Someone Could Listen

Review Questions

Answer Key

1. When you visit a website, the path the information takes between your computer or phone and the server where the website's content is stored is not simple.

    a. Give examples of *two* other devices that might be part of that path.

    Examples might include: Wireless routers, wired routers, DSL/cable modems, cell towers, phone lines, network hubs, switches, satellites, other servers….

    b. Can the people who own or control those devices see the information you send, or that the website sends back to you? Why or why not?

    Answers might include:

    In most cases, they could capture the data, but if it's well-encrypted at a different layer, they can't actually make sense of it/use it.

    It depends on their hacking skills.

    Students may also give specific examples, such as that someone else who has the password to your wireless router may be able to see your data, but if it's also encrypted by the website, they can't read it.

    c. Does the information take the path with the shortest distance? Explain your answer.

    Target answer: No; it may go all over the place geographically.

    Ideal answers may explain that part of the path depends on which cell towers or lines/hubs your service provider owns or has access to and/or that data is split up and sent along different paths, in part to make sure no one transmission line gets overloaded.

2. What does a password-protected wifi network do to protect your information that a wifi network with no password doesn't do?

    Target/ideal answer: Communications on a password-protected network are encrypted (the communication between your device and the wireless access point is encrypted), so that devices outside the network can't see them by listening in on the wifi signal. Communications on an open wifi network are visible to everyone (unless encrypted at another layer).

3. Password-protected wifi networks are often called “secure networks” or “private networks”, while wifi networks with no password are often called “public networks”.

   Are password-protected networks always private and safe to use? Why or why not?

   Target/ideal answer: No; if you are on a network where lots of people have the password (like schools, libraries, or coffeeshops), anyone else who has the password (as well as the provider of the wireless access) can see your communications (unless encrypted at another layer).

4. Name one thing you can do to protect yourself better when using a non-password-protected or public/shared wifi network, and explain in one sentence how that method or tool works.

   Examples may include: Check for HTTPS when connecting to websites, encrypt your email, use a VPN and/or proxy service.... These methods ensure all communication is encrypted between you and the HTTPS-enabled website, or between you and the VPN/proxy.

5. Besides your answer in (4)...

   a. Name *two* other things you can do to make it harder for others to eavesdrop on your online activities.

   b. For *each method* you named in (a), explain in one sentence what kind of eavesdropping or attack that method prevents.

      Good examples might include:

      Using strong passwords prevents hackers from guessing them (using password-guessing software).

      Using two-factor authentication makes it harder for hackers to use a password they’ve already gotten.

      Installing virus/malware protection makes it harder for malware to install itself and run on your computer to capture your information and/or attack other computers.

      Paying attention to browser warnings prevents you from man-in-the-middle attacks/protects you from hackers capturing information you thought you were sending to a trusted website.

      Using a proxy or VPN means your ISP can’t see what websites you visit, and websites can’t see your IP address.

      Checking that websites and apps are using HTTPS means your data is encrypted so hackers who try to capture it along the way can’t read it.

6. In one sentence, how does encryption protect your online communications?

   Target/ideal answer: Encryption uses a code to scramble the data so it looks like jibberish to any person or computer who doesn’t have the key to decode it.