cyberskills

CYBERSECURITY AWARENESS TRAINING FOR THE FINANCIAL SERVICES SECTOR

Duration: 7 hours (Theory: 5 hours Practical: 2 hours)

Level: Intermediate

Delivery method: In-person (Preferred) or Online

Target Audience: Employees working in the financial services sector who make increasing use of information technology to carry out their day-to-day tasks.

Prerequisites: None

ABOUT THIS COURSE

Undoubtedly, during the past years, the financial services sector has undergone massive digital transformation resulting in new and innovative financial offerings but at the same time increasing financial organizations' dependence on the use of technology. Moreover, the attack surface of financial companies is growing at an unprecedented rate. The financial services sector is now, one of the most targeted industries by cybercriminals due to the nature and sensitivity of the transactions and the huge amount of personally identifiable information they deal with on a regular basis. According to CSOonline, the average cost of a data breach tops USD 5 million within the financial services sector, surpassing the average cost of USD 3.86 million across all industries. This one full-day cybersecurity awareness training workshop has been tailored for employees working in the financial services sector and covers many aspects of how employees, with an increased cybersecurity awareness, can help to strengthen the cybersecurity posture of their organizations.

Part 1: The new financial cybersecurity landscape

- Why the Financial services sector is one of the most targeted industries?
- Threat actors affecting the financial services sector.
- Sophisticated financial malware
- The evolving cybercrime landscape affecting PII.
- Advanced social engineering techniques

Part 2: The impact of data breaches in the financial services sector

- The biggest financial data breaches and related implications
- Laws, regulations, and financial obligations of organizations operating in the financial services sector.
- An anticipatory approach to deal with financial cyber risks

Part 3: Sophisticated ransomware attacks targeting the financial services sector.

- The evolution of ransomware
- Ransomware with exfiltration techniques
- Ransomware infection vectors: Internet-facing vulnerabilities and misconfigurations, phishing, Precursor malware infection

Part 4: Malware types

- Understand the different types of malicious software.
- The latest trends in cyber attacks
- Preferred vectors of cyber attacks

Part 5: Email phishing attacks

- Social engineering techniques targeting financial institutions.
- Email as a preferred vector of attack
- Types of phishing attacks – Email phishing, Spear phishing, Whaling, Smishing, Vishing
- Techniques to identify sophisticated phishing emails.
- Business email compromise

Part 6: Passwords

- Understanding password complexity vs password length
- Passphrase vs Passwords
- Create secure authentication and know when your password is compromised.

Part 7: 10 ways to protect your organization and its data.

- Multi-factor authentication - Creating secure authentication using 2FA, 2SV, or MFA.
- Software patching
- Identifying sophisticated attacks using fake URLs
- Detect potentially infected attachments.
- Securing your data over public networks
- Securing mobile devices
- Protecting privacy online
- Learn how encryption can protect your data.
- Protect your online privacy.
- Protect from ransomware and other sophisticated attacks.

Part 8: The anatomy of a cyberattack resulting in a financial data breach

- Learn about the different phases involved in a cyber-attack.
- The reconnaissance phase – passive and active reconnaissance.
- Weaponization and delivery of infected payloads
- Exploitation and Installation of payload phase
- Data exfiltration and action on objectives

Part 9: Cybersecurity requirements from a legal and regulatory standpoint

- Protecting Confidentiality, Integrity, and Availability of data
- Cybersecurity requirements in GDPR
- Mapping cybersecurity requirements to information security program
- A risk-based approach to cybersecurity

Part 10: Quiz

- Multiple choice questions on all the topics of the training