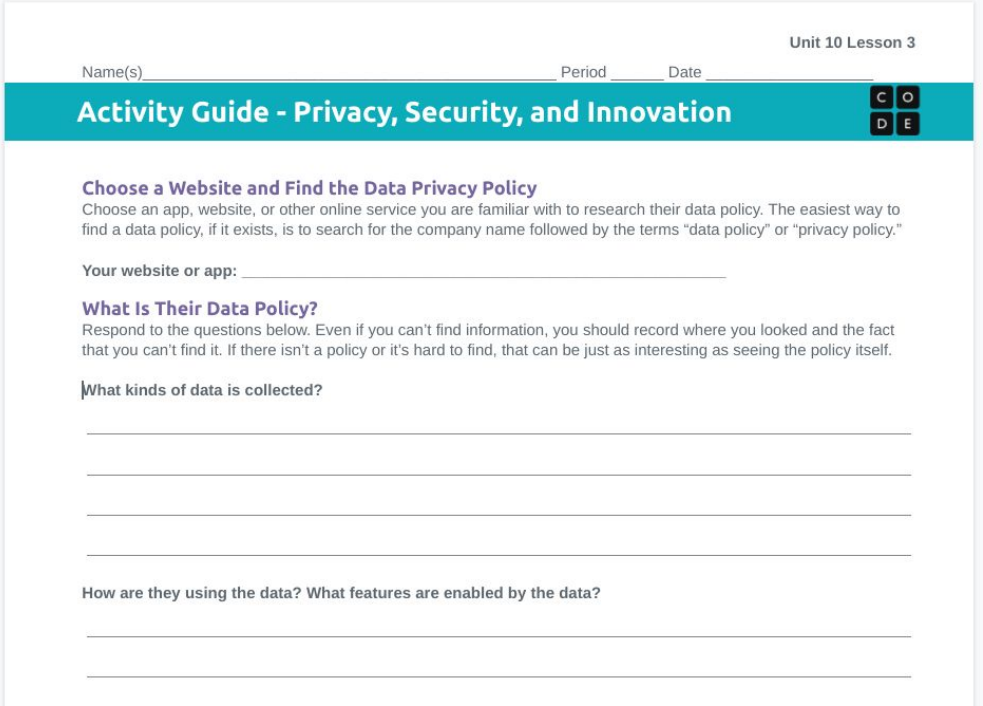
Unit 8 - Lesson 2
Data Policies and Privacy

Computer Science Principles

Pick a website or app of your own and complete the **front page of the activity guide.** 30 mins

Some apps / services to consider:

- Education: Code.org, Khan Academy, Codecademy.com
- Social media: Facebook, Twitter, Instagram, Snapchat, Tik Tok
- Online store: Amazon, Target, Walmart
- Search: Google, Bing
- Maps: MapQuest, Yahoo Maps, Google Maps
- Productivity: MS Office Online, Google Docs
- Mail & communication: Gmail, Hotmail, Yahoo Mail, Skype, Google Hangouts
- Streaming sites: Netflix, Spotify, Pandora
- Gaming sites: Steam, Xbox Live
- Banks and financial institutions: Chase, Citibank



Unit 10 Lesson 3

Name(s)_____ Period _____ Date _____

Activity Guide - Privacy, Security, and Innovation

C O D E

Choose a Website and Find the Data Privacy Policy

Choose an app, website, or other online service you are familiar with to research their data policy. The easiest way to find a data policy, if it exists, is to search for the company name followed by the terms "data policy" or "privacy policy."

Your website or app: _____

What Is Their Data Policy?

Respond to the questions below. Even if you can't find information, you should record where you looked and the fact that you can't find it. If there isn't a policy or it's hard to find, that can be just as interesting as seeing the policy itself.

What kinds of data is collected?

_____

_____

_____

_____

How are they using the data? What features are enabled by the data?

_____

_____

Key Takeaways

- **Personally Identifiable Information (PII):** information about an individual that identifies, links, relates, or describes them.

- Technology enables the collection, use, and exploitation of information about, by and for individuals, groups, and institutions. Geolocation, cookies, and browsing history can all be used to create knowledge about an individual. Most digital technology needs some kind of PII to work (for example street navigation needs to know your location or PII stored online to simplify making online purchases).

- Other times websites collect more data to improve their services.

- Many services and websites collect information (like your browser history) that can be used to advertise to you by creating detailed profiles of who you are and what you like. Search engines also can record and maintain a history of searches made by users. This information can be used to suggest websites or for for targeted marketing.

- Once data is made digital, and especially once it's shared online, it's much harder to control.

- PII can be used to steal the identity of a person, or stalk them online. Information that is often posted on social media can be combined to create a profile on you.

