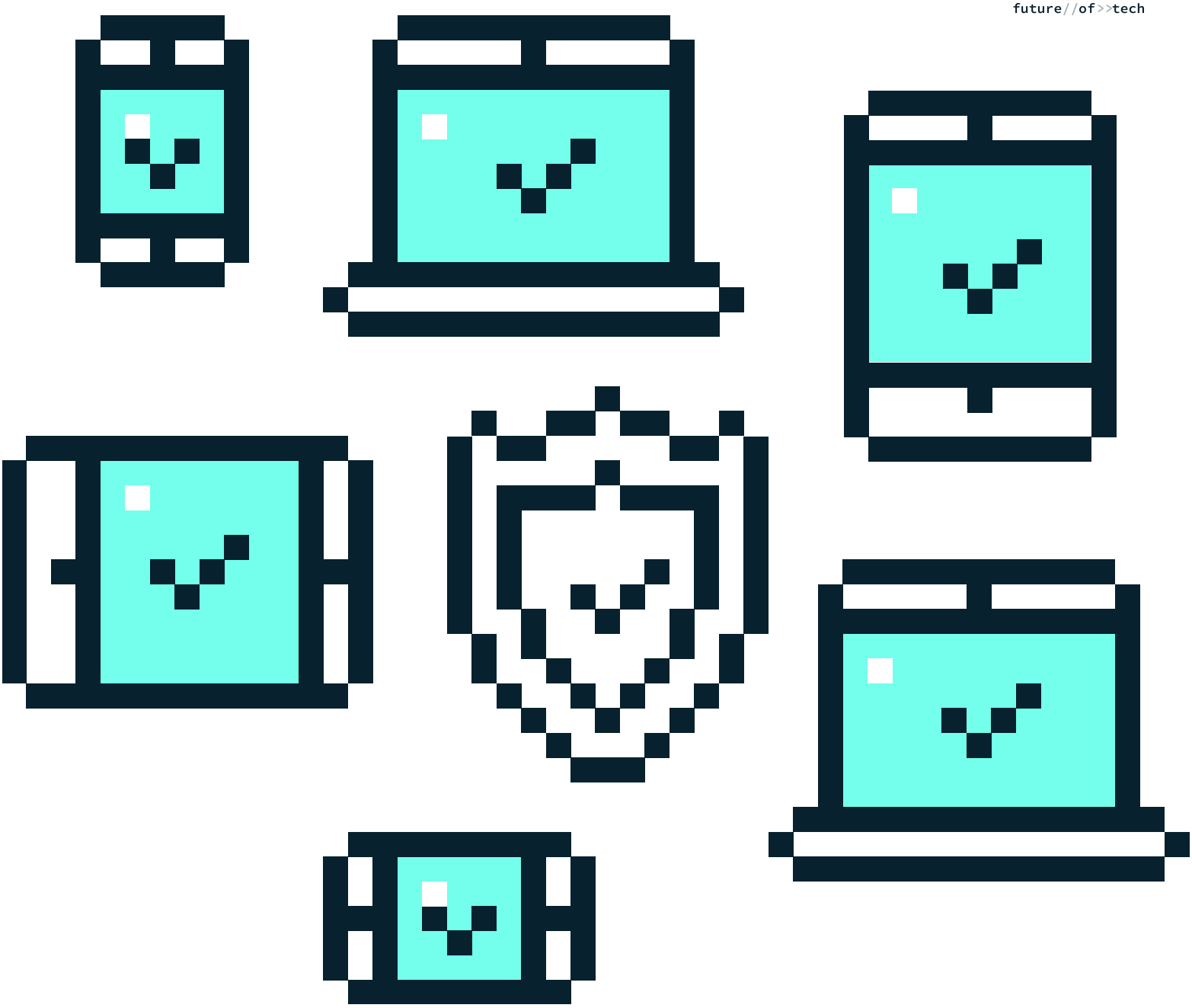
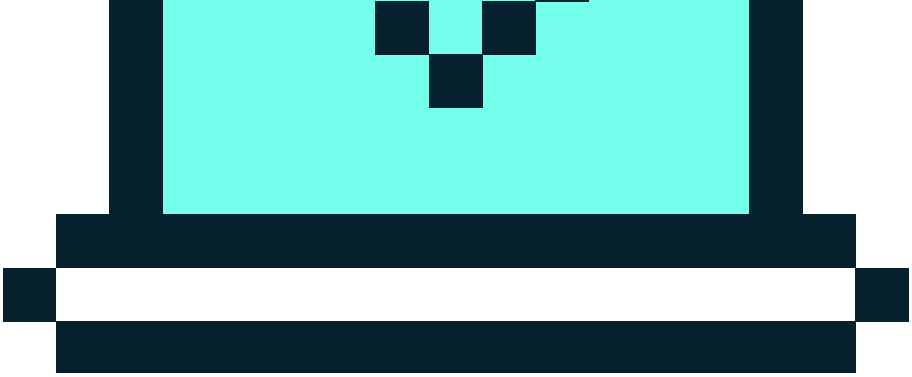


