Cybersecurity, Phishing, & Spam

Created: March 2016
Last Updated: July 2018

Estimated time:	85 minutes ● [20 minutes] Activity #1 ● [20 minutes] Activity #2 ● [15 minutes] Activity #3 ● [30 minutes] Assignment Depending on the time you have allotted for each group meeting, we suggest you engage in the final exercise of this learning experience ("Assignment") in your second group convening.
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: Information Literacy, Privacy and Reputation, Safety and Well-being
License:	

Learning Goal

Participants will learn about malicious online users who might attempt to use security weaknesses to gather information about them. Participants will be able to describe some of the security risks associated with being online, develop strategies to engage in safer behaviors, identify spam messages, and explain who should ask for their password.

Materials

- [One per group of 2-3 participants] Handout: Spam [educator version and participant version]
- [For educator] Computer with Internet access
- Projector and projection screen
- [One per participant] Paper
- [At least one per participant] Colored pens or pencils

Resources

- Report: Access to Social Media Usernames and Passwords - by The National Conference of State Legislatures
- Browser Extension: HTTPS Everywhere - by The Electronic Frontier Foundation
- Browser Extension: uBlock Origin - by Raymond Hill (GitHub)
- Browser Extension: Privacy Badger - by The Electronic Frontier Foundation
- Browser Extension: Ghostery - by Ghostery

Activity #1: Online Risks

SAY:

- When you use the Internet, you may expose yourself to risks through the mere act of accessing a web page, communicating online, or downloading data. It's sometimes possible for websites you access, people on the same network, or even third parties to figure out your location or other information about you when you browse.

ASK:

- Who might take advantage of online security vulnerabilities to see your personal information? [Possible answers include malicious hackers, government surveillance, etc.]

SAY:

- When you browse the web, it's possible for malicious hackers to collect data on you the same way Internet providers do. To reduce this risk, you must access websites using a secure connection. Regardless of your connection, many websites try to track your usage patterns across multiple platforms. They can watch your browser, location, and other usage patterns to try to figure out who you are.

ASK:

- Why might malicious hackers try to access your information online? What information are people looking for? Why would a website you are not logged into want to keep track of who you are? [Any personally identifiable information and any information that can be sold or used for monetary gain.]
- Does anyone know what malware is? What can it do?

SAY:

- Malware is a harmful code that surreptitiously runs on your computer. Some malware can collect data from any part of your local computer, from your hard drive to your browser data. It can also allow hackers to take control of your computer and use it any way they'd like. Most malware is simpler though, such as websites that imitate secure portals like a bank or extensions that put advertisements in your browser to make money.

ASK:

- What can you do to protect yourself against malware, spying, or tracking?

SAY:

- Be careful when clicking links, ads, or social media posts. Does the URL match what you expect? Do you get to the same page when you type it again yourself or search for the website? A good rule is that SSL / TLS should protect any login page for an important account (like Google, Facebook, Twitter, or bank accounts). SSL / TLS makes it very hard for a hacker on the same network to send you a fake website if you type in the correct URL, which could otherwise be very simple.

- Some websites will be able to run code to access your personal information or online accounts if those platforms make a coding mistake. They can then use your accounts to spam others.
- Only download or install software from trusted sources and be thoughtful about when you download executables (.exe, .pkg, .sh, .dll, or .dmg extensions). Executables are anything that will execute an action on devices such as desktop computers and mobile devices. Sometimes, these can be bad actions. For example, someone can write an executable text to erase someone's hard drive or install a fake browser. This is why you should only download and install things from trusted sources.
- You can use anti-virus software to prevent you from running malware. Some anti-virus software comes with your computer (e.g., Microsoft Security Essentials for Windows); while some operating systems, like those on Apple computers, have security settings that block software from untrusted sources from being installed. Think carefully before overriding these settings.
- You may also consider browser extensions like Privacy Badger that can, for instance, block plug-ins that make it harder for websites to figure out who you are or track you. The same plug-in, however, can block the functionality of websites, such as the ability to watch videos. Whether or not you decide to install browser extensions comes down to your preferences and the trade-offs you are willing to make in terms of online security. You might consider questions such as, How inconvenient is it for me to be tracked? How much is my privacy worth? How much do I want to watch this piece of content (if, for instance, the browser extension blocks a plug-in that renders video)?

Activity #2: Security Tools

[Please note: Part of the content of this activity has been covered in "Activity #1: Online Risks." We defer to your judgment in terms of whether or not you would like to go over this material again if you have already engaged in Activity #1, or skip it.]

ASK:

- How do you know whether you are secure when you use the Internet?

SAY:

- Without taking the proper precautions, it's difficult, if not impossible, to successfully protect yourself against online risks [Various online risks are described in Activity #1.]
- New online risks also crop up all the time, so it's important to stay vigilant.

ASK:

- There is technology you can use to avoid or reduce these risks. Does anyone know of any?
- What are strategies and actions you can take to increase the likelihood that you, your device, and your information remain secure?

