The Who, What, Where, and Why of Cyberattacks
Lesson 3
Middle School Cybersecurity Unit: Can you Hack the Cyber Attack?

Lesson Overview	Career Highlight
How do computers communicate with each other? Computers "talk" with each other through the internet, which is a series of networks that allow this communication. People have been known to use these networks to steal information from others. There are many different areas where these nefarious people can gain access to the information that they steal. Once we understand the access point for these areas of weakness, we can develop safeguards to make it harder for the thieves to steal the information. In this lesson, students will explore the differences between hosts, clients, servers and networks. Students will play a game of Kahoot to demonstrate their understanding of these three kinds of devices. Students will gain a basic understanding of the networks used throughout the internet. Students will also explore the kind of data collected by some popular apps. Students will explore the different types of cyberattacks that our society has faced; phishing, malware, denial of service attacks, and many others. Students will use a simulation to defend and protect a social media company's network. Finally, students will create a plan for helping someone recover from an identity theft. As students go through this lesson, they will be able to distinguish between different types of cyberattacks and ways to fix or prevent them. Students may then apply this knowledge to help them develop their app idea for their final project in this unit.	Students will learn about how malicious hackers use different kinds of attacks to infiltrate networks and steal information. While students learn about the attacks, they will also learn about the IT professionals who defend the systems and make sure that they are safe. *Teacher Note: Use of the common "black hat" term to denote a malicious hacker can promote harmful associations and propagate unconscious bias. There is a debate in the information security community about changing this language to promote inclusion, regardless of its history. Terms such as "ethical (vs. unethical) hacker" or "legal (vs illegal) hacker" can be used as replacements.*

STEM Course Connections	Timing
Computer Science General Science	Five class sessions at 45 minutes each

Engineering Activity	
Science and Engineering Practice #	In pairs, students will work together to undergo a cybersecurity simulation where they need to analyze and interpret data to design solutions for a company being targeted by various cyberattacks. Students will also work in teams to assess an identity theft scenario, conduct research, and design an action plan for the victim.

	4. Analyzing and interpreting data 6. Constructing explanations (for science) and designing solutions (for engineering) 8. Obtaining, evaluating, and communicating information

Essential Questions

1. Why are networks important in the communication of computers?
2. What kinds of devices can act as clients and how might they be vulnerable?
3. Is privacy something a user can expect with any app or program?
4. What are the different types of cyberattacks?
5. How can individuals decrease the likelihood of being victims of cyberattacks?

Lesson Objectives

Learning Goals:

- Students will distinguish between and provide examples of hosts, clients, and servers.
- Students will explain how data collected online is available to the global network.
- Students will explore and debate different perspectives of data collection, etc.
- Students will describe the similarities and differences between various cyberattacks.
- Students will distinguish between phishing sites, emails, and messages from legitimate ones.
- Students will create an action plan for someone who is a victim of an internet crime.

Materials

All materials in Student Handouts, unless otherwise noted.

- Computer Network Kahoot!
- Cybersecurity App Project Journal *(This journal will be used for every lesson)*
- NOVA Cybersecurity Lab Note Catcher (answer key)
- Action Plan Graphic Organizer
- Day One Station Two: Matching Terms and Descriptions *(Print a few copies of this document and cut into pieces. Students will physically match each term to its description. Alternatively, this document can be turned into a jamboard.)*

Lesson

Teacher Note: If you did not do Lesson One of this unit, it may be a good idea to give the students the Class Poll from the Lesson One Student Handouts before beginning this lesson.

- **Day One - What is a Computer Network?**
  - **Whole Group (10 minutes)**
    i. What do you know about networks?
      - Have students play a 10 question Computer Network Kahoot! testing their knowledge of what they already know about computer networking.

      - While students are signing in to Kahoot!, point out the unique access code that allows the students to connect to the game. Emphasize the point that this is creating a network between the student device and the "host" of Kahoot!

- **Individual (10 minutes)**
    - Have students create a map of devices using the Map of Devices Template from the Student Handouts that they will use throughout the day showing the following:
        - Labeling whether the device connects to the internet or not
        - Where they use the device during the day
        - Example:
            - Location: School
            - List of devices:
                - Cell phone %
                - School chromebook *
- **Small Group (10 minutes)**
    i. Stations
        - Students may work in small groups of three to four students. Depending on the number of groups you have, you may want to have 10 computers open for Station One and 10 sets ready for Station Two.