Lesson Plan >

CYBERSECURITY



SNAPSHOT:

Providing access to our personal data and information isn't something that any of us does lightly. Companies work hard to protect their data and their customers' data from hackers and other nefarious parties. Sometimes it seems the companies are successful at thwarting attacks, but then there's an announcement that millions of people have had their information compromised. It seems like a never-ending race to protect or steal information. This lesson explores several key elements associated with cybersecurity, the field that concerns itself with protecting online data.

STUDENT LEARNING OBJECTIVES: **Students will be able to:**

- Define Cybersecurity
- Describe key terminology associated with cybersecurity
- Discuss the evolution of cybersecurity
- Explain the anatomy of a breach
- Identify the top vulnerabilities for computer systems
- Identify careers associated with cybersecurity
- Examine the FutureProof Project

SYNOPSIS:

Interactive: Decipher and Encryption	(20 minutes)
Teacher Input	(20 minutes)
Wrap Up	(5 minutes)
Assessment	

TEACHER'S GUIDE:

MATERIALS:
- KWL Worksheet
- Interactive: Decipher and Encryption
- Cybersecurity: Interesting Insights
- Cybersecurity Assessment
- Cybersecurity Assessment Answer Key
- Devices with Internet capabilities.
- Braingle Website

You'll want to refer often to the Future of Tech Website: **futureoftech.org**

To receive the answer key to the assessment, please email Eric Larson at elarson@comptia.org

INTRODUCTION:

Ask the students what comes to their mind when they think about cybersecurity. Record their responses on the board. Distribute the KWL Worksheet. Have the students to complete the first column and write down what they know about cybersecurity. Discuss their responses. Briefly explain that today's lesson will introduce them to the in's and out's of Cybersecurity.

Ask the students, "Why do you think it is important for us to be proactive in protecting data and what type of data should be protected. Record their responses on the board. Have the students complete the second column of the KWL Worksheet - "What do you want to learn about cybersecurity?" Allow the students to share what they want to learn about cybersecurity.

INTERACTIVE:

Introduce the interactive by explaining that Julius Caesar created a method of protecting his private military messages. The Caesar Cipher, a substitution cipher, is one of the simplest encryption methods. A Caesar Cipher involves replacing each letter of a secret message with a different letter of the alphabet which is a fixed number of positions further in the alphabet. Using the cipher (n+3) below, countless encrypted messages could be created. For example: "Look in the box" is encrypted as "orrn lq wkh era."

