likelihood that a social media message involves an attempt to phish the user's personal data.

Learning Types: The student will rate messages using a Likert scale. The justification for each rating will be explained using complete sentences. Students will participate in a class discussion to consider the tabulated results.

How will you facilitate learning? Warm up activity, focused activity closure, reflection? The lesson will begin with an anecdote describing a teen's personal data that has been phished. A brief discussion of phishing indicators will occur. Then, each student will view several messages as they may appear on various social media platforms. After reading the message, the student will use a Likert scale to estimate the likelihood of a phishing attempt. At the end of the activity, the class will have a discussion of the tabulated results.

Materials List: Students will need a device with which to complete a Google form.

Accommodations: No special accommodations are needed.

Description of Activity: The following phishing clues will be discussed—

1) Generic or missing greeting
2) "Friend" in trouble
3) Too good to be true
4) Spelling, grammatical, and obvious factual errors.
5) Alert! Alert!
6) Sense of urgency
7) Shortened URL

Several messages will be presented on a Google form as they might appear on a social media platform. The student will rate the likelihood of each message being a phishing attempt by using a Likert scale. The student will use complete sentences to explain each rating.

Ratings from all of the students will be tabulated. Then, students will discuss the tabulated ratings together.