        - Instruct students go to two different five-minute stations learning about hosts, clients, servers, and networks in order to answer the following prompts in their Cybersecurity App Project Journal:
            - Prompt 1: What are hosts, clients, servers, and networks and examples of each?
            - Prompt 2: How do the different parts of a computer network share data?
            - Prompt 3: How do you think a network can become vulnerable to cyberattacks?

        - Station One: Video 3: How Do Computers Communicate?

        - Station Two: Matching Terms and Descriptions *(Print a few copies of this document and cut into pieces. Students will physically match each term to its description. Alternatively, this document can be turned into a jamboard.)*

- **Individual (two minutes)**
    i. Students go back to their Map of Devices Template and label their host devices as a "client" or "server."

- **Small Group (three minutes)**
    i. Have students share their Map of Devices Template with their elbow partner to check if their partner labeled their map correctly.

    ii. Instruct students to come up with two ways networks can become vulnerable to cyberattacks using information they have learned about hosts and clients with their elbow partner.

- **Whole Group (10 minutes)**
    i. Computer Network Kahoot! - What did you learn?
        - Have students play 10-question Computer Network Kahoot! again testing their knowledge of what they learned about networks.

        - Ask students: "Using the new terms we learned today about networks, how were we able to play this Kahoot! on our devices?"
            - Possible student answer: "Our phone is a client and data was transmitted

through communication media like WiFi through our school LAN. The unique access code was sent to the server or host that contains the Kahoot! website data. The server then sends the code to a web browser which translates the data into a Kahoot! game that we see on our phones (the client).

- **Day Two - The Who and What of Cyberattacks**
  - **Individual/Whole Group (15 minutes)**
    i. Engage - What do students already know about the word, "hacking?"
      1. *Teacher Notes: For this activity, students could discuss answers with an elbow partner or at table groups. Students can share out responses using an online word cloud website like https://www.vevox.com, https://answergarden.ch/, or https://www.sli.do/. Students can also write on whiteboards to share out answers.*

      2. Ask students the following questions:
         a. "Have you ever had a stain on your clothes that you needed to get out? What different hacks have you tried to remove the stain?"
         b. "What other cleaning hacks or home organization hacks have you seen before?"

      3. Have students come up with a class definition for the word, "hacking" that relates to the questions about cleaning and home organization. Tell them to write this definition in their Cybersecurity App Project Journal.

      4. Ask students: "Where have you heard of the word 'hack' when it comes to computers?"

      5. As students watch the video, instruct them to either add or improve their definition of "hacking."
         a. Hacker Video: *The Secret Lives of Hackers* (PBS LearningMedia, 2021)

Teacher Note: Use of the common "black hat" term to denote a malicious hacker can promote harmful associations and propagate unconscious bias. There is a debate in the information security community about changing this language to promote inclusion, regardless of its history. Terms such as "ethical (vs. unethical) hacker" or "legal (vs illegal) hacker" can be used as replacements.

  - **Individual/Pairs (30 minutes)**
    i. **NOVA CYBERSECURITY LAB DAY 1:**
      1. Instruct students to log into *Cybersecurity | NOVA Labs | PBS* with an account so they do not lose their progress.

      2. Say this excerpt from NOVA Labs to get the students excited about the activity: "Take cybersecurity into your own hands. In this Lab, you'll defend a company that is the target of increasingly sophisticated cyberattacks. Your task is to strengthen your cyberdefenses and thwart the attackers by completing a series of cybersecurity challenges. You'll crack passwords, craft code, and defeat malicious hackers."

      3. Have students work independently or in pairs to complete the challenges. They must fill out the NOVA Cybersecurity Lab Note Catcher from Student Handouts as they complete the game.

- **Day Three - The Who and What of Cyberattacks**
  - **Individual/Pairs (45 minutes)**
    i. **NOVA CYBERSECURITY LAB DAY 2:**
      1. Instruct students to log into *Cybersecurity | NOVA Labs | PBS* with an account so they do not lose their progress.

