SIEMENS STEM DAY | Science Technology Engineering Math

GRADES 9–12

SIEMENS STEM DAY ACTIVITY

AVOIDING CYBERCRIME

OBJECTIVES

Students will be able to:

- **understand** the types of cybercrime.
- **explain** how to defend against cybercrime using cybersecurity techniques to ensure privacy and security.

THIS LESSON FOCUSES ON

Engineering Design Cycle

- Defining the Problem
- Designing Solutions

21st Century Skills

- Collaboration
- Critical Thinking

OVERVIEW

In cyberspace, cybercrime is a prevalent illegal activity done via computers. Students will learn the foundations of cybersecurity and work together to analyze a variety of cybercrime scenarios. Additionally, they will propose cybersecurity measures that could prevent each type of cybercrime from occurring.

STEM incorporates Science, Technology, Engineering, and Mathematics to focus on real-world issues and problems guided by the engineering design process. This type of instruction supports students in developing critical thinking, collaboration, reasoning, and creative skills to be competitive in the 21st-century workforce.

Each Siemens STEM Day classroom activity highlights one or more components of the engineering design cycle and an essential 21st-century skill.

MATERIALS

- *Learning about Types of Cybercrimes* matching activity, one per two students
- *Understanding Ways to Avoid Cybercrimes,* one per student
- *Cybercrime Scenarios,* one per student
- Computers with internet access for research

HAVE YOU EVER WONDERED . . .

Why did I receive an email awarding me twenty-five thousand dollars? What is this all about?

MAKE CONNECTIONS!

How does this connect to students?

Students spend a great deal of their **time in cyberspace**. It is important that they understand the different types of cybercrime that exist, so that they can avoid falling prey to such schemes and crimes.

Increased connectivity brings with it an increased threat of risk and fraud. Students must learn what they can do to help **combat cybercrime**. There are even a few simple ways to protect a home computer such as: having a firewall, using antivirus software, being selective with downloads and even getting in the habit of turning off the computer.

Cyber citizenship is another valuable aspect of combating cybercrime. Teaching students about the dangers they face on the internet and smart surfing habits is critical.

How does this connect to careers?

There are literally hundreds of jobs that relate to cyber-security. A **cybersecurity analyst** is also commonly known as an information security analyst. These professionals are responsible for monitoring and maintaining organizations' networks free of security violations.

Law enforcement and FBI agents frequently investigate cyberattacks such as theft and fraud. According to the FBI, "Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated."[1]

How does this connect to our world?

"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."[2] Risks are often associated with both physical and cyber threats and hazards. It is essential to learn forms of protection from **cybersecurity tools**.

The impact that cybercrime has had on not only our country but worldwide is staggering. The amount of personal and professional business conducted on the internet is unimaginable. **Cyber Action Teams** travel around the world at a moment's notice to help solve a multitude of cybercrimes.

[1] FBI: Cyber Crime, https://www.fbi.gov/investigate/cyber
[2] Homeland Security: Cybersecurity, https://www.dhs.gov/topic/cybersecurity

BLUEPRINT FOR DISCOVERY

1. To engage students in what they will be learning, ask them if they have ever heard about people receiving emails that say that they will be awarded twenty-five thousand dollars. What is this all about? Ask students if they have heard of scams such as this. Facilitate a discussion to hear about the students' experiences.

2. Explain to students that in order to help them learn about a variety of cybercrimes, they are going to participate in a partner matching activity. Ask students to select a partner to work with for this activity. Then pass out the **Learning about Types of Cybercrimes** handout and review the directions with the students. When the students have completed the matching activity, check each partner set's work for accuracy.

   Note: It is important to have the headings, terms, and descriptions cut out and shuffled, since the **Learning about Types of Cybercrimes** handout is the actual answer key displaying the cybercrime terms with each corresponding description.

3. Next, tell the students that although there are so many types of cybercrimes, the fortunate thing is there are many actions that people and companies can take to protect themselves from falling victim to a cybercrime. Pass out the **Understanding Ways to Avoid Cybercrimes**, one to each student. Explain that they are going to use their devices to conduct some research about each of these strategies that can be used to enhance cybersecurity. Allow the students time to complete this research activity, then facilitate a group conversation about each strategy.

4. Ask the student to form groups of 3-4 students. Tell them that they will now be given cybercrime scenarios to identify and analyze as a group. Explain that they will be applying the previous information they learned about types of cybercrimes and ways to avoid it. Pass out one copy of the **Cybercrime Scenarios** to each student. Instruct them to collaborate as a small group to complete this activity.

