The Ransomed Files

EXERCISE-IN-A-BOX LESSON PLAN (16-17 years old)

OVERVIEW

This lesson will provide students with an understanding of cybersecurity, cybercrimes, and ransomware, highlighting the potential consequences of falling victim to these attacks. By learning about these concepts, students will be better equipped to protect themselves and their personal information from online threats.

LEARNING OBJECTIVES

Students will be able to:

• Demonstrate an understanding of how cybersecurity works and the impact when security is breached.

• Identify the cybercrime attacks and describe the motivations behind why cybercrimes occur.

• Examine the basic characteristics of ransomware and evaluate strategies for protecting devices from ransomware attacks.

DURATION

60 minutes

KEYWORDS

• **Cybersecurity**: Cybersecurity refers to the practices and technologies used to protect devices, networks, and data from unauthorised access, theft, or damage. It involves measures like antivirus software, firewalls, and password protection to prevent cyber attacks.

• **Cybercrime**: Cybercrime refers to criminal activities committed using the internet or other digital technologies. It can include online identity theft, hacking, fraud, and cyberstalking, among others.

• **Ransomware**: Ransomware is like a digital "kidnapping" of your files. It is a type of malicious software that is designed to block access to a computer system or data until a ransom is paid. It can be installed through malicious email attachments or links, and once installed, it encrypts files on the victim's computer, making them inaccessible until the ransom is paid.

INTERNET INDEPENDENT FRAMEWORK

The learning objectives in this workshop are aligned with the **Privacy & Information Security** pillar of the Internet Independent Framework. Visit cyberlite.org for more information.

The Ransomed Files

EXERCISE-IN-A-BOX LESSON PLAN (16-17 years old)

WARM-UP
5 MINUTES

Slide 1

Say: Today, we will be learning about privacy and information security. Cybersecurity is an important part of how we protect ourselves online, because there are a lot of cybercrimes and bad actors that want to exploit our vulnerabilities.

Slide 2

Ask: What settings do you currently use to keep yourself safe and your devices secure?
Common settings include having a passcode or Face ID enabled to unlock your phone, enabling two-factor authentication for online accounts, and installing antivirus software.

Slide 3

Ask: Can you name some different kinds of cybercrimes?
Some cybercrimes students may be familiar with are phishing, internet scams, hacking or unauthorised access to accounts, and stealing of personal information.

DEFINE THE KEYWORDS
15 MINUTES

Slide 4

Ask: Does anyone know what cybersecurity, cybercrime, and ransomware mean?
Allow students to guess or extrapolate meanings. Guide students to think about these key concepts in the context of privacy and information security.

Slide 5

Read the contents of the slide aloud.

Discuss: Do you think people take online security seriously enough? Why or why not?
Encourage students to voice their opinions on online security as it is a good opportunity to learn how seriously students are taking this matter. If most students have a relaxed view on cybersecurity, it is important to emphasise the negative consequence of weak security practices.

Slide 6

Read the contents of the slide aloud.

Discuss: Have you heard of any cases of cyberattacks or cybercrimes in the news lately?
It is recommended to prepare some relevant news stories ahead of the lesson. Try to find recent cases of cybercrimes that have occurred in your local area, or with recognisable brand names for students to relate to.

Slide 7

Read the contents of the slide aloud.

Discuss: What do you think are the motivations of cybercriminals to send out ransomware?
A cybercriminal's main motivation in a ransomware attack is mainly for financial gains. Holding files ransom means the cybercriminals are demanding money in exchange for an encryption key to unlock the victim's files.

INVESTIGATE THE SCENARIO
30 MINUTES

Slide 8

Say: In this next section, we will explore a scenario about a company called Pets Couture. Remember to keep the keywords we've just learned in mind as I show you five pieces of evidence we'll investigate together. Think critically about the information we're examining and consider the discussion questions.

(Optional) Select eight students to read as these characters: Email sender, Ransomware hacker, Clarke, Ralph, Elsa, Yusef, Suresh, and Denise. Commenters: Gary and Vanessa.

Slide 9

Read this email sent to the finance department of Pets Couture.

