Cyber-Security Awareness Training
(A 3-day Instructor led Program)

Table of Contents

Training Summary

Global Solution Partners LLC is pleased to deliver a comprehensive 3-Day Cyber Security Awareness Training for your organization.

This three-day **Cyber-Security Awareness** course is designed for employees of organizations who have varying levels of technical expertise. Its primary objectives are to:

- **Increase awareness of current cyber threats** and how attacks exploit human and technical vulnerabilities.
- Explain **cyber-security regulations** and why training and compliance are mandatory for organizations.
- Teach **best practices for password management, email and social-media safety, safe browsing, and data protection**, including role-specific advice for non-technical staff and IT personnel.
- Equip employees to recognize and respond to **social-engineering and phishing attacks**, using hands-on simulations and serious-game elements
- Develop **incident response skills** and promote cyber hygiene through regular updates, backups, encryption and awareness of remote-work risks

Explore **emerging threats** (ransomware, IoT risks) and encourage a culture of continuous learning and security resilience

Course Objectives and Learning Outcomes

By the end of this training program, participants will be able to:

1. **Describe the cyber-threat landscape** and common attack vectors.
2. **Summarize Omani cyber-security laws and regulations** (Information Technology Law, Cyber Crime Law) and explain why ongoing training is mandatory for compliance
3. **Apply best practices** for password management, email and social-media safety, safe browsing and data protection.
4. **Detect and respond to phishing and social-engineering attacks** through simulations and reporting procedures
5. **Demonstrate incident response skills** and understand organizational reporting lines.
6. **Implement cyber hygiene measures** such as regular updates, backups, encryption and secure remote-work practices
7. **Identify emerging threats** (e.g., ransomware, IoT vulnerabilities) and commit to continuous learning.
8. **Achieve Certification:** Pass the final assessment program on proficiency of the concepts learned

Day-Wise Curriculum

Day	Focus Area	Topics & Activities	Learning Outcomes
Day 1	**Foundations of Cyber-Security & Regulations**	• Welcome & Orientation – Pre-course gamified poll • Introduction to Cyber-Security & Threat Landscape – interactive video & quiz • Omani Cyber-Security Laws & Responsibilities – case study & group discussion • Password Management & Authentication – hands-on tool demo • Email & Social-Media Safety – simulated inbox & quiz • Workshop: Recognizing Attack Vectors – group analysis of scenarios • Safe Browsing & Data Protection – live demo & Q&A • Gamified Quiz & Reflection	• Understand fundamental concepts of cyber-security and common attack vectors. • Explain Omani cyber laws and compliance requirements. • Apply strong password and authentication practices. • Identify and avoid unsafe email/social-media behaviours. • Adopt safe browsing and data protection habits.
Day 2	**Social Engineering, Phishing & Data Protection**	• Recap & Warm-up Quiz • Social Engineering & Psychology of Attackers – role-play exercises • Phishing Awareness & Simulation Lab – live phishing test	• Recognize psychological manipulation and social-engineering tactics. • Detect and report phishing through real simulations • Apply secure communication and data-handling practices

		• Hands-on Workshop: Secure Communication & Data Protection – encrypt, classify, and share data safely • Incident Response Fundamentals – role-played breach scenario • Workshop: Social-Media & Mobile-Device Security – case analysis • Gamified Quiz “Escape the Phish” + Reflection & Action Plan	• Demonstrate correct steps in incident response and reporting • Develop guidelines for social-media and mobile-device security • Reinforce phishing detection through gamified learning.
Day 3	**Cyber Hygiene, Emerging Threats & Certification**	• Recap & Energiser Poll • Cyber Hygiene & Resilience – lecture and checklist exercise • Emerging Threats & Future Trends – ransomware, IoT, AI risks • Hands-on Lab: Secure Configuration & Resilience Planning – firewall, backup, restore simulation • Group Project: Develop Cyber-Awareness Campaign – posters, slogans, emails • Comprehensive Review & Q&A – collaborative mind-map • Final Certification Exam & Certificate Awarding	• Implement daily cyber-hygiene practices (updates, backups, encryption). • Identify emerging cyber threats and mitigation measures. • Configure basic security and resilience settings. • Design and present an internal awareness campaign aligned with Omani culture. • Consolidate and demonstrate course knowledge via certification exam.

Training Methodology and Format

Our program maximizes engagement and retention by blending expert instruction with hands-on, interactive learning tailored to client's operations.

- ✓ **Instructor-Led Presentations:** Experienced trainers deliver clear, interactive lectures using slides, real-world examples, and analogies to demystify complex topics.
- ✓ **Small-group workshops and case studies:** Research shows small-group workshops enhance cyber-awareness and encourage peer learning
- ✓ **Group Discussions & Q&A:** Open dialogue is encouraged participants share experiences and collaborate on solutions, making lessons directly relevant to their work environment.
- ✓ **Phishing simulations:** Targeted simulations allow employees to experience attacks safely, reducing susceptibility and encouraging correct reporting
- ✓ **Frequent knowledge checks and polls:** Regular quizzes maintain attention and allow facilitators to adjust pacing based on learner comprehension.
- ✓ **Assessment program:** The course concludes with a supervised exam (Day 3) to validate comprehension and readiness. Passing earns an appreciation certificate.
- ✓ **Comprehensive Materials:** Participants receive up-to-date printouts, handouts, and reference materials aligned with global standards, for use during and after training.

This blended, practical approach ensures attendees gain not only knowledge but also the confidence and skills to apply best practices in team's daily operations.

Deliverables

- ✓ **Three Days of Expert Instruction:** On-site, 3-day training led by a certified instructor, fitting to client’s schedule (about 7 hours/day, including breaks) for minimal operational impact.
- ✓ **Course Materials:** Comprehensive printed materials for each participant—presentation slides, module notes, reference standards (as allowed), worksheets, and case study handouts—all for future use.
- ✓ **Hands-On and Interactive Exercises:** In-class demonstrations with tools/props
- ✓ **Assessment Certificate:** Based on your participation and performance we shall present a certificate to all individuals
- ✓ **Post-Training Support:** 30 days of email/phone support for questions and clarifications, helping apply knowledge to real-world operations.