Understanding How TLS Works

TOPIC: FOUNDATIONAL PRINCIPLES OF CYBERSECURITY

GRADES: 6-8, 9-12

LESSON DURATION: 45-60 MINUTES

SOFT SKILLS: COMMUNICATION, CRITICAL THINKING

Learning Outcomes:

- Students will understand basic public key encryption methodology.
- Students will apply this understanding to the process of safe e-commerce transactions.

Materials:

- Background reading for teacher
- How TLS Works Handout

Activities:

1. The teacher should introduce the lesson. Today's topic is encryption methodology. Specifically, we will talk about the use of SSL and TSL in data encryption.
2. Ask students for a definition or recognition of the terms SSL and TLS. SSL=secure sockets layer; it has since been replaced by TLS=transport layer security. For our sake, TSL is an updated, more secure version of SSL. It is the methodology used for encrypting data across web services.
3. It is important to note the influence of e-commerce on cybersecurity. Without e-commerce and online shopping, encryption may not relate to as many people. However, due to the fact that many of us shop online for something, it is important that we understand the basics of how the transactions are protected.
4. At this point the teacher can hand out the worksheet entitled, How TLS works. Each student should have a copy.
5. Talk through and read the example in class.
6. Afterwards, review the information and answer any questions that may exist. Remind students that major websites will use this method as well as be secure (https://) in order to make our transactions as safe as possible.

Remedial Pre-activity:

1. If students have no background knowledge on these topics, it would be best to begin with a remedial simulation. Instructions are below. This should be done prior to going over the hand out.
2. Secret handshake game:

- Students should partner up. Each pair should be given 3 minutes to develop a SECRET handshake that only they know.
- Then, select 2-3 students at a time to be the “authenticators” – have the authenticator students wear a blindfold and sit in a chair.
- Each authenticator should have written note beside them that states either – true or fraud. The student should not see the note.
- Send the students’ actual partner and a second student (fraudster) over to the blindfolded student.
- The authenticator asks, “Who’s there?” and the authenticator’s real partner says his or her name.
- Then, depending on the what the written note says, either the real partner OR the second student attempts to do the secret handshake and get “authenticated.”
- If the handshake is right, the student who did it is authenticated and gets a token. Then the authenticator takes off the blindfold and audits who was authenticated – is it the partner?

3. Debrief discussion – were there any types of handshakes that kept out fraudsters? How difficult was it for the authenticators to determine their partners handshake? What would they do different the next time around to protect their partnership and secret handshake?
4. Explain to students that this is similar to what goes on inside a computer within a network all the time. And just like the handshake game, sometimes the information is secure and sometimes (most times) it’s not and we can be fooled.