5. Conclude the lesson by engaging the class in a group discussion. First, discuss the five scenarios on the handout. Then ask for volunteers to share the scenario that their small group created. After they read their scenario, encourage the students to call on their classmates to identify the type of cybercrime and the avoidance strategies or actions that can be taken.

TAKE ACTION!

Students can take action and be more informed digital citizens. By participating in a Cyber Citizenship program, students will better understand the importance of the digital footprint they leave behind. Google for Education offers a variety of teacher and student digital citizenship and safety courses that address internet safety, privacy, savvy searching, and ways to stay safe from phishing and scams. Go check them out!

[3] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/

NATIONAL STANDARDS

Standards for Technology Literacy	Standard 6: Students will develop an understanding of Technology and Society. This includes learning about the role of society in the development and use of technology. Standard 12: Students will develop Abilities for a Technological World. This includes becoming able to use and maintain technological products and systems.
Next Generation Science Standards	HS-ETS1-2: Engineering Design- Design a solution to a complex real-world problem by breaking it down into smaller, more manageable problems that can be solved through engineering. HS-ETS1-3: Engineering Design- Evaluate a solution to a complex real-world problem based on prioritized criteria trade-offs that account for a range of constraints, including cost, safety, reliability, and aesthetics as well as possible social, cultural, and environmental impacts.

LEARNING ABOUT TYPES OF CYBERCRIMES

Types of Cybercrime	Descriptions
Cyberbullying	Intentional and repeated harm caused by the use of electronic devices such as computers or phones
Identity Theft	Illegally obtaining someone's personal information such as their date of birth, Social Security number, financial account numbers, passwords
Credit Card Theft	Theft and use of a person's credit information and personal credentials
Network Intrusions	Unauthorized activity on a digital network that jeopardizes the security of data and/or the network
Software Piracy	The act of stealing software by copying, modifying, or selling software that is legally projected
Phishing	The theft of confidential information or money, fake accounts, spam and malware, site compromise, and information disclosure
Pharming	A type of phishing in which hackers infiltrate a computer system with malicious code that redirects the user to illegitimate websites that obtain personal information

UNDERSTANDING WAYS TO AVOID CYBERCRIMES

Use digital resources to research each of the cybercrime avoidance strategies listed below.

Avoidance Strategy	Description
Anti-virus software	
Two-factor authorization	
Email encryption software	
Intrusion detection software	
Password management software	
Firewalls	
Incident report form	
Ransomware software	
Contain, Eradicate, Recov	
Cyber Security Incident Response Team (CSIRT)	
Information Security Plan	

CYBERCRIME SCENARIOS

Analyze each scenario below and first identify the type of cybercrime that the scenario represents. Then use the avoidance strategies you previously learned to provide 1–2 tips for how to avoid each cybercrime scenario. *Please note: A few scenarios will ask for suggested actions, rather than avoidance strategies.*

Cybercrime Scenario	**Type of Cybercrime**
Bernard logs in to his online bank account and realizes that there are withdrawal transactions that he did not make. Although there are a variety of ways that this could have occurred, he finds out that he had previously logged in on a phishing website that captured his personal login information.	**Avoidance Strategies**

Cybercrime Scenario	**Type of Cybercrime**
A mailing and shipping company received a ransomware attack with payment demanded. This attack encrypted their system's information and locked customers out of their accounts. The cyberattack was quickly identified and a response team worked to recover its systems.	**Avoidance Strategies**

Cybercrime Scenario	**Type of Cybercrime**
A large banking corporation discovers that emails they have sent containing personal customer information are being intercepted. These emails include financially sensitive communications about establishing a home mortgage.	**Avoidance Strategies**

CYBERCRIME SCENARIOS CONTINUED

Cybercrime Scenario	Type of Cybercrime
Cynthia is a high school freshman who has been receiving very aggressive cyberbullying messages repeatedly on her social media sites. She tried ignoring it, but the harassment has increased. Cynthia knows that bullying is not right but she's not sure what steps to take to help herself.	**Suggested Actions** *Rather than focusing on avoidance, address what actions Cynthia can take.*

Cybercrime Scenario	Type of Cybercrime
Online auction sites allow people to buy and sell merchandise. While there are many legitimate products sold, there is also a great deal of software piracy sales. Buyers believe that they are purchasing legal software, and they are often unaware of the illegal activity that is taking place.	**Avoidance Strategies**

Create Your Own Cybercrime Scenario	Type of Cybercrime
	Avoidance Strategies

Works Cited

- https://cyberbullying.org/social-media-cyberbullying-and-online-safety-glossary
- https://www.cisa.gov/combating-cyber-crime
- https://www.dhs.gov/science-and-technology/cybersecurity
- https://www.stopbullying.gov/resources/what-you-can-do