



Cyber Awareness 🕒 1.3 hours of content

1. Introduction to Cybersecurity

- Understanding the Cyber World
- What is Cybersecurity?
- The importance of awareness and preparedness
- Overview of the course structure and objectives

2. Threat Landscape & Attacker Motivation

- High-Profile Cyber Attacks and Their Impact
- Why attackers target individuals and organizations
- Strategic importance of your digital assets
- Attacker Perspective:
- Motivations of Malicious Actors
- Common attack methods and goals

3. Password Security

- The Role of Passwords in Cyber Defense
- Importance of password diversity and uniqueness
- How attackers crack passwords (Live Demo)
- Best Practices for Password Storage
- Understanding Strong Passwords
- How to assess password strength
- Practical criteria for evaluating password resilience
- Changing and securing passwords
- Secure storage tools
- Q&A session

4. Data Breaches

- What is a Data Breach?
- Consequences of Exposed Information
- How to prevent data leakage

5. Social Engineering

- Introduction to Social Engineering
- What is phishing?
- Demonstration of malicious link manipulation
- Phishing Statistics and Real-World Cases
- Volume of attacks and victim demographics
- Prevention methods and user behavior
- Social Engineering in Organizations
- High-risk teams
- Detection and mitigation techniques
- Physical Social Engineering Simulation

6. Safe Browsing & Network Security

- Secure Internet Browsing
- Identifying safe and unsafe websites
- Recognizing threats in daily web activity
- Public Wi-Fi Risks and VPN Usage
- Why open networks are dangerous
- Role of VPN in safe browsing
- Account Protection Techniques
- Two-Factor Authentication (2FA)
- Extra tips for account security

7. Malware Awareness

- What is Malware?
- Common types (viruses, ransomware, spyware)
- How malware spreads and how to avoid it

8. Course Summary

- Recap of Key Concepts
- Building a Security-First Mindset
- Final Recommendations for Everyday Cyber Hygiene