

"Empower Your Team: Cybersecurity Training for Your Employees"

Course Outline

[Section 1: Welcome, Overview, and How to Use This Course](#)

By the end of this section, you will be familiar with the course structure, instructor, and the vital role of cybersecurity.

Introduction to the course, instructor, and cybersecurity

- A brief overview of course content
- Learning objectives and alignment with goals
- Guidelines for navigating and engaging with the course

[Section 2: Cybersecurity Fundamentals](#)

You will understand the fundamentals of cybersecurity and be aware of common threats upon completion of this section.

- Definition and importance of cybersecurity
- Common misconceptions
- Security awareness and common threats

[Section 3: Protecting Personal and Company Information](#)

At the end of this section, you will learn how to protect personal and corporate information across various platforms.

- Device protection: passwords
- Device protection: Downloads
- Device protection: Screen lock
- Device protection: Outdated software
- Device protection: Backup and restoration
- Mobile device security: updates, biometric authentication
- Social media and web browsing safety guidelines

[Section 4: Email Security - A Gateway for Attacks](#)

Upon completing this section, you will be able to recognize email vulnerabilities and implement effective protective measures.

- Understanding email vulnerabilities

- Spotting and avoiding phishing scams and malicious attachments
- Implementing email security measures

Section 5: Advanced Security Measures

After this section, you will be proficient in advanced security measures, including Two-Factor Authentication, firewalls, and anti-viruses.

- Two-Factor Authentication (2FA): Introduction and best practices
- Firewalls and Anti-Viruses: Types, functions, and maintenance

Section 6: Social Engineering and Scam Awareness

By the end of this section, you will know how to identify and defend against social engineering tactics and various scams.

- Social engineering: Types, techniques, countermeasures
- Awareness of scams and malicious content
- Protecting against phishing, strong passwords, public Wi-Fi

Section 7: Cybersecurity Policies and Incident Reporting

Upon completion of this section, you will understand company cybersecurity policies and the process for reporting security incidents.

- Cybersecurity company policy
- Incident reporting: Reasons, best practices, forms

Section 8: Conclusion and Q&A

At the end of this section, you will be able to consolidate your learning, reflect on key takeaways, and raise any remaining questions.

- Recap of key takeaways
- Opportunity for questions and clarification

Bonus and Resources

- Sample forms
- PowerPoint/Slides
- NIST Framework
- Examples and Case Study