      2. Tell students to complete the game and their NOVA Cybersecurity Lab Note Catcher from Student Handouts.

    ii. Optional extensions for students who finish early:
      1. Have students add to their NOVA Cybersecurity Lab Note Catcher from Student Handouts by researching this website, *What is a Cyberattack?* (Cisco, 2022), for more information on other types of cyberattacks.

    iii. When students are done with their NOVA Cybersecurity Lab Note Catcher from Student Handouts, instruct them to answer the prompts Cybersecurity App Project Journal for Lesson Three, Day Three:
      1. "Think about one app or website you use every day. What types of cyberattacks do you think this company faces regularly?"
      2. "What types of cyberdefense methods do you think this company has to prevent hacking?"
      3. "Who does the cyberattacking? What motives do people have for creating cyberattacks on individuals and companies?"
      4. "Write your own definition of hacking. Is there such a thing as good computer hacking and bad computer hacking? Explain."
      5. "What type of cyberattacks do you want to teach about in your app?"

- **Day Four - The Why of Cyber Attacks: Identify Theft Crime**
  - **Whole Group (10 minutes)**
    i. Instruct students to go to *';--have i been pwned?*

    ii. Tell them to check to see how many times their information may have been compromised by entering their email address, or a parent or guardian's email address.

    iii. Discussion:
      1. "What do you wonder or notice about this activity?"

      2. *Teacher Notes: You may want to drive the discussion to discuss what types of information were being stolen and by whom. You will also want to ask the students why they think people want to steal others' personal information. Students should notice how easily available people's personal information can be hacked and shared with others.*

  - **Whole Group/Small Group (15 minutes)**
    i. Phishing Cyberattack Review - Are you able to determine if the example is phishy? This activity will help you determine if students understand the differences between fraudulent activity versus legitimate sources.
      1. Open *Can you spot when you're being phished?* for the class.

      2. Tell students to give a thumbs up if the example is "Legitimate" and a thumbs

down if it's an example of "Phishing."

ii. Show students Video 4 - Let's go Phishing!
    1. As students watch the video, have them write answers to the following questions on the Action Plan Graphic Organizer from Student Handouts:
        a. "What types of cyberattack happened to the grandmother?"
        b. "What are things someone can do with a stolen social security number?"

iii. Class Discussion
    1. Ask students to share answers about the video questions. Write down some of their responses on the board or visible area for students to see during this lesson.

- **Small Group (20 minutes)**
    i. In groups of two to three students, instruct students to create an action plan for the grandmother on what to do next after realizing their identity was stolen.

    ii. Instruct students to fill out the Action Plan Graphic Organizer from Student Handouts and have them make a presentation that they will present to the class.
        1. *Teacher Notes: Students can create a slide deck or create a poster with action steps listed.*

    iii. Homework: Instruct students to ask family members, teachers, or other adults to review their action plan and provide feedback.

- **Day 5 - The Why of Cyber Attacks: Identify Theft Crime**
    - **Small Group (15 minutes)**
        i. Have students meet with their team to review or edit their slide deck or poster and practice presenting their slide deck or poster. Remind students to incorporate feedback from their family or other adults who reviewed their action plan.

        Teacher note: This would be a great time to invite a STEM professional or another adult into the classroom, to watch student presentations and provide feedback.

    - **Whole Group (20 minutes)**
        i. Instruct the groups to partner up with two other groups. Have groups take turns presenting their action plans to the other two groups.

        ii. During presentations, students must jot down at least one similarity and difference in their action plan from each presentation in their Action Plan Graphic Organizer from Student Handouts.

    - **Whole Group/Individual (10 minutes)**
        i. Exit Ticket
            1. Instruct students to retake the Class Poll from the Lesson One Student Handouts.
                a. Ask them: "If your rating changed, explain why you changed your rating. If your rating is the same, what have you learned so far that has confirmed your rating?"
        ii. Instruct students to answer the following prompts in their Cybersecurity App Project Journal:
            1. "Which age group are you considering in educating for your app?"
            2. "Who does the cyberattacking for this age group?"

3. "What motives do people have for creating cyberattacks on individuals in this age group?"