SAY:

- HTTPS is a standard used by websites to encrypt data passed over the Internet. Encryption can prevent a third party from easily viewing 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.

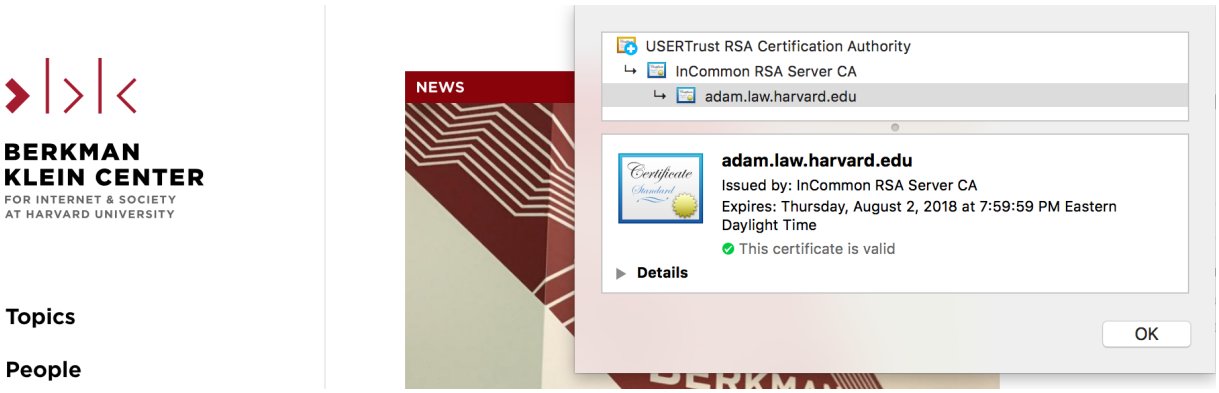
(Optional) ASK:

- Let's say I really needed to use the Internet, and there's only a public network available. If I use the HTTPS:// prefix for all the websites I use (e.g., social media, email, banking), will I be safe?
    - The answer to that question depends on what you are using the Internet for. As previously mentioned, not all websites support HTTPS. Also, HTTPS only secures your connection to the website; it doesn't guarantee that the website you are using is a good actor. If you really need to use the Internet, you should consider how sensitive the information you are trying to access is. Some people might decide not to use banking websites on

public Wi-Fi as a rule. Some people may decide that using social media on public Wi-Fi is not safe; others might weigh the potential consequences and decide how important it is to access social media at that moment.

SAY:

- 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 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 may be helpful, on the projection screen, to demonstrate how to find "View Certificate." How you navigate to this varies by browser. For example, on Chrome, under "View," click "Developer" and then "Developer Tools." From "Developer Tools" click the "Security" tab, then "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)].



- Aside from not running software from untrusted sources, anti-virus software can prevent you from visiting untrusted pages and downloading malware.
- The act of “phishing” primarily occurs over email from a spammer pretending to be a legitimate party. Spammers ask for your password, which they hope you will send over email or enter into a fake website. Spam filters can prevent some of these emails from showing up in your inbox. To make your spam filters more effective, be sure to mark any suspicious emails that end up in your inbox as spam.

ASK:

- What actions could you take to prevent yourself from accidentally downloading files that are harmful to your computer?

SAY:

- Always double check that you are accessing downloads from trustworthy websites. Be extremely careful about opening email attachments that you don’t recognize and clicking on pop-up windows and error messages. You might also consider installing reputable anti-malware programs on your computer.

Activity #3: Sharing Passwords

ASK:

- When do you think it’s okay to share your password? [Possible answers include shared accounts (e.g., a media streaming service).]
- What risks might be associated with sharing your password? [If a malicious person gets their password, then their account could be hacked. Sharing their password makes it more likely that someone will have access. If the same password is used on other websites, they could access those too.]

SAY:

- It’s standard practice that you shouldn’t share passwords with anyone besides the application that requires it for login. Phishing is the act of tricking someone into sharing their password [For more information about phishing, please view “Activity #2: Security Tools”].

- However, some people may explicitly ask for your password to access your accounts, claiming that your account may be in danger. While some of these people may have good intentions, like a friend who wants to help you look at something in your account that is puzzling you, it's unwise to share your password, especially if you use that password for multiple accounts. If you do plan to share a password, make sure it's not used anywhere else and use a password manager to share access. A password manager is a website / app that allows users to store their passwords. One example of a popular password manager is LastPass. [Feel free to project this site on the projection screen and briefly review some of the site's features.]
- Sometimes, the people asking you for your passwords may be adults whom you know and trust, like your parents / caregivers, teachers, or employer. Even though you know and trust these adults, typically it's a positive experience for everyone (both you and them) to have a conversation about why they are making this request and how they will handle your passwords. Especially with adults outside of your family, it's a good idea to ask them directly if there is a law or other type of rule that they believe requires you to give them your passwords.
- Asking polite and clear questions about laws and rules is particularly important when a password request comes from an adult outside your family whom you don't already know personally, like a law enforcement officer. If you are asked by a police officer or other government official for your social media passwords, stay calm and be respectful. Ask why they are making this request and which law(s) or rule(s) they believe gives them the right to have this information from you.
- Depending on the circumstances of a request by a parent / caregiver, teacher, employer, law enforcement officer, government official, or another adult, you may need to give them your passwords. The circumstances that would make you need to give your passwords include situations where there is a law or rule in place that requires you to do so or your judgment that the benefit you would get from their help outweighs the risks of password sharing.
- If you get a request from an adult for your passwords, and that request makes you uncomfortable in any way, seek out a parent / caregiver or other trusted adult immediately, ideally before you need to respond to the request.