Key Takeaways

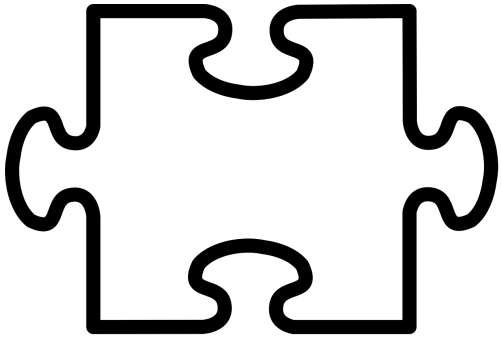
- Our private data powers a lot of computing innovations in ways we like. It makes products that are convenient, interesting, personal, useful, and often “free” because we “pay” with our data.
- Not every effect of a computing innovation is anticipated in advance.
- This data can also be used by companies, governments, or criminals in ways that we didn’t intend or that threatens our privacy.
- The balance between innovation, privacy, and security is continually being debated. You’re part of the next generation that will decide what kind of digital society we live in.
- Legal and Ethical Concerns are raised by:
  - Computing innovations that harm people
  - Computing innovations that play a role in social and political issues
  - Examples:
    - software that allows access to digital media downloads and streaming
    - algorithms with bias
    - devices that collect and analyze data by continuously monitoring activities

Computing innovations can have unintended consequences. Some of these unintended consequences are positive and some are negative.

While it is impossible to predict every outcome, by thinking critically and bringing multiple perspectives to the table we can try to better predict the ways our innovations may impact the world.

Unit 8 - Lesson 5
Security Risks Part 1

Computer Science Principles



Jigsaw:

With your jigsaw group, navigate to your assigned level on Code Studio.

Keylogging (level 1)
Phishing (level 2)
Malware (level 3)

- Look at the examples
- Read the articles
- Create a PSA (Public Service Announcement) slide.
  - What is the security risk?
  - How are people targeted?
  - What are the warnings?

Note: Add at least 1 visual per slide! Don't write a paragraph on your slide. Each person in the group needs to make a slide on their respective topic.

Vocabulary:

Phishing: a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Keylogging: the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information

Malware: software intended to damage a computing system or to take partial control over its operation

Rogue Access Point: a wireless access point that gives unauthorized access to secure networks.

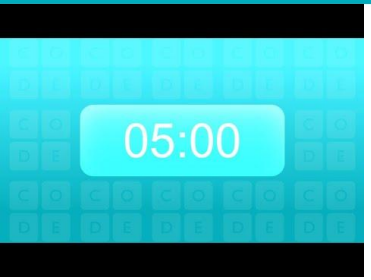
Unit 8 - Lesson 6
Security Risks Part 2

Computer Science Principles

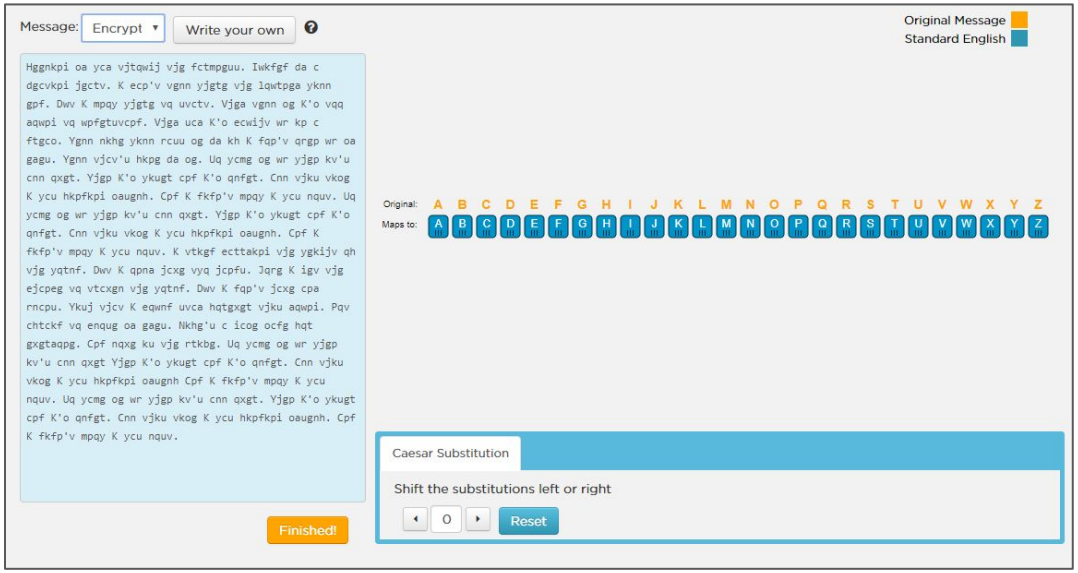

THE INTERNET
CYBERSECURITY
& CRIME

Unit 8 - Lesson 8
Protecting Data Part 1

Computer Science Principles



Caesar Cipher



Do This:

- Navigate to Level 1
- Experiment with the tool: click things, poke around, figure out what it's doing
- Choose one of the messages from the drop-down menu and try to crack it using the tool.

Encryption Terms

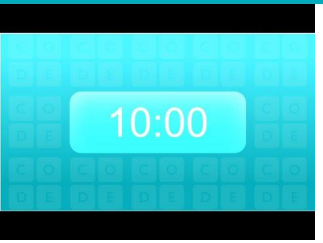
Encryption: a process of encoding messages to keep them secret, so only "authorized" parties can read it.

Decryption: a process that reverses encryption, taking a secret message and reproducing the original plain text.

