# Chapter 4: Cybersecurity & Digital Trust

## 1.Setting the Stage

### Activity 1: Digital Dilemma (Think & Decide)

You receive the following message:
*"Urgent: Your university account has been compromised. Click here immediately to secure it."*
Answer the questions:

1. What are the red flags in this message?
2. What would be your first reaction?
3. How would you verify its authenticity?

## 2.Take a Listen

### Activity 2:*Attack Identification Challenge*

What is Cybersecurity.mp4

Read each scenario below (based on the video). Choose the correct type of cyber attack from the list: *Phishing Attack, Malware Attack, Man-in-the-Middle Attack, Password Attack, SQL Injection Attack, DoS/DDoS Attack, APT (Advanced Persistent Threat).*

Write your answer next to each scenario.

**Scenarios:**

1. Anne received an email that appeared to be from ShoppingCart.com asking her to enter her account credentials to receive a discount voucher. She lost money from her account afterward.

2. Anne downloads an attachment from an unknown sender. Her system becomes corrupted by hidden viruses embedded in the file.

3. Anne uses an unsecured public Wi-Fi network. A hacker secretly intercepts the communication between her device and the shopping website, taking over her IP address.
4. A hacker tries to guess Anne's password by using common passwords and then attempting all possible alphabetical combinations.
5. A large corporation experiences a prolonged attack where hackers remain inside the network for months, continuously stealing confidential information.
6. A company's website becomes unresponsive because its network is flooded with so much traffic that legitimate users cannot access it.

## Activity 3: Match the Security Practice

Column A lists cybersecurity practices mentioned in the video.
Column B contains shuffled descriptions of what each practice does.
Match each practice in Column A to its correct description in Column B.

| Term (Practice) | Shuffled Descriptions (Match the correct letter to each term) | Answer Key |
|---|---|---|
| 1. Firewall | A. Detects and removes malicious software like viruses and trojans from your system. | |
| 2. Honeypot | B. Prevents phishing attacks by not engaging with suspicious or fraudulent messages. | |
| 3. Unique alphanumeric passwords | C. A virtual wall that filters incoming and outgoing traffic to safeguard your network. | |
| 4. Antivirus software | D. A dummy system designed to attract and deceive attackers, keeping the real system safe. | |
| 5. Avoiding emails from unknown senders | E. Hard to guess or crack because they combine letters, numbers, and symbols. | |

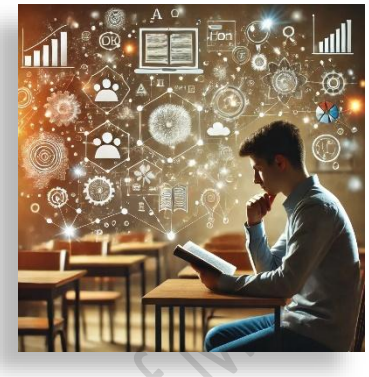
## Activity 4:Cybersecurity Quiz

Answer the following multiple-choice questions based on the video.
Circle or write the correct letter (A, B, C, or D) for each question.

**Questions:**

1. **What type of cyber attack did Anne experience?**
   A) Malware attack
   B) Man-in-the-middle attack
   C) Phishing attack
   D) Password attack
2. **Which attack involves a hacker taking over the client's IP address to intercept communication?**
   A) DDoS attack
   B) Man-in-the-middle attack
   C) Phishing attack
   D) Password attack
3. **What is a "honeypot" in cybersecurity?**
   A) A type of antivirus software
   B) A dummy system used to attract and deceive attackers
   C) A strong password containing letters and numbers
   D) A firewall that filters internet traffic
4. **Which type of attack uses multiple systems to flood a network with traffic?**
   A) SQL injection attack
   B) Malware attack
   C) APT (Advanced Persistent Threat)
   D) DDoS (Distributed Denial of Service) attack
5. **What does a firewall do?**
   A) It creates dummy systems to trap hackers
   B) It filters incoming and outgoing traffic to protect the network
   C) It guesses and cracks passwords
   D) It sends fraudulent emails to users
6. **Who is responsible for the overall safety of information in an organization?**
   A) Ethical hacker
   B) Security architect
   C) Chief Information Security Officer (CISO)
   D) Software developer

## 3. Read & Reflect



# What Educational Institutions Can Do to Protect Data

Educational institutions hold vast amounts of sensitive data, making them prime targets for cyber threats. Below are key actions schools, colleges, and universities can take to protect their data and build digital trust.

## 1. Invest in Cybersecurity

Just as physical security is essential, cybersecurity must be a priority. Investing in risk assessments, security frameworks (e.g., NIST), policies, and awareness programs helps minimize known and emerging threats.

## 2. Follow Cybersecurity Frameworks

Frameworks like **HECVAT** (designed for higher education) and **NIST CSF** provide guidelines to manage cloud security and build stronger IT programs, significantly reducing cyber risk.

