**Pre-Reading Activity**

Think about cybersecurity and online safety. Have you or someone you know ever experienced a cyber threat, such as a phishing email, a hacked account, or a scam? Write your answer in 3-5 sentences.

* I know the basics of cybersecurity to prevent certain attacks but I don't have superior knowledge. I know some people who work on it and as curious as it may sound, the most dangerous/vulnerable thing will always be the human factor, no matter how confident you are, it is the only variable that cannot be controlled 100%.

**Cybercrimes that shocked the world**

In recent years, cybercrimes have become a global concern, affecting individuals, businesses, and even governments. While cyberattacks happen every day, some cases stand out due to their scale, impact, or the unusual techniques used by criminals. Here are some of the most shocking cybercrimes in recent history.

One of the most infamous cyberattacks took place in 2017 when the WannaCry ransomware infected over 200,000 computers in 150 countries. The malware exploited a vulnerability in Microsoft’s operating system, encrypting users' files and demanding a ransom in Bitcoin to unlock them. Hospitals, banks, and government institutions were among the victims. The attack caused chaos, forcing hospitals in the UK to cancel appointments and surgeries. It was later revealed that the attack had been carried out by a group of hackers linked to North Korea.

Another remarkable case occurred in 2013 when Yahoo suffered the biggest data breach in history. Over three billion user accounts were compromised, exposing personal details such as names, email addresses, and passwords. The company initially reported that one billion accounts had been affected, but later investigations confirmed that the number was much higher. The breach raised serious concerns about data protection and forced Yahoo to strengthen its security measures.

In 2020, Twitter experienced a shocking security breach that targeted some of the most influential people in the world. Hackers gained access to the accounts of high-profile figures, including Barack Obama, Elon Musk, and Bill Gates. They posted messages promoting a Bitcoin scam, promising to double any money sent to a specific wallet. Many people fell for the scam, losing thousands of dollars. Investigations later revealed that the attack was carried out by a group of young cybercriminals who exploited Twitter’s internal systems.

Another disturbing example is the rise of cyber extortion cases. In 2021, the American company Colonial Pipeline suffered a ransomware attack that forced it to shut down its fuel supply system. The attackers, a cybercriminal group known as DarkSide, demanded millions of dollars in ransom to restore operations. The attack caused fuel shortages across the East Coast of the United States, highlighting the vulnerability of essential services to cyber threats.

These cases demonstrate how cybercrimes are evolving and becoming more sophisticated. Governments and companies are investing heavily in cybersecurity, but hackers continue to find new ways to exploit weaknesses. As technology advances, individuals must also take precautions to protect their personal data and online accounts. The world is becoming increasingly digital, and staying informed about cyber threats is more important than ever.

**Post-Reading Activities**

**1. Cybercrime Terminology Match-Up**

Match the following terms (a-h) with their correct definitions (i-viii):

a) Ransomware

viii. A form of malware that locks a user’s files and demands payment for their release.

b) Phishing

iii. A scam where attackers send fake emails or messages to steal personal information.

c) Identity Theft

vi. A type of cybercrime where criminals steal personal data to impersonate someone else.

d) DDoS Attack

ii. A cyberattack that floods a website or service with excessive traffic to make it unavailable.

e) Data Breach

iv. A security failure where sensitive information is exposed without authorization.

f) Social Engineering

i. A technique where hackers manipulate people into revealing confidential information.

g) Malware

v. Malicious software designed to damage, disrupt, or gain unauthorized access to a system.

h) Encryption

vii. A method of converting data into a secure code to prevent unauthorized access.

**2. Examples**

Write a sentence using each of the terms from the previous exercise.

Ransomware: Ransomware locked the company's files, demanding payment for their release.(Bitcoin)

Phishing: Technique of sending messages to steal information from them

Identity Theft: Now with IAS, identity theft is booming

DDoS Attack: The website was taken offline by a massive DDoS attack.

Data Breach: A data breach exposed sensitive customer information to unauthorized parties.

Social Engineering: Social engineering tactics convinced an employee to disclose confidential information.

Malware: The computer was infected with malware after downloading a malicious file.

Encryption: Encryption ensured that the sensitive data remained secure during transmission.

**3. Fill in the Blanks**

Complete the sentences using the correct word from the list: (Cybersecurity, Encryption, Hackers, Data Breach, Passwords, Malware, Social Engineering, Online Fraud)

* Many companies invest in \_cybersecurity\_ to protect their networks from cyber threats.
* \_Encryption\_\_\_ is the process of converting data into a secure code to prevent unauthorized access.
* A \_Data\_Breach\_\_ occurs when sensitive information is exposed due to a security failure.
* Strong and unique \_\_passwords\_\_\_ help protect personal accounts from being hacked.
* \_\_Hackers\_\_ are individuals or groups that attempt to gain unauthorized access to systems.
* Many viruses and spyware fall under the category of \_\_malware\_\_\_.
* Some cybercriminals use \_social engineering\_\_\_\_ tactics to trick people into giving away sensitive information.
* Credit card scams and fake websites are examples of \_online\_fraud\_\_\_\_.

**4. True/False Statements**

Decide whether each statement is true or false. If false, correct the sentence.

* The WannaCry ransomware attack only affected a few hundred computers worldwide. F
* Phishing scams trick users into providing personal information by pretending to be trustworthy sources.T
* Yahoo’s data breach in 2013 was the biggest in history, compromising billions of accounts.T
* In the Twitter attack of 2020, hackers only targeted small business accounts.F
* The Colonial Pipeline attack led to major fuel shortages in the United States.T

**5. Comprehension Questions**

Answer the following questions in your own words:

* What was the WannaCry ransomware attack, and why was it so damaging?

It was an attack that affected organizations around the world to more than 200k computers in more than 150 countries

* Why was the Yahoo data breach considered one of the most serious cybersecurity incidents?

Because stole names, emails, phone numbers, birthdays and encrypted passwords from Yahoo's user database

* How did hackers exploit Twitter in 2020, and what was their goal?

He has gained access to twitter´s administrative tools so that they could alter the accounts themselves and post the tweets directly.

* Why do cybercriminals use ransomware, and how does it affect businesses?

Allows cyber criminals to infiltrate your systems and stop you from accessing your files or devices unless a ransom fee is paid.

* What are some ways people can protect themselves from cybercrimes?

Check the strength of your passwords.

Avoid these passwords.

Use a password manager.

Use multi-factor authentication.

Trust no one (on emails, phone or text)

Update your software