Extension

- **Debate about Network Security**
    i. Students will read about three different case studies where clients and servers were not kept secure. (Example: baby monitors being hacked)
        1. *Mother's horror at hearing creepy man "shushing" two-year-old son through baby monitor.* (Phillips, 2022)
        2. *'9–1-1: Lone Star' Recap: Season 3, Episode 5 "Child Care."* (L., 2022)
        3. *I Was Stalked with an Apple AirTag—Here's What I Wish I'd Known.* (Kim, 2022)

    ii. Students will participate in a class debate about whether the data collected by apps should be allowed.
        1. Students will be split into four teams for the debate; two teams for the collection of data is necessary for the site to function and two teams that are against the site collecting extraneous information.

        2. Provide the teams time to prepare for the debate by doing extra research and searching for more case studies.

        3. Use "Want to Facilitate a Debate in *Your* Class?" to conduct the debate.

- **Networking Analogy**
    - Instruct students to create an analogy to help explain how computer networking is like a school, city, or maybe an amusement park. They need to include analogies for hosts, clients, nodes, and communications media.

- **How Can Your Information be Used through Cookies?**
    - Have students read the following articles about internet cookies and write a one-page report about what cookies are and how information is used through cookies:
        i. *Internet Cookies* (Federal Trade Commission, 2022)
        ii. *Internet Advertising Is About to Change. Here's What Consumers Need to Know.* (Tanner, 2021)
        iii. *Why are internet cookies called cookies?* (inLIFE, 2015)

CA NGSS Standards

MS-ETS1-1 Engineering Design

MS-ETS1-2 Engineering Design

Resources

';--have i been pwned? (n.d.). Haveibeenpwned. https://haveibeenpwned.com/

AnswerGarden. (n.d.). AnswerGarden. https://answergarden.ch/

Can you spot when you're being phished? (n.d.). Jigsaw | Google. https://phishingquiz.withgoogle.com/

Cybersecurity | NOVA Labs | PBS. (n.d.). PBS. https://www.pbs.org/wgbh/nova/labs/lab/cyber/

Internet Cookies. (2022, February 10). Federal Trade Commission. https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies

Kahoot! (n.d.). Kahoot! https://create.kahoot.it/share/computer-networking/d0148cfc-3357-4e35-9c1b-1fe3b81a2b81

Kim, M. (2022, February 11). *I Was Stalked with an Apple AirTag—Here's What I Wish I'd Known*. Reader's Digest. https://www.rd.com/article/apple-airtag-stalking/

L. (2022, February 8). *'9–1-1: Lone Star' Recap: Season 3, Episode 5 "Child Care."* Nerds & Beyond. https://www.nerdsandbeyond.com/2022/02/07/9-1-1-lone-star-recap-season-3-episode-5-child-care/

Phillips, J. (2022, February 16). *Mother's horror at hearing creepy man "shushing" two-year-old son through baby monitor*. Mail Online. https://www.dailymail.co.uk/news/article-10518765/Mothers-horror-hearing-creepy-man-shushing-two-year-old-son-baby-monitor.html

slido. (n.d.). *Slido - Audience Interaction Made Easy.* https://www.sli.do/

Tanner, B. A. (2021, November 9). *Internet Advertising Is About to Change. Here's What Consumers Need to Know.* Consumer Reports. https://www.consumerreports.org/advertising-marketing/internet-advertising-is-about-to-change-third-party-cookies-a6221885875/

The Secret Lives of Hackers. (2021, February 24). PBS LearningMedia. https://ca.pbslearningmedia.org/resource/nvcy-sci-slhackers/the-secret-lives-of-hackers/

Vevox. (n.d.). *Vevox | The No.1 rated Polling and Q&A platform for hybrid*. https://www.vevox.com

What Is a Cyberattack? (2022, April 6). Cisco. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#%7Etypes-of-cyber-attacks

Why are internet cookies called cookies? (2015, July 22). inLIFE. https://www.inlife.co.uk/why-are-cookies-called-cookies/

NOVA Cybersecurity Lab Note Catcher

Directions:

1) To access the Cybersecurity Lab, go to: *Cybersecurity | NOVA Labs | PBS*

2) Sign in with a Google account or create a PBS account to make sure your work saves.

3) As you play the game, write down the definition and other notes about each term in Table 1. If there are questions, be sure to answer them as well. Identify each term as a cyberattack or a cyberdefense.

4) In Table 2, be sure to click on the Cyber Story articles in the game and jot down three things you found interesting about the articles and write one question you still wonder about for each article.