Explain that cybersecurity operates today much like Julius Caesar did in his day. It tries to stay one step ahead of the game to protect our data and privacy. Protecting data and privacy is just as important as protecting lives in today's data driven world. Hackers however are always trying to break codes and find gaps, which is why businesses and industry now have teams dedicated to cybersecurity. Now that " wkh vhfuhw lu rxw" (the secret is out), let the students try to crack the code on their own.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(Alphabet shifted by 3 spaces)

Divide students into groups of 2. Distribute "Interactive: Decipher and Encryption." Allow the students to solve and create their own secret messages.

TEACHER INPUT:

Explain how the Interactive: Decipher and Encryption introduced the students to various ways to code our private messages. Ask the students what type of information might be important to keep secure or encrypt in a way that others would have to decipher what it means. Discuss their responses. Encourage the students to identify both personal types of information and information collected by business and/or industry.

Transition to the Future of Tech website, explaining to the students that this website will enable us to explore the role of cybersecurity in more depth.

Divide the students into pairs. Utilizing the Future of Tech website, ask each group to identify five interesting insights related to one of the following categories under the Cybersecurity Learning Unit:

- What Is Cybersecurity?
- The Technologies Behind Cybersecurity
- Cybersecurity Past And Present: A Timeline
- How — And Why — A Hack Happens
- Top Vulnerabilities
- The Future Of Cybersecurity And Career Opportunities

Have the students record their insights on the "Cybersecurity: Interesting Insights" worksheet and report their insights to the class.

WRAP-UP:

Whitfield Diffie said, "The decisions we make about communication security today will determine the kind of society we live in tomorrow." Ask students to reflect on this statement and briefly describe how they envision the world they will live in based on the availability and abundance of data. How will cybersecurity shape and define their world?

ASSESSMENT:

Have the students complete column 3 on their KWL Worksheet –
What did you learn about cybersecurity?

EXTENDED LEARNING OPPORTUNITIES:

- Encourage students to compete in state and national competitions related to cybersecurity
    - TSA Cybersecurity Competition
- Have students complete a Career Interest Survey to see where their interests lie and discuss how their interests may align with career opportunities associated with cybersecurity.
- Using a 3D printer or Laser Cutter, have students design and fabricate their own Caesar Cipher. Search the internet for various templates and design ideas.
- Invite guest speakers from the field to your class to discuss the role that cybersecurity plays in business, school and/or public service.
- Search the Internet for age-appropriate activities related to the keywords cryptography, computer forensics and hacking to extend learning opportunities for your students.

WEBSITE RESOURCES:

The Cybersecurity Lab

STANDARDS ALIGNMENT:

CSTA K-12 Computer Science Standards (2017)

- 1A-IC-16 Compare how people live and work before and after the implementation or adoption of new computing technology.
- 1B-NI-04 Model how information is broken down into smaller pieces, transmitted as packets through multiple devices over networks and the Internet, and reassembled at the destination.
- 1B-IC-18 Discuss computing technologies that have changed the world, and express how those technologies influence, and are influenced by, cultural practices.
- 1B-IC-20 Seek diverse perspectives for the purpose of improving computational artifacts.
- 2-NI-04 Model the role of protocols in transmitting data across networks and the Internet.
- 2-IC-20 Compare tradeoffs associated with computing technologies that affect people's everyday activities and career options.
- 2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
- 3A-CS-01 Explain how abstractions hide the underlying implementation details of computing systems embedded in everyday objects.
- 3A-CS-02 Compare levels of abstraction and interactions between application software, system software, and hardware layers.
- 3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
- 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
- 3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 3B-AP-18 Explain security issues that might lead to compromised computer programs.
- 3B-IC-26 Evaluate the impact of equity, access, and influence on the distribution of computing resources in a global society.
- 3B-IC-27 Predict how computational innovations that have revolutionized aspects of our culture might evolve.

