Public Wi-Fi

Created: March 2016
Last Updated: July 2018

Estimated time:	60 minutes ● [10 minutes] Activity #1 ● [15 minutes] Activity #2 ● [10 minutes] Activity #3 ● [10 minutes] Activity #4 ● [15 minutes] Assignment
Group or individual activity:	Group
Ages:	15-18 years old
Grades:	Grades 10-12
Online / offline elements:	This learning experience contains links to online resources to help facilitate a group-based discussion, with an offline writing assignment.
Areas:	Main area: Security Additional areas: Digital Access, Information Literacy, Privacy and Reputation
License:	

Learning Goal

Participants will learn about public Wi-Fi networks and their benefits and risks. More specifically, they will learn to recognize unsecured Wi-Fi when it's available to them,

understand the tradeoffs inherent in using unsecured Wi-Fi and make informed decisions about when to connect to and use unsecured Wi-Fi.

Materials

- [One per group of 2-3 participants] Handout: Connection Safety [educator version and participant version]
- [For educator] Computer with Internet access
- Projector and projection screen
- [One per participant] Paper
- [One per participant] Pens or pencils

Resources

- Article: Why You Should Be Using a VPN (and How to Choose One) - by Alan Henry (Lifehacker)
- Article: Staying Safe On Public Wi-Fi This Summer - by Rebecca Kielty (The Family Online Safety Institute)
- Article: Choosing the VPN That's Right for You - by The Electronic Frontier Foundation
- Wikipedia Entry: Transport Layer Security - by Wikipedia
- Video: FTC: Public Wi-Fi Networks - by The United States Federal Trade Commission

Activity #1: What is Wi-Fi?

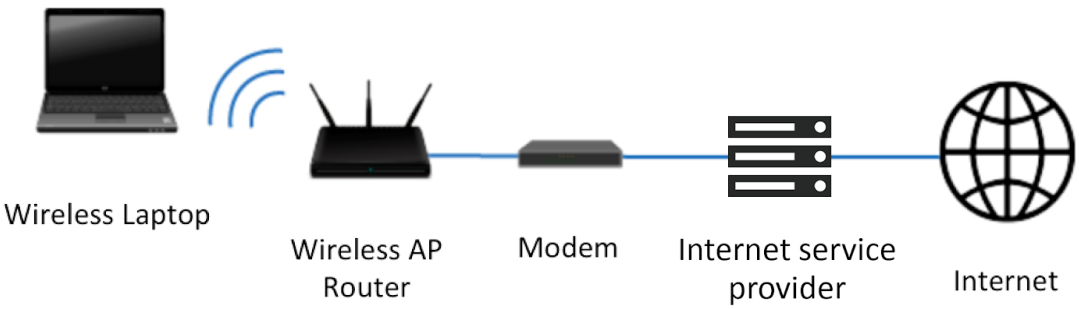
ASK:

- Which devices do you use to access the Internet?
- How do those devices connect to the Internet? [Wi-Fi]

SAY:

- Wi-Fi is a common way to connect devices to the Internet. Wi-Fi uses radio signals to connect devices without a physical or wired connection.

- Imagine that you have a laptop in your home that you'd like to connect to the Internet. To do that, you will need the following:
- [To visualize the various components of a Wi-Fi connection, please project the diagram below on a projection screen.]



- **An access point:** An access point is anything that transmits a Wi-Fi signal and provides access to the Internet. Your devices need to pick up these signals to connect to the Internet. Sometimes you may need special permission (e.g., a username and password) to sign in and use the wireless signal that an AP transmits.
- **A router:** A router is a device that creates a network between all the devices (such as desktop computers, tablets, mobile phones) in a given location (like a school, library, or your home). Typically, routers have an access point built into them (see diagram).
- Routers have a limited (usually short) range. That's why if your device is too far away from the router, you will get a weak Wi-Fi signal or none at all. Also, if there is something between you and the router (such as a building or a brick wall), that will reduce your signal.
- Although connecting to a router offers access to a network, this does not automatically translate to Internet access. For several devices on a network to be able to connect to the Internet, a router has to be connected to a modem.
- **A modem:** A modem is a device that creates and maintains a connection to your Internet Service Provider (ISP) to give you access to the Internet. It converts

signals from outside your given location into signals that can be read by your computer and other digital devices.

