Rapid Research - Cybercrime

Unit 4 Lesson 10 (U4L10)

Table of Contents

The Internet: Cybersecurity and Crime

(5:01)

Worksheet - Video Guide for "Cybersecurity and Crime"

[Video Guide Answer Key]

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

Project Overview: Cybersecurity and Crime

In this small project, you will research a recent cybercrime event and present a “one-pager” about it. In particular you will focus on the data privacy and security concerns raised by the event.

The One-Pager

You will do a bit of online research and then prepare a one-page summary or “one-pager” to show the rest of the team or colleagues about the highlights of what you found. For this project you will prepare a one-pager that explains:

- The details of a specific recent cybercrime event
- The specific data security or privacy concerns raised by the event.

General Process & Requirements

- Review the One-Pager Template (provided by your teacher) and the **Rubric** below.
- Choose a cybercrime event using the guide below to help.
- Conduct your research by following the **Research Guide** below.
- Complete the one-pager.

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

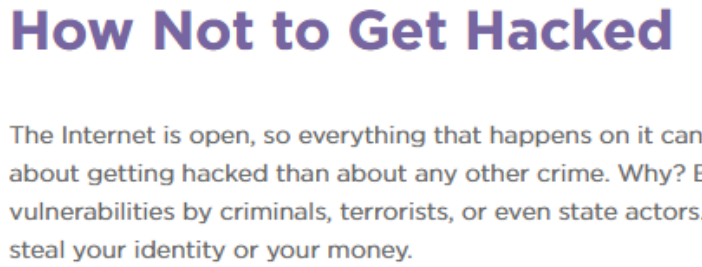
Choose Your Cybercrime Event

You should choose a recent cybercrime event that you find personally relevant or interesting. For the purposes of this project, we'll define a cybercrime event as any instance where digitally stored data falls into the hands of someone not originally intended to have access to it.

Read *How Not To Get Hacked*

Get some ideas of different types of cybercrimes or risks by reading the

- (link in Code Studio) https://code.org/curriculum/csp/docs/hownottogethacked
- Each of the 9 tips listed is related to a particular type of cybercrime


How Not to Get Hacked

The Internet is open, so everything that happens on it can
about getting hacked than about any other crime. Why? E
vulnerabilities by criminals, terrorists, or even state actors
steal your identity or your money.

Choose an Industry / Product / Company of Interest

Choose an industry, product, or company of interest and try to find instances of it having been hacked or leaked in some way. Aim to find stories where a piece of technology actually was hacked or failed, leading to the release of data. Avoid stories where someone just posts private information online.

Potential search terms include:

- "_____ leak"
- "_____ hack"
- "_____ breach" or "_____ data breach"

Check the news

The rate of cybercrime seems only to be increasing, and it's likely that recent news includes some instance of cybercrime. Search through recent news stories and see if you can quickly identify a cybercrime event as your topic. Just make sure your cybercrime actually involves data falling into the wrong hands.

Conduct Your Research

You already have some practice finding good resources online. You'll want to find **recently published documents** from **authoritative sources.** There is no need to use overly technical documents, but keep an eye out for familiar terminology and topics.

Key Information to Find

- **Overview:** Whose data was stolen? When did this happen? Briefly explain the context of the event.
- **Data Specifics:** What specific data fell into the wrong hands?
- **How was it stolen / How to Prevent:** How specifically was the data stolen? Is this a flaw in the technology? Were there any cybersecurity measures in place? How might this type of attack be prevented in the future?
- **Data Privacy / Security Concerns:** What specific concerns arise from this data being stolen? Is there already evidence of the data being used in concerning ways? Try to find how the privacy or security of some people were compromised.

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

In Classroom, use the One-Pager Template.

ALL text in *Italics* MUST be REPLACED and/or DELETED.

Cybersecurity and Crime One-Pager Template
<change this to your title>

Note: *All text in Italics, including this text, is intended to be replaced by your responses, and deleted once you've completed your one-pager.*

Overview
When did the event happen?
Whose data was lost / stolen / leaked? How many people / organizations were affected?
Provide any other context necessary to understand the "big picture" of the event.

How and How to Prevent
What specific type of attack / mistake led to the data falling into the wrong hands? Reference terms in "How Not to Get Hacked" where applicable. What types of cybersecurity techniques might be used to help prevent this from happening again?

Data Specifics
What specific data was stolen? Try to avoid vague terms like "financial data" and instead find the specific pieces of information like "credit card numbers". Specific answers here will strengthen your explanation in the next section.

Data Privacy / Security / Storage Concern
What specific concerns arise from this data being used in unintended ways or by unintended people? Is there already evidence of the data being used in these ways? Cite sources if you can find specific news stories.

Sources
List all websites that you used to find any information you wrote here. Include the permanent URL. Identify the author, title, source, the date you retrieved the source, and, if possible, the date the reference was written or posted. You should number your sources, here is a template you can follow:

[1] Author's Last name, First name. "Title of Web Page." Title of Website, Publisher, Date, URL. Date retrieved.
[2] Author's Last name, First name. "Title of Web Page." Title of Website, Publisher, Date, URL. Date retrieved.
[3] ....