Table 1. Cybersecurity Lab Key Terms

Key Term	**Notes** Definition or Description of each key term along with questions. **If the term is a type of cyberattack**, take a screenshot of where you found this term in the game and describe how you tried to defend the network from the cyberattack.	**Drawing of key term** Draw/insert a picture here to help you remember what the word means.
Virus	(Cyberattack) A computer program that can copy itself and cause harm in various ways, such as stealing private information or destroying data.	
Ransomware	(Cyberattack) A type of malware that holds victims' computer files hostage by locking access to them or encrypting them. It then demands a ransom if the victim wants their files back.	
Phishing	(Cyberattack) Attempting to trick people into revealing sensitive information, such as passwords and credit card numbers, often by using emails or fake websites that look like they're from trusted organizations.	
	What are red flags in a phishing email? Sending emails to an entire address book, sloppy grammar, creating a sense of urgency, trying to get you to send money in a way that can't be traced, misspelling their own names. What are red flags in a phishing website? No padlock or https, no proper URL, using older logos, using wrong font, sloppy spelling. What are red flags in a phishing call? Winning something you don't remember entering, creating a false sense of urgency, not addressing names, bait and switch, asking for a credit card number.	
Malware	(Cyberattack) Software that harms computers, networks, or people. Includes viruses, worms, ransomware, and other computer programs.	

	What are red flags for malware? Seeing spam from emails	
Vulnerabilities	(Cyberattack) A flaw or weakness in a computer program that hackers or malware can exploit to gain access to a system or damage it.	
Software Patch	(Cyberdefense) A piece of software designed to update a computer program in order to fix a software vulnerability or improve the program.	
Antivirus Software	(Cyberdefense) Computer programs that can block, detect, and remove viruses from malware	
DDos Attack	(Cyberattack) A distributed denial of service attack attempts to make an online service, like a website, unavailable by overwhelming it with a flood of traffic by a team of computers.	
	What does a company need most in order to be protected from this type of attack? Explain why. Cyberdefenses like bandwidth, servers, and firewalls.	
Firewalls	Are firewalls more useful for DDoS attack or for malware? Explain why. Firewalls are more useful for malware because they are specifically made to block out malware attacks.	

Table 2. Cybersecurity Lab Articles

Direction: Read each Cyber Story and jot down three things you found interesting about the articles and write one question you still wonder about for each article.

Cryptolocker	• Scrambles the computer's files using encryption • Crpytolocker infected more than 500,000 computers worldwide • Holds files hostage and demands ransom to get them back • How does scrambling computer files cause someone to lose access to them?
Data Breach	• 822 million data records were stolen in 2013 • eBay, Adobe, and Target had their data breached at one point • Can happen from one simple mistake, like leaving your phone somewhere • Can data be breached only if it falls into the wrong hands?
DDoS attack	• There are 2,000 DDoS attacks everyday

	• You can buy a week-long DDoS attack for only $150 • Attackers can instruct a network of computers to target a website • What types of programs have been created to stop DDos attacks? How successful are they? Is there any way to predict an attack?

Finished Early?

1) More on Types of Cyberattacks
    a) Go to this website: *What is a Cyberattack?* (Cisco, 2022)

    b) Write down notes below about other cyberattacks not mentioned in the lab.

Station Two: Matching Terms and Descriptions

Teacher Instructions:

1. Print a few copies of this document and cut out the pieces. Store each set in a small plastic bag or in an envelope.

2. Have students try to match each term to their description.

Computer Network	A system where two or more computers are interconnected in order to share or transmit data.
LAN	LOCAL AREA NETWORK - A type of network for computers or other devices to be connected in one building. (Example: The network in your school building)
MAN	METROPOLITAN AREA NETWORK - A type of network for computers or other devices to be connected between different buildings in a city. (Example: hospitals needing to share research with local universities)
WAN	WIDE AREA NETWORK - A type of network for computers or other devices to be connected between different buildings in different cities. (Example: The internet)
Nodes	Any type of device used in computer networking such as a PC, phone, printer, modem, router, server, etc.
Communications Media	The way the nodes are connected through copper wires, WiFi, radio waves, or fiber optics.
Server	A special computer that many users can access and that gives data to clients.
Client	A computer or device that receives data from a server.