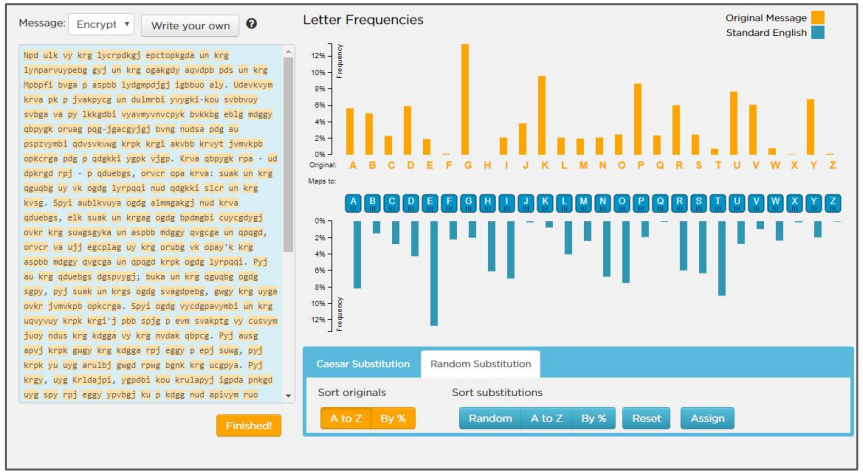
Cipher: the generic term for a technique (or algorithm) that performs encryption

Caesar's Cipher: a technique for encryption that shifts the alphabet by some number of characters.

Cracking encryption: When you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to crack the encryption.



Random Substitution Cipher



Do This: Crack a message using the tips we just talked about

- Find the short words and "crack" them first. How many one-letter words do you know? ("a"). A very common 3-letter word is "the".
- * Once you've done that, you have substitutes for some of the most common letters. You should be able to use intuition to look at other words with these partial substitutions and make good guesses.
- * After finding only a handful of hard-fought letters, the rest will tumble quickly.
- * Comparing the frequencies of letters gives good insight for making sensible guesses.


THE INTERNET
ENCRYPTION
& PUBLIC KEYS

Prompt:

What is the difference between symmetric encryption and asymmetric (public key) encryption?

Vocabulary:

Encryption: a process of encoding messages to keep them secret, so only "authorized" parties can read it.

Decryption: a process that reverses encryption, taking a secret message and reproducing the original plain text.

Symmetric Key Encryption: involves one key for both encryption and decryption.

Public Key Encryption: pairs a public key for encryption and a private key for decryption. The sender does not need the receiver's private key to encrypt a message, but the receiver's private key is required to decrypt the message.

Unit 8 - Lesson 9
Protecting Data Part 2

Computer Science Principles

What can I do to protect my data?

1. Use Multifactor Authentication

Single Factor Authentication

Something you know

Example: Password

Two Factor Authentication

Something you know

Example: Password

Something you possess

Example: Phone

Multifactor Authentication - at least two of these:

Something you know	Something you possess	Something you are
Example: Password	Example: Phone	Example: Fingerprint

What can I do to protect my data?

1. Use Multifactor Authentication
2. Update Your Software

Single-Select Questions with Reading Passage (SSQRP)

- What's SSQRP?
  - Shows up on the AP CSP exam
  - Features a pretend computing innovation with a short explanation
  - Five multiple choice questions focusing on data, purpose and effect, benefits and harms, and security concerns.

Unit 8 Lesson 9 - Activity

Single-Select Questions with Reading Passage (SSQRP) pull a total of 5 questions from each of these categories (computational thinking practices). The italics text represents text that may change depending on the computing innovation. The text highlighted in yellow represents the types of phrases you may see in these questions. The text in square brackets [ ] are different question options.

Sample Questions

Practice 3: Abstraction in Program Development	Practice 5: Computing Innovations
Which of the following input data [must be obtained/is needed] *by the upgraded system that was NOT needed by the original system?*	Which of the following is considered a potential effect of the *the application* rather than a [function/purpose] *of the application?*
Which of the following data is not [obtained/provided] *directly from the user* but is necessary for *the upgraded system to operate as described?*	Which of the following is [LEAST/MOST] likely to be a [BENEFIT/HARM] of *storing the information from each calling session in a database?*
Which of the following data is necessary for the *Call Center* to process in order to enable *it to provide an answer to the caller?*	Of the following potential benefits, which is [LEAST/MOST] likely to be provided by *the upgraded system?*
Which of the following is [LEAST/MOST] likely to be included in *the directory?*	Which of the following may be an unintended effect of the use of *Call Center?*
	Which of the following is the [LEAST/MOST] [likely/plausible] data [PRIVACY/SECURITY/STORAGE] concern *of the upgraded system?*
	Which of the following *groups* is [LEAST/MOST] likely to receive *targeted advertisements?*
	Which of the following statements is [LEAST/MOST] likely to be true about the tradeoffs of *the Call Center recording the caller's phone number?*

Vocabulary:

Multifactor Authentication: a method of computer access in which a user has to successfully provide evidence in at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). Each step provides a new layer of security.

Computer Virus Scanning Software: protects a computing system against infection.