Next Generation Science Standards

- MS-ETS1-1. Define the criteria and constraints of a design problem with sufficient precision to ensure a successful solution, taking into account relevant scientific principles and potential impacts on people and the natural environment that may limit possible solutions.
- HS-ETS1-1. Analyze a major global challenge to specify qualitative and quantitative criteria and constraints for solutions that account for societal needs and wants.
- HS-ETS1-3. Evaluate a solution to a complex real-world problem based on prioritized criteria and trade-offs that account for a range of constraints, including cost, safety, reliability, and aesthetics as well as possible social, cultural, and environmental impacts.
- HS-ETS1-4. Use a computer simulation to model the impact of proposed solutions to a complex real-world problem with numerous criteria and constraints on interactions within and between systems relevant to the problem. (Addressed through Extended Learning Opportunities)

K-W-L CHART

WHAT I KNOW OR THINK I KNOW ABOUT CYBERSECURITY

WHAT I WANT TO LEARN ABOUT CYBERSECURITY

WHAT I LEARNED ABOUT CYBERSECURITY

interactive: decipher and encryption

Name: _____

Part One

Decipher the following sentences below using Caesar Cipher.

Number of letters to shift to the right = 3
1. **vfkrro lv ixq** =_____
2. **Pb whdfkhu lv wkh ehvw** =_____

Number of letters to shift to the right = 7
3. **thao huk aljouvsvnf dvyr avnlaoly** =_____
4. **pm vusf avkhf dlyl mypkhf** =_____

Part Two

Create your own secret message.

Using the table below, create your own cipher.
What is the number of letters to shift to the right? _____
Complete the table using your cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Write out a message for your partner to decipher.

Your Message Using The Cipher Above	Partner's Decipher

What is your secret message? Did your partner decipher it correctly?

Write out a message for your partner to decipher.

Your Message Using The Cipher Above	Partner's Decipher

What is your secret message? Did your partner decipher it correctly?

Part Three

Go to Braingle.com. Click on Puzzles, then Codes and Ciphers. Explore the various categories of ciphers.

Create an example of each of the following cyphers:
• one monoalphabetic cipher
• one polyalphabetic cipher
• one polygraphic cipher
• one transposition cipher
• one other cipher

Allow the students to share their messages and discuss if time permits.

Monoalphabetic Cipher Selected: Description of Cipher Selected:	Your Message: Your Message Enciphered:

Polyalphabetic Cipher Selected: Description of Cipher Selected:	Your Message: Your Message Enciphered:

Polygraphic Cipher Selected: Description of Cipher Selected:	Your Message: Your Message Enciphered:

Transposition Cipher Selected: Description of Cipher Selected:	Your Message: Your Message Enciphered:

Other Cipher Selected: Description of Cipher Selected:	Your Message: Your Message Enciphered:

INTERESTING INSIGHTS

Group Members:

In groups, select one of the following sections of the Future of Tech website (futureoftech.org) to review.

- **What is Cybersecurity?**
- **The Technologies Behind Cybersecurity**
- **Cybersecurity Past and Present: A Timeline**
- **How — and why — a hack happens**
- **Top Vulnerabilities**
- **The Future of Cybersecurity and Career Opportunities**

Section our group chose:

Provide a brief overview of the section in two or three sentences:

List five interesting insights that your group learned while reviewing the section.

1.

2.

3.

4.

5.

cybersecurity assessment >

Name: _____

Select the best response.

1. Preventing data breaches and protecting information is known as:
a. Intel
b. Forensics
c. Cybersecurity
d. Hacking

2. A unit of information is known as
a. Data
b. BIt
c. Intel
d. Point

3. Describe the difference between a breach and hack.

Match the following:

____4. Phishing
____5. Malware attacks
____6. Social Engineering
____7. Attractive Data
____8. Bots

A. viruses or worms that burrow into a computer system and take over
B. software applications that run automated task
C. when hackers get people to turn over personally identifiable information that can later be used to hack a system
D. plays on the helpful nature of people and their willingness to trust what they're told and hand over personal information if they're scared
E. your personally identifiable information (PII)

9. List two examples of data that are attractive to hackers.

10. List the top 5 things that make systems vulnerable.