Course: Georgia Foundations of Secure Information Systems I Module: Cybersecurity and Digital Citizenship

Lesson 4.1: What is Cybersecurity?

https://codehs.com/course/8000/lesson/4.1

Description	In this lesson, students will learn what is meant by *cybersecurity* and explore a few news worthy cyber attacks. They will also discuss the *Internet of Things* and the increase in connected devices. *Cybersecurity* is the protection of computer systems, networks, and data from digital attacks. Increased connectivity via the Internet of Things and reliance on computer devices to send and store data makes users more vulnerable to cyber attacks.
Objective	Students will be able to: • Define cybersecurity • Describe how the Internet of Things makes people more vulnerable to cyber attacks • Reflect on recent cyber attacks and identify the financial and societal impact of the attack
Activities	4.1.1 Video: What is Cybersecurity? 4.1.2 Quiz: What is Cybersecurity? 4.1.3 Connection: WannaCry Ransomware Attack 4.1.4 Free Response: WannaCry Reflection 4.1.5 Example: Ransomware Simulator 4.1.6 Connection: Internet of Things 4.1.7 Connection: Cybersecurity and Connected Cars 4.1.8 Free Response: Internet of Things Reflection 4.1.9 Connection: Threat Map 4.1.10 Free Response: Why Learn about Cybersecurity? 4.1.11 Example: QR Code Generator
Prior Knowledge	No prior knowledge needed.
Planning Notes	• Review the slides and activities for the lesson before the start of class. • There is a handout that accompanies this lesson. It can be used as an in-class activity or a homework assignment. Determine how and if this handout will be used and make the appropriate number of printouts prior to the class period. • The *QR Code Generator* simulation involves students using their own devices. If this is not possible, have them create the QR code with their computer and you can scan it with your mobile device as a demonstration. • Students have probably heard about recent hacks in the news. If you have time, you may have a class discussion on what these attacks are and who was affected or ask students to bring in an article about a recent cyber attack for discussion.
Standards Addressed	

Teaching and Learning Strategies	**Lesson Opener:**
	
	• Have students brainstorm and write down answers to the discussion questions listed below. Students can work individually or in groups/pairs. Have them share their responses. [5 mins]
	
	Activities:
	
	• Watch the lesson video and complete the corresponding quiz. [5-7 mins]
	• Watch the *WannaCry Ransomware Attack* connection video and fill out the corresponding reflection. [5 mins]
	• Explore the *Ransomware Simulator!* simulation. [5 mins]
	  ◦ What would you do if this simulation were real?
	  ◦ Why do you think the hacker is asking for Bitcoin?

	◦ Allow students to look at and play around with the code. If the simulation stops working, have students go to the HISTORY tab and reset their code. • Watch the *IoT and Connected Cars* and the *Cybersecurity and Connected Cars* connection videos and fill out the corresponding reflection. [10 mins] • Explore the *Threat Map* interactive connection. [10 mins] ◦ Ask students to find at least one interesting fact from the connection to share with the class. ◦ Students can work individually or in pairs. • Complete the *Why Learn about Cybersecurity?* free response activity. [5 mins] • Explore the *QR Code Generator* simulation. [5 mins] ◦ One code can be displayed at the front of the class and all students can try to connect using their phones. How many connected devices can you get? ◦ Another option would be for students to try to "pass a message" across the room going from one phone to another. ◦ Allow students to look at and play around with the code. If the simulation stops working, have students go to the HISTORY tab and reset their code. • Complete *The Internet of Things* handout. Students can work individually or in small groups/pairs. [15 mins] **Lesson Closer:** • Have students reflect and discuss their responses to the end of class discussion questions. [5 mins]
Discussion Questions	**Beginning of Class:** • Name as many devices as you can that connect to the Internet. ◦ *Phone, TV, computer, thermostat, etc.* • How many of these devices do you have in your home? ◦ *Answers will vary.* • What devices do we have at school? In this classroom? ◦ *Answers will vary.* **End of Class:** • Why do we use IoT devices? What are the benefits? ◦ *Convenience and connectedness are usually the biggest benefits of IoT devices.* • What are the risks of using IoT devices? ◦ *Any device that can connect to the Internet can be hacked. This includes anything from airplane controls to baby monitors.* • What do you think is meant by "unintended effects" regarding the Internet of Things? ◦ *Unintended effects are usually malicious consequences of being connected to the Intenet. For example, house maps made by Roomba vacuums can be used by hackers/burglars to gain a layout to your house.*
Resources/Handouts	The Internet of Things (teacher version) The Internet of Things (student version)

Vocabulary

Term	Definition
Cybercrime	Identity theft, stealing money, stealing private information, controlling private computers.
Ransomware	Ransomware is a type cyber attack that threatens to publish the victim's data or block access to it unless a ransom is paid.
Internet of Things	The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data.

Cybersecurity	Protection of computer systems, networks, and data from digital attacks.

Modification: Advanced	Modification: Special Education	Modification: English Language Learners