CYBERSECURITY AWARENESS AND BEST PRACTICES

CABP-YN

Duration: 1 day; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

This one-day course provides a comprehensive introduction to cybersecurity for employees, focusing on awareness and best practices. Participants will learn about common cyber threats, such as phishing, social engineering, and ransomware, through real-world examples and interactive activities. The course emphasizes the importance of employee vigilance and provides actionable strategies for protecting personal and organizational data. By the end of the day, participants will be equipped with the knowledge and skills to identify and respond to cyber threats effectively.

COURSE OBJECTIVES

By the end of this course, participants will:

- Understand the importance of cybersecurity in the workplace and daily life.
- Recognize common cyber threats and attack vectors.
- Learn best practices for protecting personal and organizational data.
- Develop skills to identify phishing attempts, social engineering, and other malicious activities.
- Gain awareness of current cybersecurity trends and real-world attack examples.
- Understand the role of employees in maintaining a secure organizational environment

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentations, discussions, and practical exercises.

COURSE CONTENTS

Module 1: Introduction to Cybersecurity

Topics Covered:

- What is cybersecurity and why is it important?
- The evolving threat landscape: Why employees are the first line of defense.
- Key cybersecurity terms and concepts (e.g., malware, ransomware, phishing).

Activity:

- Interactive discussion: “What would you do?” (Participants share their experiences with cyber threats).

Module 2: Common Cyber Threats and Attack Vectors

Topics Covered:

- Phishing attacks: How they work and how to spot them.
- Social engineering: Manipulation techniques used by attackers.
- Malware and ransomware: Examples and impact.
- Password attacks and credential theft.
- Real-World Examples:

Case study: The 2021 Colonial Pipeline ransomware attack.

- Example: Phishing emails mimicking trusted organizations (e.g., banks, HR departments).

Activity:

- Phishing email simulation: Participants identify red flags in a sample email.

Module 3: Cybersecurity Best Practices

Topics Covered:

- Strong password creation and management.
- Multi-factor authentication (MFA) and its importance.
- Safe browsing habits and avoiding malicious websites.
- Securing devices (e.g., laptops, smartphones) and software updates.
- Data protection: Encryption and secure file sharing.

Activity:

- Hands-on exercise: Creating strong passwords and enabling MFA on a sample platform.

Module 4: Current Cybersecurity Trends and Real-World Attacks

Topics Covered:

- Overview of recent cyberattacks (e.g., supply chain attacks, zero-day exploits).
- The rise of AI-powered attacks and deepfake technology.

GemRain Consulting Sdn Bhd.
69-2, Block D, Jaya One, Jalan Profesor Diraja Ungku Aziz, 46200 Petaling Jaya, Selangor, Malaysia
Contact: (+60)3 7931 3036 | (+60)12 613 3667 | Email: enquiry@gemrain.net | Website: www.gemrain.net

- Insider threats and accidental data leaks.
- Real-World Examples:
- SolarWinds supply chain attack (2020).
- Deepfake audio used in CEO fraud cases.

Activity:
- Group discussion: How would you respond to a suspected insider threat?

Module 5: Role of Employees in Cybersecurity

Topics Covered:
- The human factor: Why employees are critical to cybersecurity.
- Reporting incidents: What to do if you suspect a breach or attack.
- Building a culture of security awareness in the workplace.

Activity:
- Scenario-based role-playing: Reporting a phishing attempt to the IT team.

Module 6: Recap, Q&A, and Next Steps

Topics Covered:
- Recap of key takeaways.
- Open Q&A session for participants.
- Resources for further learning (e.g., cybersecurity blogs, tools, and training).

Activity:
- Quick quiz: Test your knowledge on cybersecurity essentials