

SECURING ONLINE IDENTITIES

Authentication Best Practices in the Digital Age

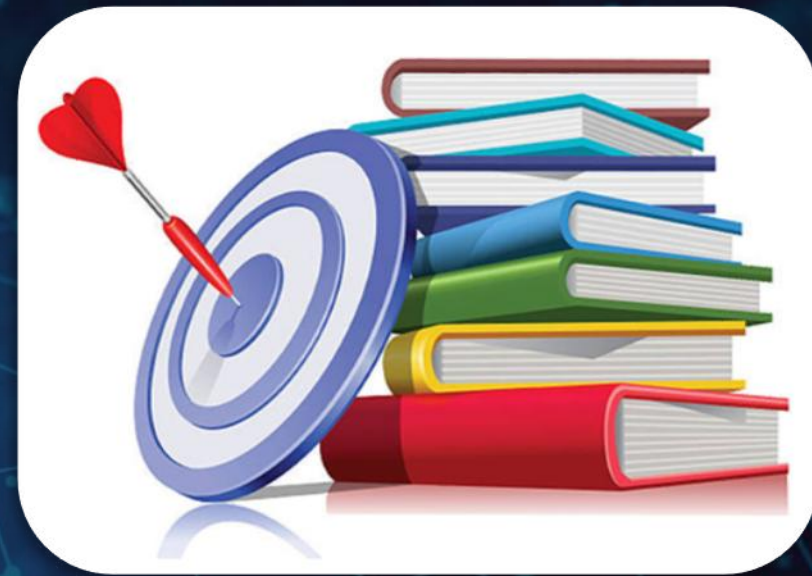


R. Ramanaruban
ramanaruban.r@sliit.lk



Intended Learning Outcomes (ILOs)

1. Identify common cyber threats and describe basic cyber hygiene principles.
2. Demonstrate the ability to recognize phishing emails and apply safe browsing practices.
3. Assess on personal online behavior and adopt better cybersecurity habits.



How Authentication Protects Against Identity Theft

**2 Factor Authentication
explained in 30 seconds.**

Understanding Cyber Threats

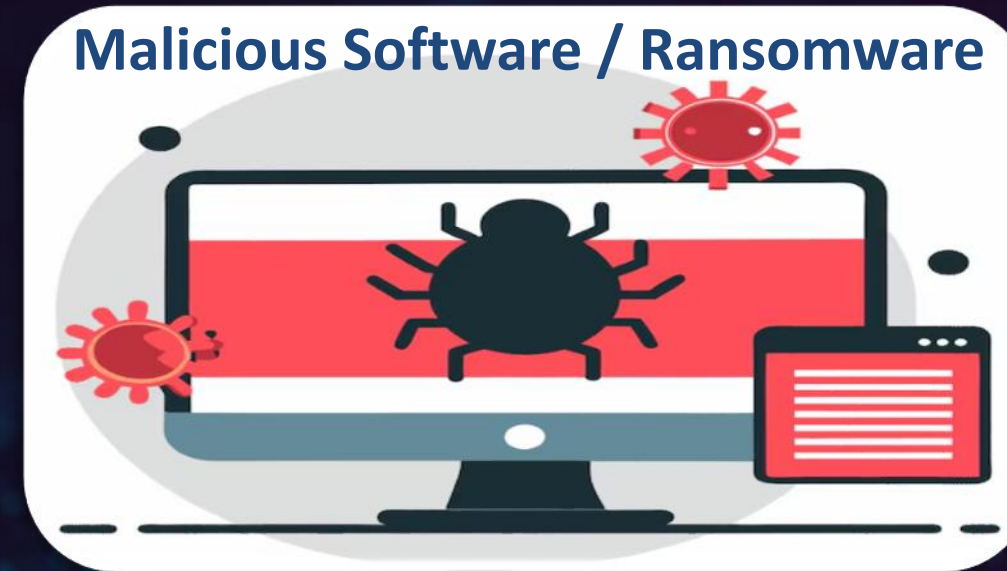
1 Phishing



3 Man-in-the-Middle (MITM)



2 Malware



4 Weak Passwords



Cyber Threats Mapped to Cyber Hygiene Practices

1 Phishing

Defenses:

- Be aware of urgent requests and strange links.
- Verify sender identities before clicking.



