(http://csmatters.org) 3 - 13

0b11 - 0b1101

Cybersecurity: Malicious Code, Identity Theft, and Remedies

Unit 3. Information and the Internet

Revision Date: Jan 05, 2020
Duration: 1 50-minute session

Lesson Summary

Summary

This lesson will increase student awareness of the concept that there are dangers associated with Internet usage. It addresses Internet Security with issues inherent to Internet usage: viruses, worms, Trojan horses, and identity theft. The primary objective of this lesson is to equip students with knowledge that will enable them to make responsible choices regarding their Internet use, to prevent security risks. This lesson introduces key vocabulary, discusses Internet security and provides students the opportunity to explore the causes and effects of common security problems.

Learning Objectives

CSP Objectives

- *EU CSN-1 - Computer systems and networks facilitate how data are transferred.*
  - LO CSN-1.A - Explain how computing devices work together in a network.
  - LO CSN-1.B - Explain how the Internet works.
  - LO CSN-1.C - Explain how data are sent through the Internet via packets.
- *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.

Key Concepts

Students will:

- Learn about the different types of malicious code and how to take prevention steps to safeguard systems, data, and identity.
- Give advice on secure cyber practices.

Outcomes

- Students will be able to identify key general attributes of the threats to the security of computers and information via the Internet such as viruses, worms, and Trojan Horses.
- Students will understand critical attributes of the sources, and consequences to individuals and society, of identity theft.
- Students will understand how to protect themselves and their computers from external threats.
- Students will develop a strategy to inform others of the security risks inherent to Internet usage.

Essential Questions

- How is cybersecurity impacting the ever increasing number of Internet users?
- What are some potential beneficial and harmful effects of computing?
- What are different types of malicious code and what is the intention of each attack?
- How can internet users protect themselves from malicious code and prevent such cybercrime attacks?
- How can internet users follow secure practices to reduce the risk of identity theft?

Teacher Resources

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

Teacher's resources:

- NA SAIT Security Video - Malicious Code - Malware Video - https://www.youtube.com/watch?v=7wAHZLFiY-E (https://www.youtube.com/watch?v=7wAHZLFiY-E)
- What to do if you are a victim of Identity Theft: ***Possible Answers*** -
  - The FTC's website is a one-stop resource to both learn about identity theft and walk you through the appropriate actions if your identity is stolen: http://www.ftc.gov/bcp/edu/microsites/idtheft/ (http://www.ftc.gov/bcp/edu/microsites/idtheft/)
  - Some possible steps if your identity is stolen:
    - Report the identity theft to the three major credit bureaus: Experian, TransUnion, and Equifax.
    - File a police report with local law enforcement.
    - Report the theft to the FTC online at www.ftc.gov/idtheft or by phoning 1-877-ID-THEFT (1-877-438-4338).
  - Possible ways for Deterring Identity Theft:
    - Shred financial documents that are not being kept for safeguarding. [This allows a teacher to cover the kind of information that should be held and for how long (in years). It also allows a teacher to cover what documents are best kept in a safe deposit box, a home safe, regular home files, etc.]
    - Do not carry around your Social Security card in your wallet.
    - Do not give out personal information over the phone or over the Internet unless you are absolutely sure who you are dealing with.
    - Choose computer and electronic passwords with care by avoiding birth dates, your Social Security number, your mother's last name, etc.
    - Try not to have your postal mail pile up in your mailbox for several days; if you are going to be away for a few days, have your mail held at the post office until you return.
    - Do not click on suspicious links in e-mail or complete forms with your account number and password. Check the web address.
    - Be suspicious about regular bills that do not arrive on time, denials of credit for no apparent reason, calls or letters about purchases you did not make, charges on your financial statements that you do not recognize.
    - Use a password to access your mobile devices such as your cell phone, tablet (iPad), etc., just as you would have a password to get access to your e-mail accounts.

Students' resources:

- writing journals
- blogs

Lesson Plan

Session 1

Getting Started (10 min)

1. **Journal:** How might malicious code be a threat to Internet security?
   - Possible answers to bring up: identity theft, data theft, stealing money, breaking down other computers, turning other computers into bots to create more problems, etc.
2. **Introduce the topic/Discussion**: Inform the students that today they will be talking about Internet security and participating in discussions about the dangers of viruses and, identity theft and malware along with resources and

prevention tips.
    - Malicious code is a programming code designed with a harmful intent (to hack, cause damage, etc.). With Internet usage comes rights and responsibilities to protect your computer from malicious code. Malicious code causes millions of dollars in damage every year.
    - How can malicious code spread across many computers so quickly?
    - Examine the idea of interconnectedness.
    - Look together at the Digital Attack Map which displays global DDoS activity on any given day. Attacks are displayed as dotted lines, scaled to size, and placed according to the source and destination countries of the attack traffic when known. Have students react to the histogram at the bottom of the map to explore historical data and select a country to view DDoS activity to or from that country at http://www.digitalattackmap.com/understanding-ddos/ (http://www.digitalattackmap.com/understanding-ddos/) .
3. **Introduce key vocabulary - have students crowdsource definitions or look up separately and compare.**
    - Computer virus
    - Spyware
    - Ransomware
    - Bot
    - Hacker
    - Malware
    - Adware