- In a typical set up, the AP and router are a single device that is physically connected to the modem, using a special cable called an Ethernet cable. This is what is referred to when people talk about a "wired" Internet connection.
- Mobile devices can also use a cellular connection to connect to the Internet, especially if they are not in a school, library, or home network. Cellular connections are a type of wireless radio signal that has a much larger coverage area than a router has. Cellular connections use particular transceivers, called cell towers, to connect your mobile device to the Internet.

ASK:

- What are the benefits of Wi-Fi?
- What might be some of the drawbacks of Wi-Fi?
- [If not brought up, ASK]: What might be some security concerns when using Wi-Fi versus a wired Internet connection?
- Why is it that you lose Wi-Fi access on your phone as you leave a building?

Activity #2: Choosing a Wi-Fi Network

ASK:

- Are all Wi-Fi networks safe? Why or why not?

SAY:

- Sometimes, you are given a choice as to which Wi-Fi network you would like to use. It's important to remember that there are serious risks if you connect to the wrong network. For instance, unsecured Wi-Fi networks are those that don't require a password to log in. If you are on an unsecured network, it's possible for other people on the same network to see your information. They may steal information you send over the network or monitor what you are doing.
- On the other hand, secure and trusted Wi-Fi networks are those that are encrypted (encryption scrambles the information you send and receive over a network, so it's much more challenging for a hacker on the same Wi-Fi network to see what you are sending or receiving), and those on which you are certain the network you are signing into is the one the network name is representing. For instance, signing into a network impersonating the name of your school's network

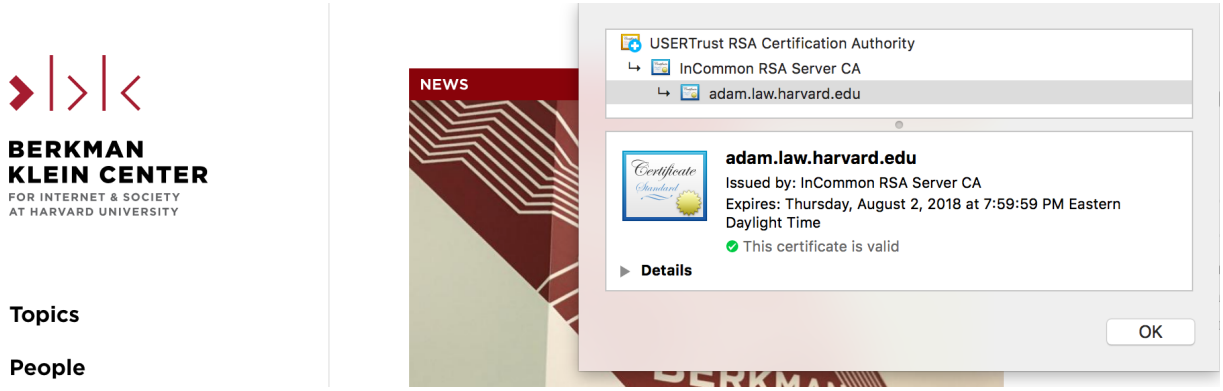
could lead to account information disclosure. Therefore, networks that are secure and trusted are the ones that offer the most protection.

- One thing to consider is the context or location of the Wi-Fi network. For example, if you are at the movie theater and you see your school's network name on your phone when looking for a Wi-Fi connection, you might consider that network is trying to imitate or "spoof" your school's network to collect passwords from unsuspecting students.
- When setting up a password-protected Wi-Fi network, the owner must select an encryption protocol. Common encryption protocols are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2. These protocols make it so that the information that is sent wirelessly over the network is encrypted (or "scrambled").
- Encryption was created to make it more difficult for hackers to see what you are sending. All of these protocols (WEP, WPA, and WPA2), however, have been shown to be vulnerable to hacking. Therefore, it's important to also rely on secure web connections when transmitting information online.
- HTTPS is a standard used by websites to encrypt data passed over the Internet. Encryption can prevent any third party from easily viewing the data from your connection. It provides an extra layer of security and can be used in any browser by adding "https://" in front of the URL you use (e.g., https://www.mysite.com). However, not all websites support HTTPS.
    - You should only enter sensitive information (e.g., passwords, credit card information) on web pages with the HTTPS:// prefix.
    - You can use software tools to ensure you always use HTTPS whenever possible. One such tool includes the browser extension HTTPS Everywhere.
    - Most major browsers have security indicators that look like locks near the address bar to indicate HTTPS connections.
    - Unfortunately, HTTPS does not guarantee that you are safe as some malicious websites can also support HTTPS. HTTPS secures the connection but does not ensure the website is a good actor.
- Secure Sockets Layer (SSL) / Transport Layer Security (TLS) are names for the technology that keeps HTTPS secure. SSL / TLS uses digital encryption keys, which work a lot like real keys. If you wrote a secret on a piece of paper for your friend, whoever found the paper could see your secret. Instead, imagine you gave them a copy of a key in person, and then sent your secrets in matching locked boxes. If someone intercepted the box, they would have a hard time seeing your secret without the key. If someone tried to replace the box with a