ASK:

- Under what circumstances should you share your password online?
    - Only when you are prompted for your password on the website you are trying to access. Never share your password anywhere else, including over email, which is usually not encrypted or secure.

Assignment

[Divide participants into groups of 2-3. Distribute the Participant Spam Handout. Afterwards, have each participant develop a flowchart to show others how they might identify spam and whether they should share specific information with certain individuals / groups of people.]

SAY:

- Read each of the scenarios and discuss whether each message is spam and whether you should share information with the person or group of people in the scenario.

[Give participants 10 minutes to work on this exercise. Afterwards, ask groups to share their responses.]

ASK:

- When should you share your password over email?

SAY:

- It's standard practice for websites and companies to never ask for your password over email. You should never transmit your password to anyone this way, even if it seems like the source is legitimate. Email is almost never secure.

[Have participants return from their groups as the following exercise is for individual participants.]

SAY:

- Now, on a sheet of paper, develop a flowchart to show individuals how they might identify spam and whether they should share certain information online with others. It may be helpful to use a particular scenario to base your flowchart on; either one of the scenarios presented on the handout (if you choose to do so, please write the number of the scenario above your flowchart), or an entirely new one! If you decide to design your own scenario, please describe it in a brief paragraph above your flowchart.

[Give participants 15 minutes to create their flowcharts.]

Spam: Participant Handout

For each scenario, identify if the message is spam and if you should share information with the person. Please write your response to each question in the space provided.

Scenario 1
You receive an email from a lawyer, informing you that a distant relative has named you a benefactor to a sum of money. It reads, “To receive the money, please send me your bank account number and routing number so that we can complete the deposit.”

Scenario 2
A friend sends you a text, letting you know that they are trying to look up a photo you showed them earlier, but they do not have permission to see it. You can’t access your computer right now to send them the photo. They respond, “I can log into your account real quick to download the photo — what’s your password?”

Scenario 3
You get an email addressed to you from your school, noting that many student accounts have been hacked. They claim, “We have recently detected that many student accounts have been compromised. We apologize and are working to fix the problem. To reset your account, please respond to this email with your username and password.”

Scenario 4
You receive an email from your bank where you have a legitimate account. The email says that they have been hacked and that you should log in to change your account

password as soon as possible and change the passwords on any accounts that share the same password.

Spam: Educator Handout

For each scenario, identify if the message is spam and if you should share information with the person. Please write your response to each question in the space provided.

Scenario 1
You receive an email from a lawyer, informing you that a distant relative has named you a benefactor to a sum of money. It reads, “To receive the money, please send me your bank account number and routing number so that we can complete the deposit.”

This email is most likely spam. Even if they correctly use your relative’s name, they may not be who they claim. The sender could have obtained the information about your relation through other means. Sharing your bank account information is always risky and should be done cautiously. Never send your information to someone unless you contacted them first, and even then be very careful. For example, it’s probably not a good idea to share your info via email since it’s unencrypted. That’s why many hospitals, lawyers, and banks have special websites for communicating with their clients and patients.

Scenario 2
A friend sends you a text, letting you know that they are trying to look up a photo you showed them earlier, but they do not have permission to see it. You can’t access your computer right now to send them the photo. They respond, “I can log into your account real quick to download the photo — what’s your password?”

While this is not spam, you should not share your passwords with other people. Once they have your password, they can lock you out of your account or access other online accounts with the same password. Additionally, if a third party, hacker, or a bystander sees your message, more people could access your account without your knowledge.

Scenario 3
You get an email addressed to you from your school, noting that many student accounts have been hacked. They claim, “We have recently detected that many student accounts have been compromised. We apologize and are working to fix the problem. To reset your account, please respond to this email with your username and password.”

It’s common practice not to ask users for this information. Even if the sender looks legitimate, you should assume that any email asking for your password is spam.

Scenario 4

You receive an email from your bank where you have a legitimate account. The email says that they have been hacked and that you should log in to change your account password as soon as possible and change the passwords on any accounts that share the same password.

The correct course of action is to open up a new browser window and access the website as you would usually access it. A disclosure of this type (that accounts have been hacked) will typically be mentioned on the company or bank's customer portal. Instructions on the portal should be able to be followed safely. As in Scenario 3, no legitimate actor will request account credentials from you in an email.