

Security Awareness Parts I and II

Why is Security Awareness Needed?

Security awareness training is a critical part of standard operating policy and procedures for businesses and schools of all sizes. Did you know the majority of security breaches involve internal employees, with some estimates as high as 85 percent according to Forrester Research? Nearly every company or school today, large or small, deploys computer systems, applications, and networks to enable their business. Physical, Technical and Administrative Security controls are put in place to manage threats to facilities, systems and information to ensure an acceptable level of confidentiality, integrity, and availability (CIA); yet documented evidence continues to show breaches in security due to lack of awareness. Employees, staff, administrators, contractors, consultants, temporaries, and other workers must understand how to protect the confidentiality, integrity, and availability of your information systems.



Training Program Description

Security is every employee's responsibility. The latest technological improvements like firewalls, intrusion detection systems, and other security devices, are completely useless if an untrained staff member endangers sensitive company or client information.

Spohn's Security Awareness Training program provides all levels of your staff with a better understanding of security risks, critical issues and the importance of security in your daily operations. This training program highlights risks and threats and provides required actions to help reduce loss.

Courses, Lengths & Recommendations

Security Awareness Part I – The Basics

- 2-hrs. - Recommended for Everyone

Security Awareness Part II – Acceptable Use Behaviors (Customer Specific)

- 2-hrs. - Recommended for Everyone

Delivery Options

Instructor-Led Live – We come to You

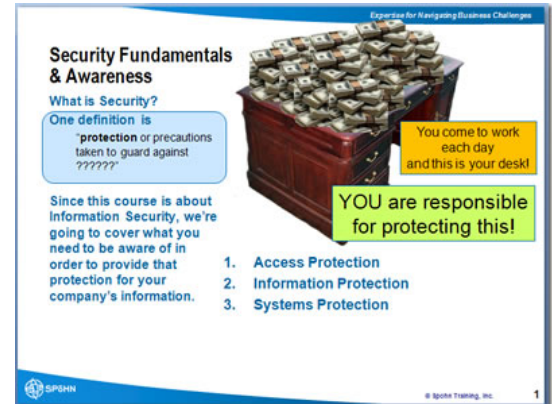
Instructor-Led Web Based – You join a Webinar

Training Program Content

Security Awareness Part I – The Basics

During this course we provide you with the overall purpose of security. We review and discuss examples of critical items your company considers as confidential or proprietary information. We provide best practices and examples for protecting 3 critical areas of concern which you are responsible for, including:

1. Access Protection
 - o Protecting User IDs and Passwords
 - o Password Creation/Maintenance Best Practices
 - o Locking your computer when unattended
2. Information Protection
 - o Guarding work materials and view of computer screen when working in public
 - o Sharing computer disks that contain confidential information
 - o Encrypting sensitive or confidential emails
 - o Securing hardcopies - Locking sensitive and confidential information when unattended
 - o Picking up confidential and proprietary items quickly off the printer, both in the office and at any client site
 - o Preventing damage caused by unauthorized access
 - o Social Engineering – what to look out for
3. Systems Protection
 - o We'll show you how to keep your application software and virus definitions current and regularly scan your hard drives for viruses
 - o We'll explain why using a personal firewall device in active mode at all times is critical
 - o We'll go into detail on email etiquette, email do's and don'ts as well as web browsing do's and don'ts
 - o We'll review why it's important to keep any laptops or other electronic devices containing Company data under your control at all times
 - o And, we have recommendations for what to do in case you have a Security Incident



Security Awareness Part II – Acceptable Use Behaviors

Spohn's Security Awareness Training Part II is customized to your policies, procedures and acceptable use behaviors with the following general course topics.

- After completing this course you will learn acceptable use behaviors required by your Company including:
 - o Why This is Important
 - o General Use and Ownership
 - o Security and Proprietary Information
 - o Unacceptable Use
 - o Your Responsibilities
 - o Security Tools
 - o Handling Security Incidents
 - o Acceptable Use of Company Resources
 - o Using Instant Messaging Resources
 - o Backup Responsibilities
 - o Copyright and Intellectual Property Regulations When Installing Non-Standard Software