similar-looking one, you would notice that your key would not work. SSL / TLS works the same way but with a website.

- Browser security indicators will also communicate Extended Validation (EV) certificate information. EV certificates are given to websites that verify their owner's identity to a certificate authority. In browsers, sometimes the EV indicator takes the form of the website's name or the registering entity next to the address bar. If you're suspicious of the content on a particular website, you can check to see if the URL in the certificate matches the URL in the browser by clicking on "View Certificate."

[It's helpful, on the projection screen, to demonstrate to participants how to find "View Certificate." How you navigate to this varies by browser. For example, on Chrome, click on View -> Developer -> Developer Tools -> Security tab -> View Certificate. (See image below for an example of what the "View Certificate" screen may look like, which will depend on the site you're on).]



ASK:

- What should you think about when connecting to any new network? [Possible answers include: location (or who owns the network), access (or who else is connected to the network), and activity (or what they are doing on the network).]
- Who owns your home's Wi-Fi network? At school? At a coffee shop? [Their parents / caregivers own their home's Wi-Fi network. The administrators and / or the district own the network at school, and the owner owns the coffee shop network.]

- Do you know these people personally? Do you trust these people? [Engage participants in a discussion about how they might trust these people differently.]

SAY:

- You should know and trust the person hosting the Wi-Fi network you are using. Sometimes, you can determine who the owner is using the network's SSID.
- The Service Set Identifier (SSID) is the name given to a Wi-Fi network that you can see when you try to connect. The SSID is often used to communicate who owns the network and other details about the network. Be careful though as nearly anyone (who knows how to) can create a SSID. For example, someone can create create a SSID that is identical to the one you use at school. This is an example of impersonating a known and trusted network, to potentially harvest usernames and passwords.
- Knowing who is hosting the network can help you determine whether the network is secure. If it belongs to a person or organization you trust, then you will likely feel comfortable connecting. However, if it's an unknown network, you should not connect as you don't know who owns the router to which you are connecting [For more information about what a router is, please view "Activity #1: What is Wi-Fi?"]. Because all traffic on the network goes through the router, the owner could be monitoring or recording your web traffic.
- When you connect to Wi-Fi, your device is connected to a local network of devices, and that network connects to the broader Internet. Because your device is exchanging information with this network, it's important to trust the other devices you're connected with — and that means any device on the network. It's just like group work you do in school — you want to be able to trust the other people you're working with!
- Using a password on the network may limit who can connect to it. This means you will have a better idea of who is on the network — whether it's your family, your friends, or other customers in a coffee shop — than if the network was completely open.
- Whether or not you decide to join a network that may might seem suspicious comes down to the trade-offs you are willing to make in terms of online security. You might consider, how should I weigh the potential of my account being breached versus the convenience of joining an available network?

ASK:

- Should you read online news / a blog using your home's Wi-Fi network? At school? At a coffee shop? [Explain that the content of a webpage is generally not sensitive information. You can probably do this on any network.]

- Should you send a credit card number using your home's Wi-Fi network? At school? At a coffee shop? [Engage in a discussion around why it's safest to do so with their home Wi-Fi and not with the coffee shop Wi-Fi. Also discuss how, while a school's network is likely trustworthy, it may not be worth the risk since this particular information is highly sensitive.]
- Should you check your personal email using your home's Wi-Fi network? At school? At a coffee shop? [Discuss how it's probably safest to do so with their home network, depending on the content of the email account. For example, some individuals have multiple emails accounts that they use for different purposes (e.g., marketing / promotion emails for one account; emails to friends and family on another account).]

SAY:

- Sensitive information, including passwords and bank information, are better sent / viewed on a private and secure network, on websites using SSL / TLS rather than on a shared public network. This private information is at risk if you submit or access it while on a shared network being used by people you don't know or trust.
- It may not be clear how sensitive or not sensitive information is because privacy is a personal decision that you must make for yourself. It's important to consider each situation on its own to determine whether you should connect to the network. Ask yourself if you trust the network's owner, others connected to it, what activity you are doing online, and what information you are sharing before deciding to connect or not.