## 3. Perform Risk Assessments

A thorough risk assessment identifies the most likely and damaging threats. It guides priorities, highlights key cybersecurity roles, and reminds everyone that data protection is a shared responsibility.

## 4. Provide Awareness and Training

Human error remains a major cause of data breaches. Ongoing training—starting from onboarding—helps staff identify phishing attempts, report unusual activity, and stay updated on evolving threats.

## 5. Develop a Cybersecurity Culture

Continuous training, leadership engagement, and regular discussion of cybersecurity in meetings create a culture where every employee becomes a line of defense against persistent attacks.

## 6. Standardize Cybersecurity Across Departments

A unified IT framework is easier to monitor and defend. Standardization enables better access management, consistent upgrades, and stronger protection across the institution.

## 7. Establish Clear Information Security Policies

Transparent, accessible policies ensure that all users—staff and students—follow consistent security practices, making it easier to identify and fix issues after an incident.

## 8. Implement Multi-Factor Authentication (MFA)

According to Microsoft, MFA can prevent nearly all data breaches. Requiring multiple forms of authentication significantly strengthens network security with minimal effort.

## 9. Enforce Strong Passwords

Strong passwords (8+ alphanumeric characters, symbols, no dictionary words) and unique credentials for each application reduce the risk of password-based breaches and credential reuse.

## 10. Use a Firewall and Monitor Continuously

Firewalls block harmful files and flag suspicious activity. However, continuous internal monitoring is also essential, as breaches often go undetected for over 200 days.

## 11. Manage Third-Party Risk

Vendors and partners can introduce vulnerabilities. Institutions must audit third-party vendors, understand their security posture, and address risks from software providers and cloud services.

## 12. Use Virtual Private Networks (VPNs)

VPNs protect privacy, prevent man-in-the-middle attacks, and help students avoid unsecured networks, keeping both users and institutional networks safer.

## 13. Encrypt Sensitive Data

Encryption ensures that lost or stolen devices do not lead to data exposure. All online transactions should use **Transport Layer Security (HTTPS)** with a padlock icon.

## 14. Maintain Regular Backups

Backups allow restoration of critical files (enrollment, exam results, research) after an incident. Regular testing and offsite cloud storage with vendor risk management are essential.

By implementing these measures, educational institutions can significantly reduce cyber risks, protect student and staff data, and foster a culture of digital trust.

## Activity 5: Data Protection Measures

Complete each sentence using the correct word or phrase from the text. The first letter of each answer is provided as a hint.

**1.** A u _____ IT framework is easier to monitor and defend than multiple separate systems.

**2.** Without clear information security p _____, it is difficult to identify what went wrong during a cyber incident.

**3.** A firewall m _____ everything attempting to enter or leave a network.

**4.** The text recommends using T _____ L_____ S_____ (HTTPS) for all online transactions, indicated by a closed padlock icon.

**5.** According to the text, c _____ culture results from continuous cybersecurity awareness training alongside other initiatives.

**6.** Third-party r _____ refers to the risk from software vendors and business partners that can impact the security of the educational institution.

**7.** E _____ ensures that lost or stolen devices do not lead to data exposure.

**8.** A strong password contains no words that you could find in a d _____.

**9.** The text states that an organization can improve its security posture most effectively when it fully understands that security p _____.

**10.** Ongoing training ensures that staff stay up to date with the cyber threat l _____.

## 4. Grammar in Action: Cleft Sentences for Emphasis and Focus


A cleft sentence is a grammatical structure that splits a simple sentence into two parts in order to highlight or focus on a specific element of information.

The team won the competition because of strong collaboration.

What is important in this sentence?
What made the team win the competition was strong collaboration.

**What-cleft:**
**What + clause + be + focus**
Example:
What we need is more practice.

**It-cleft:**
**It + be + focus + that/who**
Example:

It was the final round that decided the winner.

### Activity 6: Transform the sentence

Transform each sentence to emphasize a specific part using **cleft structures**.

1. **Base:** The audience enjoyed the debate.
2. **Base:** The team won because of strong preparation.
3. **Base:** The jury appreciated clarity and structure.
4. **Base:** The technical challenge tested communication skills.
5. **Base:** Students need more practice in speaking.
6. **Base:** The debate became interesting because of the arguments.

## 5. Speak & Debate


### Activity 7:

Answer the following question using:

Hedging: *It could be argued that…*
Emphasis: *What is important to consider is…*
Contrast: *However, on the other hand…*

*In today's digital world, can users truly trust online platforms, or is digital trust merely an illusion?*

## 6. Write with Might


Write a paragraph on how a single data breach can affect trust in digital platforms and change user behaviour.
Write one well-structured paragraph (120–180 words).
Begin with a clear topic sentence introducing the idea of data breaches and digital trust.
Explain how a data breach can affect users' trust in online platforms.

Describe at least two consequences on user behaviour (e.g., changing passwords, avoiding platforms, reducing online activity).