

Security Awareness

(Part 1 – The Basics – Part 2 – Acceptable Use Behaviors)



COURSE FEATURES

SECURITY AWARENESS PART 1

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

- **Access Protection**
Protecting User IDs and Passwords
Password Creation/Maintenance
Locking your computer
- **Information Protection**
Guarding work materials
Sharing computer disks
Encrypting emails
Securing hardcopies
Picking up items from the printer
Preventing unauthorized access
Social Engineering
- **Systems Protection**
Keeping your application software and virus definitions current
Using a personal firewall device in active mode
email etiquette
Keeping electronic devices under your control
Recommendations for what to do in case you have a Security Incident

SECURITY AWARENESS PART 2

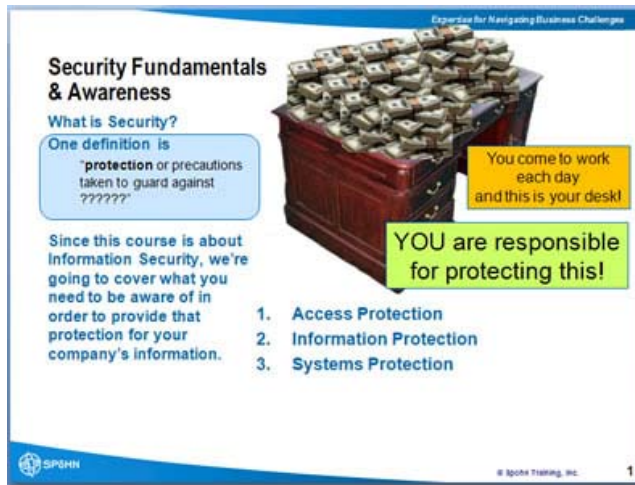
Spohn's Security Awareness Training Part II is customized to your policies, procedures and acceptable use behaviors with the following general course topics.

- Why Security is Important
- General Use and Ownership
- Security and Proprietary Information
- Unacceptable Use
- Your Responsibilities
- Security Tools
- Handling Security Incidents
- Acceptable Use of Company Resources
- Using Instant Messaging Resources
- Backup Responsibilities
- Copyright and Intellectual Property Regulations When Installing Non-Standard Software

For more information on any of our products or services please call or visit us on the Web.

Spohn & Associates, Inc.
8940 Research Blvd.
Suite 300
Austin, TX 78758
Phone: (512) 685-1000
Toll Free: (800) 687-0464
FAX: (512) 685-1800
<http://www.spohncentral.com>
<http://www.spohntraining.com>

Security Awareness Training Course Part 1 & 2



COURSE BENEFITS

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.

Course Options

- 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

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.

