(http://csmatters.org) 3 - 10

0b11 - 0b1010

Cybersecurity: Attacks, Protection, and Impact

Unit 3. Information and the Internet

Revision Date: Jan 05, 2020
Duration: 2 50-minute sessions

Lesson Summary

Pre-lesson Preparation

Assigning some of the research as homework will allow more in-depth research.

Summary

Reflecting on the fact that the Internet was not designed with security in mind, students will examine the devastating impact of cyber attacks. Students will study types of cyber attacks and the vulnerabilities they exploit and identify the roles of software, hardware, people, and the Internet. Students will identify potential cybersecurity concerns in systems built on the Internet.

Learning Objectives

CSP Objectives

- *EU CRD-1 - Incorporating multiple perspectives through collaboration improves computing innovations as they are developed.*
  - LO CRD-1.C - Demonstrate effective interpersonal skills during collaboration.
- *EU IOC-2 - The use of computing innovations may involve risks to your personal safety and identity.*
  - LO IOC-2.B - Explain how computing resources can be protected and can be misused.
  - LO IOC-2.C - Explain how unauthorized access to computing resources is gained.

Common Core Math:

- S-IC.1-2: Understand and evaluate random processes underlying statistical experiments

Common Core ELA:

- RST 12.4 - Determine the meaning of symbols, key terms, and other domain-specific words and phrases
- RST 12.9 - Synthesize information from a range of sources
- RST 12.10 - Read and comprehend science/technical texts
- WHST 12.1 - Write arguments on discipline specific content

Key Concepts

6.3 Cybersecurity is an important concern for the Internet and the systems built on it.

The Internet was not built with security in mind, leaving computers vulnerable to cyber attacks. This makes cybersecurity an extremely important concern when designing and implementing systems that are built on the Internet. Students need to be able to identify potential problems that could arise and potential options for protecting against these problems.

Essential Questions

- How is cybersecurity impacting the ever increasing number of Internet users?
- How does computing enable innovation?
- What are some potential beneficial and harmful effects of computing?
- How do economic, social, and cultural contexts influence innovation and the use of computing?

Outcomes

- Students will understand types of security violations.
- Students will understand types of protections.
- Students will compare negative impacts of different types of attacks.

Teacher Resources

Student computer usage for this lesson is: **optional**

In the Lesson Resources folder:

- "Cyber Security" : slides for instruction during the whole class
- "Cyber Attacks News Articles" : the list of news articles about real life cyber attacks for teachers (with instructions)
  - The diagram for the sticky note activity is in this document
- "Cyber Attacks Notes WS" : worksheet for students to use in taking notes on different types of attacks
- Consider including the TED talk about the first virus (about 17 minutes long) by Mikko Hyponnen https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net (https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net)

Journal Sample Response:

- "The Internet was originally designed to be used by a group of people who trusted each other. This means that it was not built with security in mind, but rather openness and sharing. Now that anybody can access the Internet, users cannot trust everybody else they are connected to. This means that security measures must be put in place to protect users and systems."

Example for Presentations:

Information to present about firewalls. (Included in the slides)

> “You can protect against certain attacks. One way to protect against them is a firewall.”

1. Where did the name come from?
    1. We have physical firewalls in school (and other buildings) that are designed to open to let people in and out, but close to keep fire contained (don’t let it through)
2. How does it work? Describe the process, making sure to note the role of each of the following: (not all will necessarily apply)
    1. A *firewall* is installed to be a barrier between a computer (or local network) and the **Internet**. A **person** has to purchase / install the firewall to protect their system. Firewalls can be **software** or **hardware** and sometimes people use both. Firewalls examine the packets attempting to go in or out from the computer (or local network) to/from the Internet. It can keep attacks like viruses out, and keep sensitive or private data in.
3. Visual from https://mdilog.com/help/security (https://mdilog.com/help/security)

Lesson Plan

(**Note**: There is a PowerPoint to be used with this entire lesson: **"Cyber Security Lesson Slides"** in the Lesson Resources folder.)

Getting Started (5 min)

In their journals or as a class, students should discuss the following:

1. Describe the “trust model” that the Internet was originally designed upon.
    - The "trust model" was introduced in Lessons 3-4, 3-5, and 3-6 that introduced the Internet.

