OPEN WIFI : MAKING A PSA FOR “PARENTS”

Lesson Description:

In this lesson instructors explain the risks of using public wifi. The instructors ask the students to create an announcement detailing the information that they have learned. This announcement is intended to be seen by their parents, friends, or people in public spots.

Prerequisite Knowledge:

Students should have familiarity with ethical practices of cyber security.

Length of Completion: 50 minutes

Level of Instruction: This lesson is appropriate for middle and high school students and all levels of learners.

Applicable First Principles &/or Concepts: Please select the Principles or Concepts covered in this lesson.

GenCyber First Principles

Domain Separation

Process Isolation

Resource Encapsulation

Modularity

Least Privilege

Abstraction

Data Hiding

Layering

Simplicity

Minimization

GenCyber Cybersecurity Concepts

Defense in Depth

Availability

Confidentiality

Integrity

Think Like an Adversary

Keep it Simple

Resources that are Needed:

For this lesson the resources needed include:

- Computers and graphic programs such as "Microsoft Paint" or "Canva" if they want to make a virtual poster.
- Markers, colored pencils, colored paper if they want to make a poster by hand.
- Recording device if they want to make a video

Accommodations Needed: N/A

LEARNING OUTCOMES

Students should be able to:

- Compare different different types of network security keys
- Apply what they have learned in this lesson when connecting to a wifi network, private or public.
- Identify security risks when connecting to a public wifi network
- Explain the concepts learned in this lesson to their peers and family.

LESSON DETAIL

Interconnection: This lesson is connected to Online Safety workshop.

Assessment: Summative assessment - At the end of the session students have created a tangible announcement summarizing everything they have learned during the session. This announcement is checked for vital information.

Extension Activities:

Watch videos and discuss with a partner:
https://www.youtube.com/watch?v=9WI8XC5gdxw

and
https://www.khanacademy.org/computing/computer-science/internet-intro/internet-works-intro/v/the-internet-wires-cables-and-wifi

and
https://www.betternet.co/blog/4-reasons-why-you-shouldnt-use-public-wi-fi/

Differentiated Learning Opportunities:

At the end of the work day, students summarize the concepts learned throughout the day by making a video using “Flip Grid” video.

For students that are already familiar with the lessons’ concepts, the instructors engage students with research encryption algorithms and make a poster describing the one they think works best and have them do an analysis of why they think this encryption algorithm is better than others and have them list the pros and cons.

LESSON

Warm Up:

Open box in the front of the room. Students might look in and ask why it is there. After class begins...
The instructors ask how many people have connected to public wifi networks in airports, coffee shops, malls, etc.
The instructors ask if the students are familiar with the risks of using a public network.
The instructors explain issues to consider when using public wifi.

Lesson:

1. Explain what Wi-Fi is, having them recall what they have done with the radio features of the Micro:Bit and how it relates to wi-fi connectivity.
2. Go over the different risks that go along with using public/private wifi networks.
3. Go over the different network security keys: WPA, WPS, WEP. Also, explain HTTPS in contrast to HTTP.
4. Ask students to plan an announcement that they could give to their parents, peers, or display on a public place. The announcement should provide information about the risks of connecting to public wifi networks and ways they can be safer while using these networks. These announcements can be posters (virtual or physical) or a video.
5. Debrief with the students and have them briefly present their posters.