3 Man-in-the-Middle

Defenses:

- Avoid public Wi-Fi usage.
- Use a Virtual Private Network (VPN).



2 Malware

Defenses:

- Keep software and browsers updated.
- Install antivirus and enable firewalls.



4 Weak Passwords

Defenses:

- Use strong, unique passwords.
- Enable Two-Factor Authentication (2FA)



Group Work

Case Study 1: The Compromised Wi-Fi Cafe

Case Study 2: The “Free Gift Card” Email



Case Study 1: The Compromised Wi-Fi Cafe

Scenario: A group of students regularly visits a nearby cafe that offers free Wi-Fi. One day, one of the student logs into their email and notices strange activity-spam emails being sent from their account. Another student's social media account was also hacked after using the same Wi-Fi.

1. List 2 Cyber Threats associated with this scenario and suggest 2 cyber hygiene practices that could prevent them in the future?

Identified Cyber Threats	Cyber Hygiene Practices
1) Man-in-the-Middle (MITM)	Use a VPN when accessing public Wi-Fi to encrypt traffic.
2) Weak Passwords	Use strong, unique passwords and enable 2FA

Case Study 2: The “Free Gift Card” Email

Scenario: A student receives an email claiming they won a free \$100 gift card from a popular online store. The email has a link asking them to “verify their account.” Another student receives a similar message via social media with a shortened Uniform Resource Locator (URL).

1. List 2 Cyber Threats associated with this scenario and suggest 2 cyber hygiene practices that could prevent them in the future?

Identified Cyber Threats	Cyber Hygiene Practices
1) Phishing	▪ Verify sender’s email address before clicking links or sharing login information.
2) Malware	▪ Hover over links to preview the full URL and avoid shortened/unknown links.

Quick Knowledge Check



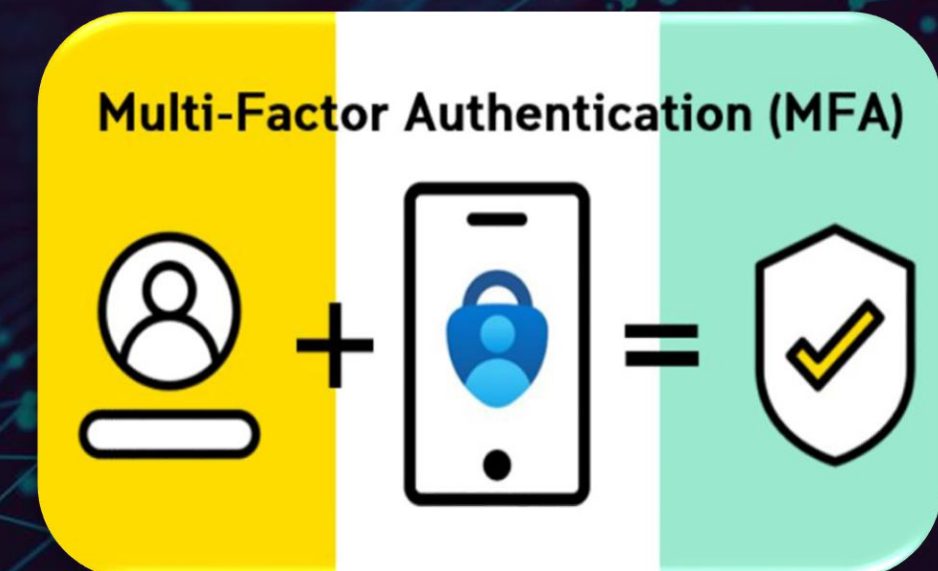
Recap – What We Learned Today

- Identified common cyber threats (Phishing, Malware & MITM).
- Understood real-life scenarios of fraudulent emails.
- Learned cyber hygiene practices to secure our online Identities.



Next Lecture

 Topic: Safe Use of Passwords & Multi-Factor Authentication (MFA)



THANK YOU!