2. List the problems with using the trust model, now that anybody can access the Internet.
3. Define cyber crime and cyber warfare. How are they different from everyday crime and warfare? (cyber crime: https://us.norton.com/cybercrime-definition (https://us.norton.com/cybercrime-definition) ; cyber warfare: http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/ (http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/))

Guided Activities (40 min)

Part 1 (10 min) - Readings

1. Each student will read a short article from the news about a specific attack that took place and identify the type of attack. Through their readings, the students will identify the negative effects of the attack. (A list of possible articles is in the "Cyber Attacks News Articles" document in the lesson folder.)
2. Students will use sticky notes to record the following information (at least one per student):
    1. The student's name
    2. The type of cyber attack
    3. The impact of the cyber attack
3. On the board, the teacher will set up space with the types of attacks on the y-axis, and the level of impact on the x-axis (see teacher resources). Students will place the sticky notes on the diagram where they think it fits.

Part 2

2a. Say: What can be done to protect our online security and privacy? Institutions can implement Multifactor (https://www.youtube.com/watch?v=07mRDyydCNY) and 2-factor authentication (https://youtu.be/0mvCeNsTa1g).
Show the videos: Multifactor (https://www.youtube.com/watch?v=07mRDyydCNY) and 2-factor authentication (https://youtu.be/0mvCeNsTa1g)Discuss: multifactor identification. Be sure all four points below are discussed. (Suggestion, play it like Family Feud, keep getting ideas until all key points below have been revealed and add other ideas as they are suggested)

1. Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.
2. Multifactor authentication is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge (something they know); possession (something they have), and inherence (something they are).
3. Multifactor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.
4. Require strong passwords.

2b. Say: What can we as users do?
Discuss with students what they think they can do. Be sure all six points below about what users can do are discussed.

1. Use strong and unique passwords for internet sites.
2. Control permissions granted to software to collect information and regularly review permissions granted to the software.
3. Avoid the installation of software from unknown or unreliable sources.
4. Keep antivirus and antimalware software up to date and active.
5. Keep operating system and application patches up to date.
6. Use a VPN whenever connected to a public wireless network.

Part 3

Group Projects

Individuals can manage passwords, network and credit card use.

1. Use strong passwords
2. Use a password manager
3. Use a password unique to each site.
4. When using a public network, use a VPN
5. Pay with Smartphones or smart cards
6. Use software data collection/privacy settings
7. Perform regular software updates.

Organize the class into seven groups and assign a topic above to each. Ask students to think about what the technology is, why it is important and how it is used.

Allow students five minutes to research the topics. Allow 5 minutes to prepare a poster about each. Present and answer questions about each.

Part 4

Survey of threats

4a. Say: All real-world systems have errors or weaknesses that make the susceptible to attack. One approach to making them safe is to detect and prevent these attacks. We are going to investigate malware and virus attacks. Show the video Malware: Difference Between Computer Viruses, Worms and Trojans (https://youtu.be/n8mbzU0X2nQ). Have a brief class discussion on computer viruses using the questions below as prompts.

- How is a computer virus like a human virus?
- Do free antivirus programs work?
- How much do commercial antivirus programs cost?

4b. Say: Attacks come from unknown senders, or spoofed or compromised known senders. Show the What is Phishing (https://youtu.be/BnmneAjVrM4) video. Have a brief class discussion on phishing using the questions below as prompts.

- What type of bait might attackers use to trick high school students?
- How should you handle a suspect email?

4c. Say: Some attacks take advantage of keyloggers. Show the Cyber Security Minute: Keyloggers (https://youtu.be/w47eY7AaPdU) video. Have a brief class discussion on keyloggers using the questions below as prompts.

- What do keyloggers do?
- What sort of information might they be used to obtain?
- How can you protect yourself from keyloggers?

4d. Ask: Why is the danger of free downloads is a special risk to young people? Visit the site 7 Quick Sites That Let You Check If a Link Is Safe (https://www.makeuseof.com/tag/4-quick-sites-that-let-you-check-if-links-are-safe/) and identify two tools you could use to identify safe downloads.

4e. Ask: What is an access point to a network? (Ans: a point of connection that can communicate with the network)

Say: According to Wikipedia, A *rogue access point* is a wireless *access point* that has been installed on a secure network without explicit authorization from a local network administrator. Rogue access points can give access to the network with authorization and can be used to intercept or modify network traffic that is traveling through it.

Solicit at least 3 examples of how this could be a problem on a secure network.