Discuss the following questions:

1. What clues can you use to determine whether or not this is a legitimate request?
The first clue is in the sender's email address - the email signature is from "Happy Cat Friends Co." but the email address is spelled differently. Many phishing emails are sent from addresses that are only a few letters off from the original domain to trick users into thinking it's authentic. Another clue is that the payment link looks suspicious, as "national" is misspelt in the URL. Remember to never click on any links from unknown senders.

2. What tactics has the sender used to persuade the recipient? Think about the tone of voice and language used.
The tone of voice and language used creates a strong sense of urgency and is

very intimidating. They have persuaded the recipient to act quickly under the threat of legal action.

Slide 10

Read this ransomware note.

Discuss the following questions:

1. How does ransomware work? What have the hackers held hostage?
The hackers have held the company's files hostage, including all documents, photos, and databases with an encryption cipher. This means no one in the company is able to access anything unless the ransom is paid off.

2. What are the potential risks and rewards of paying off the hackers?
The potential risk of paying off the hackers if they may not actually release the files back to you as they could disappear without a trace. The reward would be if the hackers kept their word and restored the files.

3. How do these cybercriminals want to receive payment?
The cybercriminals have asked to receive payment in cryptocurrency. Cybercriminals typically ask for ransom payments in cryptocurrency, such as Bitcoin, because it is difficult to trace.

Slide 11

Read this conference call between Clarke, Ralph, Elsa, and Yusef.

Discuss the following questions:

1. What are some of the consequences of a ransomware attack for a company?
Some consequence Pets Couture faces is the loss of sales as they can't process any orders on their website now, and customers might lose trust in the business.

2. How can companies prevent a ransomware attack from happening?
Companies can prevent a ransomware attack by training their staff and making sure no one clicks on phishing emails with malicious links. They can also install stronger antivirus software so the virus isn't able to access the entire network.

Slide 12

Read this social media post by Suresh.

Discuss the following questions:

1. How has Pets Couture's cyberattack affected their company's reputation and customer trust?
Cyberattacks can compromise sensitive customer information and damage the reputation and trust of a company. Customers may be hesitant to continue doing business with a company that has experienced a cyber attack or data breach.

2. What is the impact of the Pets Couture website being down on their business and customers?
The Pets Couture website being down prevents customers from making purchases, which can lead to lost revenue and damage to the company's reputation. The frustration expressed by customers on social media can also discourage potential customers from doing business with Pets Couture in the future.

Slide 13

Read these messages between Clarke, Ralph, and Denise.

Discuss the following questions:

1. Split into two groups and conduct a mini debate. Group A will argue for Clarke to pay the ransom and Group B will argue that he should wait for the authorities to step in.
Here are three points for each group:

Group A (arguing for Clarke to pay the ransom):

1. *Time is of the essence in this situation and waiting for the authorities to step in could take too long, leading to significant financial losses and damage to the company's reputation.*
2. *Paying the ransom may be the only way to retrieve the stolen data and avoid further harm to the company and its customers.*
3. *The hackers may not release the data even if the authorities get involved, leaving the company in a worse position.*

Group B (arguing against paying the ransom):

1. *Paying the ransom is illegal and unethical, and sets a dangerous precedent that could encourage further cybercrime in the future.*
2. *Waiting for the authorities to step in is the right thing to do, as it prioritises the safety and security of the customers' data.*
3. *Even if the company pays the ransom, there is no guarantee that the hackers will keep their promise and release the data. It could be a scam to get more money out of the company.*

KEY TAKEAWAYS
10 MINUTES

Slide 14

Say: Here are some things we've learned from this lesson.

1. Cybersecurity is a shared responsibility, and everyone has a role to play in protecting themselves and their communities from cyber threats.

2. Ransomware attacks can cause significant damage to individuals, businesses, and governments, including financial losses, reputational harm, and disruption of critical services.

3. It is important to take proactive measures to prevent cybercrimes and be cybersecure, such as keeping software up to date, using strong passwords, and backing up important data.

Ask: **What are some key takeaways you've learned from this lesson?**
Call on volunteers to share what they've learned.