Cybercrime Investigator

#16 Information Security

Description:
In this activity, after exploring topics in cybercrime, students research stories of cyberattacks to better understand the nature and costs of the crime, vulnerabilities of targets, and potential defenses or solutions. In so doing, students will:

- Describe cybersecurity (e.g., risks, threats, vulnerabilities).
- Use technology ethically (e.g., appropriately using social networks, managing personal information).
- Explore common workplace policies (e.g., acceptable use policy [AUP]).
- Describe the value and need for protecting confidentiality (e.g., protecting login information and, customer information)
- Identify workplace-security procedures and protocols.

This activity was created to be used primarily with:
16. Information Security

Secondary skills include:
2. Critical Thinking and Problem Solving
3. Initiative and Self-Direction
4. Integrity
5. Work Ethic
11. Big-Picture Thinking
12. Career and Life Management
14. Efficiency and Productivity
15. Information Literacy
17. Information Technology
18. Job-Specific Tools and Technologies
20. Professionalism
21. Reading and Writing
22. Workplace Safety

1. Teacher will define Information Security as:
   basic Internet and email safety and follows workplace protocols to maintain the security of information, computers, networks, and facilities

   identifying various information types/formats (e.g., paper, electronic)
Note: Remind students that while this activity focuses on cybercrime, this skill area is fundamentally about protecting and respecting confidentiality. Whether working in a hospital to protect patient records or operating independently online, students should always first pay attention to ensuring the private information sharing is scrutinized and avoided whenever possible. Understanding policies and protocols is crucial.

describing cybersecurity (e.g., risks, threats, vulnerabilities)

using technology ethically (e.g., appropriately using social networks, managing personal information)

abiding by workplace policies (e.g., acceptable use policy [AUP])

protecting confidentiality (e.g., protecting login information and, customer information)

following workplace-security procedures.

Note. While this activity addresses one aspect of information security, cybersecurity, additional activities should focus on confidentiality and its importance in the workplace, including laws around it.

2. Teacher will present various strategies students could use to improve information security skills at school and home. Ask them how they protect their privacy online and how and why companies help them do this.

Note: Ask: What careers are related to cybercrime and cyber forensics? Try to expand this list beyond purely IT and into administration, government, military, law enforcement, journalism, and researchers and investigators of any kind.

3. Teacher might introduce this topic/activity by asking the students what is risked if employees expose information management systems to cyberattacks. Ask them to provide a recent story of an important cyberattack and how it was resolved. See additional resources for related info and idea starters. Students research stories of cyberattacks to better understand the nature and costs of the crime, vulnerabilities of targets, and potential defenses or solutions.

Note: Teacher might ask how information security relates to the Efficiency and Productivity skill and to Integrity.

Additional resources:
Differentiation:

Create learning stations:

- Divide the class and have some students research good cybercrime stories for the others.
- Divide the class and have some students investigate ransomware stories.
- Divide the class and have some students look into trends and how companies and governments are responding to cyberattacks.

Have students research podcasts on cybersecurity.

Vocabulary:

Students use the following link for exercises on Quizlet:
https://quizlet.com/_9z4865?x=1qqt&i=wcwth

credential reuse, a server-side attack that allows hackers to be able to target vulnerabilities on any site you use to login, then they apply that same login information to other major consumer sites to see if you reused your login and password

cyberattacks, an attempt by hackers to damage or destroy a computer network or system
cybercrime, criminal activities carried out by means of computers or the Internet
cybersecurity, the protection of information systems against unauthorized access (e.g., hacking, identity theft)
end-user attacks, unethical and often unnoticed attacks by others in the public sphere when operating online (e.g., malware, phishing, Trojan horse, virus, worm, spam, rootkit)
ethical Internet use, using online services and social networking ethically, by being a good online citizen, by adhering to privacy and safety guidelines, and by facilitating thoughtful and considerate communication with others
Internet security risks, the level one exposes one's self or professional network to unethical intentions (e.g., end-user attacks, server-side attacks)
Internet use policy, a formal document with which many organizations require employees to comply, addressing the separation of personal and workplace use of the Internet, email etiquette, and security measures and safeguards that employees must obey.
malware, includes viruses and ransomware running on your device which can take over the operation of your device or quietly watch your operations and keystrokes and steal confidential information from your network; usually requires the user to initiate by unwittingly installing the malicious software
personal Internet use, using the Internet for anything other than work tasks
phishing, pretending to be someone you trust or a system you work with, to get you to visit a fictitious site and enter your login or other private info
professional Internet use, using the Internet, ethically, for work-related tasks
ransomware, a type of malicious software designed to block access to a computer system until a sum of money is paid
rootkit, malware that accesses or controls a device without being detected
server-side attacks, attacks focused on the workplace Network workers access.
social network, a website that allows people of similar interests to interact and exchange information that is typically personal
spam, the unethical distribution of mass digital messages. This is the main way that malware is opened and spread
SQL injection attack, cyberattack that targets the server side to get customer information from the database, such as credit card numbers
Trojan horse, malware disguised as a trusted source that convinces the user to open a link or an attachment and install itself.
virus, malware that spreads by users from an infected device to the rest of the devices on a network/system
vulnerability, a flaw or weakness that allows a threat agent to bypass security
worm, a type of virus that does not rely on users to copy and spread but can replicate itself, once inside a network/system

Pre-Quiz:
What are some careers that are related to cybersecurity?
Which industries need cybersecurity the most?
What happens when there is a breach in consumer confidentiality? How do companies respond?
What is the motivation for criminals who try to gain access to your private information?
What is the motivation for criminals who commit ransomware crimes?

Reflection Quiz:
How are governments and industries responding to ransomware crime?

Why is ransomware crime identified as a national security threat?

What do you think the future holds for advances in cyber forensics and cybercrime?

What can individuals do to prevent security or confidentiality breaches at work or at home?

What has been your personal experience (or with anyone you personally know) with cyberattacks or cybercrime? How did it make you feel?