4f. Ask: What does it mean if something is malicious? (Ans: it has bad intentions)
Say: According to ZDnet (https://www.zdnet.com/article/most-malspam-contains-a-malicious-url-these-days-not-file-attachments/),"85% of all malspam sent in Q2 2019 (April, May, and June) contained a link to a malicious file download, rather than the actual malicious file attached to the email." Have a brief class discussion on malicious email using the questions below as prompts.

- What makes a link malicious?
- Why do you think attackers may be using malicious links instead of email attachments?
- Do you think there are malicious links on web pages? (yes, for sure!)

4g. Say: In addition to attachments and malicious links - whether in an email, message or on a web page, email from an unknown sender or a known sender whose computer has been compromised may contain active contents such as forms or videos that can be used to compromise your computer security, your privacy or both. Discuss with students ways malicious software can be installed on their computers. Be sure to address the points below.

- Active content in email or messages
- Free downloads
- Malicious content isn't always from unknown sources, it can come from a known website (it could be hacked) or sender (their email could be spoofed, or they might unknowingly be sending something bad or have been hacked)

Optional programming activity.

Visit the PyPi website keylogger 2.7.3 (https://pypi.org/project/keylogger/) and read the Use cases.

- What are three legitimate uses for a key logger?

- What are three illegitimate uses for a key logger?

Optional research activity.

Students will be grouped by the type of attack they read about. They will conduct research to answer the following questions: (some resources will be provided, but students can also search for others. If no computers are provided, it will be up to the teacher to find these additional resources)

1. Where did the name come from?
2. How does the attack work? Describe the process, making sure to note the role of each of the following: (not all will necessarily apply)
    1. The Internet
    2. Software
    3. Hardware
    4. People
3. Find or create a visual that illustrates the attack OR act out the process.

1. Each group (or at least some, depending on time) will present their findings to the class in 2 minutes or less.
    1. Students should use the "CyberSecurity Notes WS" document to take notes for use in studying for the Unit 3 assessment.

Wrap Up (5 min)

Visit the Top 10 Malware January 2019 (https://www.cisecurity.org/blog/top-10-malware-january-2019/) report.

Visit the us-cert.gov report on Ransomware (https://www.us-cert.gov/Ransomware).

What is ransomware?

How can you protect yourself?

- What security concerns does this raise?
- What can be done to protect student data?

Homework:

Real World Connection: Protecting your Computer

Choose one of the following articles to read, based on the operating system you have running on one of your home computers, or the computer you normally use.

- Windows: http://windows.about.com/od/maintainandfix/a/4-Questions-To-Determine-If-Your-Windows-Pc-Is-Secure.htm (http://windows.about.com/od/maintainandfix/a/4-Questions-To-Determine-If-Your-Windows-Pc-Is-Secure.htm)
- Mac: http://www.pcmag.com/article2/0,2817,2408623,00.asp (http://www.pcmag.com/article2/0,2817,2408623,00.asp)
- Linux: http://www.zdnet.com/blog/btl/five-tips-for-improving-linux-security/35798 (http://www.zdnet.com/blog/btl/five-tips-for-improving-linux-security/35798)

Answer the following questions:

1. Does the computer have anti-virus software installed?

If yes, answer the following questions:

1. What is the name of the anti-virus software installed on the computer?
2. Is the anti-virus software on the computer up to date?
3. What features does the anti-virus software provide?

If no, do the following:

1. Find at least two different anti-virus programs for your operating system (one that is free and one that you must purchase).
2. Compare and contrast the anti-virus programs based on the features that they offer.
3. Talk to an adult about installing anti-virus software on your computer if you own one.
4. Does the computer have a firewall enabled?
5. Is the operating system up to date? Which version of the operating system is the computer currently running?
6. What other security measures have been taken to protect the computer?

Optional: Use this extended checklist to enhance the security of your computer.

http://m.wikihow.com/Secure-Your-PC (http://m.wikihow.com/Secure-Your-PC)

Evidence of Learning

Formative Assessment

The teacher will see where the students place the cyber attacks as they read about them on the impact graph and give appropriate feedback.

The teacher will monitor the research on cyber attacks and check for accurate information.

The teacher will clarify misconceptions that become evident during the group presentations.

Summative Assessment

Students will complete a journal entry by responding to questions about their personal and school related data being accessible through the Internet.

(http://www.umbc.edu/)


(http://www.umd.edu/)


(http://www.nsf.gov/)

Authored by: CS Matters in Maryland
Website: csmatters.org (http://csmatters.org)
Email: csmattersinmaryland@gmail.com (mailto:csmattersinmaryland@gmail.com)