MERCURY

Comprehensive Cybersecurity Awareness and Phishing Prevention Training

22 – 26 December 2026
Dubai (UAE)

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Comprehensive Cybersecurity Awareness and Phishing Prevention Training

Ref: 15671_1001115 **Date:** 22 – 26 December 2026 **Location:** Dubai (UAE) **Fees:** 4900 Euro

Introduction:

In today's digital era, cybersecurity threats are becoming more complex, frequent, and targeted. Organizations face increasing risks from phishing, malware, data breaches, and social engineering attacks. This Cybersecurity Awareness and Phishing Prevention course empowers professionals to defend against these threats through practical awareness and secure behavior.

This Cybersecurity Awareness and Phishing Prevention training course offers comprehensive insights into securely handling emails, mobile devices, social media, and browsing activities. It emphasizes phishing testing and campaigns to simulate real-world attack scenarios.

Participants will develop practical skills to assess risks and adopt preventative measures proactively. This Cybersecurity Awareness and Phishing Prevention program is essential for safeguarding personal, professional, and organizational data in today's evolving cyber threat landscape.

Targeted Groups:

This Comprehensive Cybersecurity Awareness and Phishing Prevention training targets professionals seeking specialized knowledge and skills:

- IT professionals working in cybersecurity and system administration.
- Employees handling sensitive information or client data.
- Human resource managers are responsible for employee onboarding.
- Finance and procurement officers process digital transactions.
- Public sector employees have access to internal portals.
- Executives and senior management targeted cyberattacks.
- Marketing and communications staff are using email campaigns and social platforms.
- Health sector professionals manage patient or medical records.
- Educational staff handling student databases and systems.
- Remote workers and hybrid teams accessing company systems from off-site.

Targeted Competencies:

Participants will gain the following competencies during the Cybersecurity Awareness and Phishing Prevention program:

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Skillfully identify phishing and fraudulent communications.
- Apply best practices in mobile and media device security.
- Use secure methods when accessing or sharing information online.
- Communicate cybersecurity risks clearly to non-technical audiences.
- Interpret social engineering cues in digital environments.
- Lead basic phishing awareness workshops for internal teams.
- Conduct and analyze simulated phishing assessments.
- Design risk-aware guidelines for safe email and social media use.
- Align cybersecurity behavior with organizational policies and frameworks.

Course Objectives:

Participants will achieve the following objectives by completing the Comprehensive Cybersecurity Awareness and Phishing Prevention course:

- Recognize and analyze different types of phishing emails and digital scams.
- Apply secure practices when using corporate and personal email platforms.
- Identify security risks associated with mobile device use and mitigate vulnerabilities.
- Demonstrate the ability to secure removable storage and portable drives.
- Develop a risk-aware mindset while browsing and interacting with web content.
- Evaluate web links, attachments, and downloads for authenticity and safety.
- Implement responsible behaviors while using social media on behalf of organizations.
- Detect red flags and anomalies in online interactions and messages.
- Engage in simulated phishing exercises and assess their responses.
- Design and roll out phishing campaigns to assess organizational preparedness.
- Recommend corrective actions based on phishing campaign results.
- Communicate cyber threats and response strategies within teams effectively.
- Monitor and report suspicious activities following incident response protocols.
- Build a security-first culture in the workplace through awareness and example.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Course Content:

Unit 1: Secure Handling of Email Services, Especially Phishing Emails:

- Understand the anatomy of a phishing email.
- Identify suspicious sender addresses, links, and attachments.
- Learn the psychological tactics used in phishing urgency, fear, authority.
- Avoid clicking or downloading from unknown email sources.
- Understand spear-phishing and its impact on high-profile targets.
- Use multi-factor authentication MFA for email access.
- Safely report phishing attempts using internal IT protocols.
- Evaluate email security using built-in client features e.g., spam filters, headers.
- Implement organization-level controls to mitigate email-based threats.

Unit 2: Secure Handling of Mobile Devices and Storage Media:

- Recognize threats related to lost or stolen devices.
- Enable screen locks, biometric authentication, and encryption.
- Disable auto-connect features for Wi-Fi and Bluetooth.
- Avoid installing apps from untrusted or unknown sources.
- Understand the risks of using public charging stations juice jacking.
- Safely store and transport USB drives and external hard disks.
- Detect signs of device compromise, including abnormal behavior.
- Ensure regular updates for mobile OS and apps.
- Review mobile management tools for organizational use.

Unit 3: Secure Internet Browsing:

- Use secure, HTTPS-encrypted websites only.
- Understand browser vulnerabilities and keep browsers updated.
- Avoid using saved passwords on shared or public computers.
- Configure privacy settings to limit data collection.
- Recognize fake websites and URL spoofing techniques.
- Prevent downloading malicious plugins or extensions.
- Clear cache and cookies regularly for secure sessions.
- Use trusted search engines to avoid clickbait or drive-by attacks.
- Utilize VPNs for enhanced browsing security when remote.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Unit 4: Secure Use of Social Media:

- Recognize social media phishing angler phishing, fake profiles.
- Avoid oversharing personal or corporate information online.
- Implement two-step verification for social platforms.
- Review privacy settings to control content visibility.
- Monitor brand impersonation and identity theft on platforms.
- Be cautious when sending direct messages from unknown contacts.
- Understand the impact of posts on corporate reputation and security.
- Report malicious or suspicious activities to the platform administrators.
- Educate peers about social media etiquette and safety.

Unit 5: Phishing Testing:

- Understand phishing simulations and their purpose.
- Participate in real-time testing with realistic scenarios.
- Analyze test outcomes and identify response patterns.
- Discuss errors and missed indicators during simulations.
- Improve detection through iterative feedback and learning.
- Use dashboards to track awareness progress over time.
- Encourage healthy competition to foster vigilance.
- Tailor tests based on department-specific risks.

Unit 6: Phishing Testing Campaign for All Users:

- Plan and schedule phishing testing campaigns organization-wide.
- Segment users based on risk exposure and departments.
- Develop campaign templates with varied difficulty levels.
- Communicate the campaign purpose to stakeholders and managers.
- Automate email delivery and result tracking.
- Evaluate user behavior metrics and click rates.
- Provide personalized training follow-ups to high-risk individuals.
- Use insights to refine cybersecurity strategies and policies.
- Promote continuous improvement through periodic campaigns.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Final Insights & Key Takeaways:

This Cybersecurity Awareness and Phishing Prevention training empowers professionals with practical skills to guard against digital threats. Participants leave with improved awareness, analytical capability, and response readiness. A culture of cyber vigilance begins with informed, trained individuals. Phishing resilience starts with people, not just technology.