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

Day 1 - Choose Cybercrime Event, Read and Research

Review Activity Guide and Rubric: At the beginning of the project, emphasize the importance of reviewing the one-pager template and rubric. Students may assume that more is required of them than is actually the case. Point out that the written component is quite short. They probably have space for at most 100-150 words per response.

Choosing Your Cybercrime Event: It is recommended that you place a time limit on this process (e.g. 20 minutes). Students should not leave class after the first day without a topic in mind and ideally with some resources identified. Luckily, in choosing their topics, students will likely have begun to identify resources they can use in completing their project.

Conducting Your Research: This document is intended to serve primarily as a guide to students for identifying online sources of information. The skill students need to develop is identifying useful resources on their own and then synthesizing this information. Being presented with a structured way of doing this means students will have a model for how to complete their research when completing the actual Explore PT.

Day 2 - Prepare one-pager

Complete One-Pager: Students should find this aspect of their project most familiar. The prompts are similar in style and content to prompts students have already seen. Emphasize the need for clarity in their writing, and remind them that everything must fit on a single page. If they have responded completely to each of the prompts, it is fine to write less.

Sharing/Submission: You may want to collect students' one-pagers, have them share in small groups, or with the whole class. Since students were researching something of their own choosing, they might be eager to show what they found out.

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

Component	1	2	3	Score
Written Responses				
Data Specifics	The description of the data that was lost / stolen lacks any specific details. The description may discuss the device that was compromised rather than the data it was capturing.	The response identifies the category of data lost / stolen but may not provide specific details. The response does refer to data specifically, rather than the device used to store or capture it.	The response specifically identifies the types of data that were stolen / lost in the event. If the response describes both the device capturing the data and the data itself it clearly distinguishes between the two.	
Data Concern	The concerns described are not directly related to the data that was lost / stolen.	The response describes general data security or privacy concerns without specifically tying them to the data released in the event.	The response describes a data security or privacy concern directly related to the specific data that was leaked. It may be reinforced with a citation to a news story about the aftermath of the leak.	

Unit 4 Lesson 4 (U4L10)
Rapid Research - Cybercrime

Cybercrime Definition: The definition of a cybercrime event as "any instance where digitally stored data falls into the hands of someone not originally intended to have access to it" is used to help align this task to the Explore PT.

In particular this definition sets up the last two prompts of the activity guide where students must both specifically identify the data used by an app and describe concerns specifically related to this data. These are critical skills students must use when describing the computing innovation they will research. Make sure you reinforce this definition as students choose their topics.

Review Cybersecurity Terms

Implementing cybersecurity has software, hardware, and human components.

- This is a theme for the whole lesson
- Vulnerabilities in hardware and software can be compromised as part of an attack.
- But, as mentioned in the video, a large percentage of cybersecurity vulnerabilities are human-related, such as choosing bad passwords, (unintentionally) installing viruses, or giving personal information away.

Review Cybersecurity Terms

Sockets layer/transport layer security (SSL/TLS)

- An encryption layer of HTTP. When you see the little lock icon and https it means that you are visiting a website over HTTP but the data going back and forth between you and the server is encrypted.
- SSL (secure sockets layer) and TLS (transport layer security) use public key cryptography to establish a secure connection.

Cyber warfare and cyber crime have widespread and potentially devastating effects.

- This is especially true in the case of warfare which (fortunately) we have not experienced much of on a global scale. But using cyber attacks to cripple basic infrastructure (power, water) and communication could be devastating

Review Cybersecurity Terms

Cyber warfare and cyber crime have widespread and potentially devastating effects.

- This is especially true in the case of warfare which (fortunately) we have not experienced much of on a global scale. But using cyber attacks to cripple basic infrastructure (power, water) and communication could be devastating

Distributed denial of service attacks (DDoS)

- Typically a virus installed on many computers (thousands) activate at the same time and flood a target with traffic to the point the server becomes overwhelmed -- doing this can render web services like DNS, or routers, or certain websites useless and unresponsive.

Review Cybersecurity Terms

Phishing scams

- Typically a thief trying to trick you into sending them sensitive information. Typically these include emails about system updates asking you send your username and password, social security number or other things.
- More sophisticated scams can make websites and email look very similar to the real thing.

Review Cybersecurity Terms

Viruses / Antivirus software and firewalls

- A virus is program that runs on a computer to do something the owner of the computer does not intend. Viruses can be used as a Bot Net to trigger a DDoS-style attack, or they can spy on your computer activity, such as capturing all the keystrokes you make at the computer, or websites you visit, etc.
- Antivirus software usually keeps big lists of known viruses and scans your computer looking for the virus programs in order to get rid of them.
- A "firewall" is simply software that runs on servers (often routers) that only allows traffic through according to some set of security rules.