Guided Activities (30 min) - Malicious Code and Identity Theft

1. Play the NA SAIT Security Video: "Malicious Code - Malware" at https://www.youtube.com/watch?v=7wAHZLFiY-E (https://www.youtube.com/watch?v=7wAHZLFiY-E) (3 minutes, from 2013)
    - AnnMarie Keim, IT Specialist, discusses the concepts of Internet Security and introduces the different types of malicious code and how to protect from this type of cybercrime. Keep your system updated, use antivirus and firewall. Backup important files.
2. Review the following words from previous lessons:
    - routers
    - firewalls
3. Discuss: Is malicious code the only way to cause harm on the Internet? (no)
    - https://vimeo.com/63422786 (https://vimeo.com/63422786) (0:30) Google mini-video to show what phishing is, using a brick through a glass window example to get attention.
    - Talk about social hacking, using ordinary everyday life tricks to get information like looking over somebody's shoulder when they type their password, sneaking inside of a locked door before it closes, etc. Point out that it is a combination of people, software and hardware that are both the problem and the solution to Internet security.
4. Students work in groups to explain how unauthorized access to computing resources is obtained and what can be done to protect against them in terms of human behavior, software, and computer hardware. Student groups could create a blog post about their topic to share at the end of class or report using another method. Suggested access methods to address include:
    - Computer viruses
    - Virus hoaxes
    - Worms
    - Trojan horses
    - identity theft
    - Phishing scams
    - Cellphone and texting scams
    - Ransomware

Wrap Up (5 min)

Students will read the following prompt and respond in their journals:

- The only 100% way to prevent malicious code attacks and identity theft is to not go on the Internet. Do you see that as a viable solution for individuals? Corporations? Support your answer.

Consider the following questions and discuss answers as a class:

1. Have you or someone you've known experienced a virus or malware? What was the outcome? What did you take away from this experience?
    - Cover the following:

        - Time and Money spent – (by corporations and by an individual to protect computer assets)
        - What were the consequences?
        - What did the victim go through?
    2. How can you avoid malicious code?
        - *Possible Answers*:
            - Anti-virus software
            - Anti-spyware software
            - Anti-adware software
            - Restore points
            - Keep patches and updates current on your computer
            - Careful use of email
            - Careful use when downloading items

Homework (optional)

On your home computer, see how vulnerable you are to malware and identity theft:

- Carry out some remedies and prevention tips (minimum of three tasks) that you learned today.
- On your blog, list what you did to safeguard your system, your data, and your identity.
- Be prepared to share in the next class

Options for Differentiated Instruction

Extensions/Differentiation:

- Malicious Activity World Map - http://www.team-cymru.org/Monitoring/Malevolence/maps.html (http://www.team-cymru.org/Monitoring/Malevolence/maps.html) - a map that shows malicious activity in world
- Malware Classifications - http://maple.cs.umbc.edu/ce21/instruction/login (http://maple.cs.umbc.edu/ce21/instruction/login) - provides classifications of different types of malware
- Current Threat Activity - http://www.trendmicro.com/us/security-intelligence/current-threat-activity/ (http://www.trendmicro.com/us/security-intelligence/current-threat-activity/) - shows what the current malware threats are and what can be used to prevent them from impacting your computer.
- Threat Encyclopedia - http://about-threats.trendmicro.com/us/glossary/all (http://about-threats.trendmicro.com/us/glossary/all)
- Threat Intelligence Resources - http://about-threats.trendmicro.com/us/infographics (http://about-threats.trendmicro.com/us/infographics)
- Why do cyber attackers do what they do? - http://about-threats.trendmicro.com/us/security-roundup/2014/1Q/cybercrime-hits-the-unexpected/ (http://about-threats.trendmicro.com/us/security-roundup/2014/1Q/cybercrime-hits-the-unexpected/)

If there is additional time, watch one of the TED talks

- James Lyne: Everyday cybercrime -- and what you can do about it (17:26)
- The Internet is on fire | Mikko Hypponen | TEDxBrussels (19:16)

Students can create an "Identity Theft Prevention Action Plan," including a purpose and list of ten guidelines, to share with family and friends after they have researched prevention tips on the FTC website.

- Students may use their choice of the following Web 2.0 websites to create their action plan:
    - http://www.powtoon.com/ (http://www.powtoon.com/) - create a presentation
    - http://www.livebinders.com/welcome/home (http://www.livebinders.com/welcome/home) - create a curation
    - http://goanimate.com/ (http://goanimate.com/) - create an animation
    - https://www.podomatic.com/login (https://www.podomatic.com/login) - create a podcast
    - http://piktochart.com/ (http://piktochart.com/) - create an infographic
- Students will embed their action plan to a blog post in order to share with teacher, classmates, friends, and family. Students should email friends and family (minimum of three people with the teacher cc'd) the link to this blog post on Identity Theft Prevention Action Plan (title of blog post and subject line of email).

Evidence of Learning

Formative Assessment

- Journal writings
  - Introduction question prompts
  - Wrap-up question prompt
- Class discussions - answers, input, and further inquiry by students
- Identity theft prevention plan

Summative Assessment

Unit Assessment and Investigate/Explore Performance Project – at end of unit.

 (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)