GROUP ACTIVITY:	01	DATE:	Insert date
SUBJECT:	**ITP1231 – Information Assurance and Security**		
GRO NO:	##		Engagement:
LN, FN MI	LN, FN MI		15%
LN, FN MI	LN, FN MI		05%
LN, FN MI	LN, FN MI		10%
LN, FN MI	LN, FN MI		70% / 100%

Activity: CYBERSECURITY UNDER ATTACK: A VIRTUAL ESCAPE ROOM

SCENARIO
The university's IT system has been hacked, and critical data is at risk! The students, acting as cybersecurity analysts, must identify security threats, recognize vulnerabilities, and implement security measures to stop the attack before the system crashes.
Setup:

- Divide students into groups of 4-5 members.
- Each team will work through a series of cybersecurity challenges related to threats, vulnerabilities, risk assessment, and security policies.

Challenge Structure:

💻 Stage 1. Password Crisis (Authentication & Access Control)

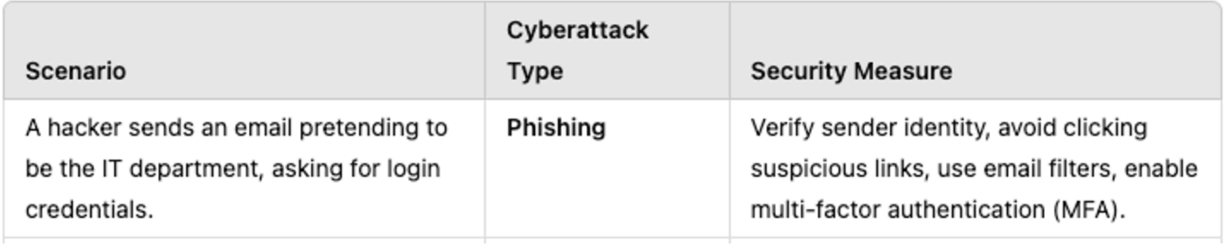
Clues / Guide:

- Students must *decrypt a scrambled password* to gain access to the system.
- They will be given *clues about weak passwords* and must figure out the *best security practice* for password creation.
- Students must *identify the original password* and *determine why it is still weak* despite its complexity.
- Then, they *create a more secure version* of the password following best practices.

🛑 Stage 2: Identify the Threat! (Types of Cyber Attacks)

Clues / Guide:

- Teams will *match real-life attack scenarios* (e.g., phishing, malware, spyware, Trojan horse, zero-day attach, denial-of-service, DNS spoofing etc.) with their definitions and possible security measures. *#there should be no overlapping of cases*
- Example: "A hacker sends an email pretending to be the IT department, asking for login credentials." (Answer: *Phishing*)
- Create a similar scenario as shown below:



Scenario	Cyberattack Type	Security Measure
A hacker sends an email pretending to be the IT department, asking for login credentials.	**Phishing**	Verify sender identity, avoid clicking suspicious links, use email filters, enable multi-factor authentication (MFA).

🔎 Stage 3: Spot the Vulnerability (Risk Assessment)

Clues / Guide:

- Teams will analyze *a case study of a company that suffered a cyberattack*.
- They must *identify vulnerabilities* and recommend *risk mitigation strategies.*

Case Study:

ABC Corporation, a mid-sized e-commerce company, suffered a **data breach** where customer payment details were stolen. An investigation revealed the following security flaws:

1. Outdated Software – The company's web application was running on *an old, unpatched version* with known security vulnerabilities.
2. Weak Password Policies – Employees were *reusing weak passwords* and *not using multi-factor authentication (MFA).*
3. Phishing Attack on HR Department – A *malicious email* tricked an HR employee into entering login credentials on a fake website.

4. No Network Segmentation – Hackers gained access to *all internal systems* once inside, as *critical data was not isolated.*
5. Lack of Security Monitoring – The IT team had *no real-time intrusion detection system (IDS)* to alert them of unauthorized access.

Complete the table below:

Vulnerability	**Risk**	**Recommendations Mitigation**
#choose 3 vulnerability case/s		

🔐 Stage 4: Secure the Network (Security Policy Implementation)

Clues / Guide:

- Each team must *draft a mini security policy* addressing *confidentiality, integrity, and availability (CIA triad).*
- The best security policy (judged by clarity, effectiveness, and completeness) **earns a bonus hint** for the final challenge.

Format:

Section 01: Purpose
Section 2: CIA Triad Implementation

Security Principle	**Policy Guidelines**	**Implementation Measures**
#clue: five pillars of IA model #pick only 3		#bulleted format (keep It short and simple) #KISS or straightforward

Section 03: Enforcement & Compliance

- Violations of this policy may result in disciplinary action, including access restrictions or termination.
- #add two more
- #add two more

#note: Use this document/file format, and use paper size: 8x13", font: Arial 10;