Activity #3: Secured and Unsecured Networks

[Please note: Part of the content of this activity has been covered in "Activity #2: Choosing a Wi-Fi Network." We defer to your judgment regarding whether or not you would like to go over this material again if you have already engaged in Activity #2, or skip it.]

SAY:

- Unsecured Wi-Fi networks are those that don't require a password to log in. The use of unsecured networks poses a risk to the data you transmit and receive over the network.

- Secured Wi-Fi networks are those that require a password and have encryption enabled. The person who configured the network is the one who chooses whether or not to enable encryption. Encryption scrambles the information you send and receive over a network, so it's much more difficult for a hacker on the same Wi-Fi network to see what you are sending or receiving.
- Just because a network is secured does not mean that your data is safe. It's certainly more reliable than using an unsecured network; however, a determined hacker may still find a way to access your information.
- There are three common encryption protocols for Wi-Fi networks: They are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2. WEP and WPA are outdated, and relying on these should be thought of as unsecured. Furthermore, WPA2 has also been shown to be vulnerable to hacking.
- To make sure your information is protected to the fullest extent, check to see that the websites you are using are encrypted using SSL / TLS.

ASK:

- Can anyone think of an example of a password-protected network that they have used? [Some examples include their home Wi-Fi, a school's Wi-Fi, and Wi-Fi networks at some public locations like cafes.]
- Can anyone think of an example of an unsecured network that they have used?
- How about examples of a secured network?

SAY:

- You can check whether a Wi-Fi network is encrypted by examining the network or wireless settings on your device.

[Before this activity, conduct an Internet search to review how to check Wi-Fi network encryption types for different operating systems. Then, on the projection screen, demonstrate how to find out what kind of encryption a network uses. For instance, on MacOS, click on System Preferences -> Network -> Select Wi-Fi -> Select the appropriate Network Name. Under the Wi-Fi tab, there will be a list of known networks and a column indicating which encryption type is used.]

- Not all connections are equal. When a network is unsecured, anyone can connect to the network, and it's unclear who controls the network. Joining an unsecured network leaves you vulnerable, because the information you send and receive, like your web traffic (pages, passwords, etc.), could potentially be viewed by anyone on the network if you aren't using an SSL / TLS connection.

[Depending on your participants' technical knowledge, you may wish to discuss the use of Virtual Private Networks (VPN) as an additional layer of security when using Wi-Fi. Please refer to the VPN link in the Resources section for further information.]

Activity #4: Recognizing Connection Safety

[Divide participants into groups of 2-3. Pass out Connection Safety: Participant Handout and assign a scenario to each of the groups. Give participants 5 minutes to discuss their scenarios. Afterwards, ask groups to share their responses. The answers are in green on the educator handout.]

Assignment

SAY:

1. Draw a timeline of a regular day, marking the Wi-Fi networks to which you connect.
2. From the selected networks depicted on the timeline, choose two, and in a short paragraph for each, describe the network — who else is connected to it? How secure is it?
3. Additionally — for the two networks chosen — describe what opportunities connecting to these networks come with and what the associated risks might be.

Connection Safety: Participant Handout

For each scenario, consider the location, level of access, and the activity you are doing online. Then determine whether the risk of doing the activity is low, medium, or high and explain why.

Location	Access	Activity	Risk
Friend's house	Your friend's family	Online game	
Coffee shop	Customers only	Social media	
Library	Members only	Financial transaction	
Airport	General public	Email	

Connection Safety: Educator Handout

For each scenario, consider the location, level of access, and the activity you are doing online. Then determine whether the risk of doing the activity is low, medium, or high and explain why.

Location	Access	Activity	Risk
Friend's house	Your friend's family	Online game	Low: There is a small number of people on the network, and you trust them. The activity probably does not include sensitive information.
Coffee shop	Customers only	Social media	Medium: Social media is not necessarily sensitive, but anyone who has been to the cafe before will have access to the network and may be able to steal your passwords.
Library	Members only	Financial transaction	High: Banking information is highly sensitive, and while the library's access is somewhat limited, you don't know who might maliciously access your information.
Airport	General public	Email	High: Even if your email is not sensitive, using a public network is unsafe.