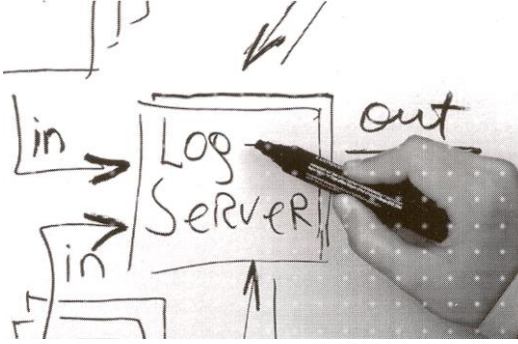
# Security Awareness Seminars

## Training Content for Enterprise Employees




## Summary

Giving out sensitive data to people without first authenticating their identity and access privileges, is one of the most common and worst mistakes employees can make. Allowing a stranger inside an organization without authorization is yet another example of a broken link in the human firewall chain. Social engineering is evolving so rapidly that technology solutions, security policies, and operational procedures alone cannot protect critical resources. Even with these safeguards, hackers commonly manipulate employees into compromising corporate security. Victims might unknowingly reveal the sensitive information needed to bypass network security, or even unlock workplace doors for strangers without identification. While attacks on human judgment are immune to even the best network defense systems, companies can mitigate the risk of social engineering with an active security culture that evolves as the threat landscape changes.

Our Security Awareness Seminars seek to assist organizations in mitigating the risks from Human based attacks, which are capable of circumventing a wide range of deployed controls by publishing the culture of "defending people by people." Our seminars educate the new concept of the "Human being firewall," how it could be applied to maintain a good security posture, and finally providing practical guidance on responding to incidents effectively and efficiently. Our structured awareness training should be considered in every organization that needs to maintain a good security posture.

**Duration: 4 hours**

**Prerequisites**
None

**Who should attend?**
Employees that need to follow organization specific policies for proper handling of business information and acceptable usage of information systems.

**Learning Objectives**
By the end of this seminar, employees will demonstrate basic knowledge of information security, security awareness best practices and the importance of information security in accordance with enterprise-level compliance requirements.

*"Amateurs hack systems, professionals hack people."*
Bruce Schneier

## Course Agenda

Modules in the awareness program include but are not limited to:

- Common Social Engineering Attacks
- Addressing Physical Security Threats
- Personal Computing Security
- E-mail Communications Threats and Countermeasures
- Best Practices for Password Usage
- Online Web Browsing Threats and Countermeasures
- Mobile Devices Threats and Countermeasures
- Common e-Banking Threats and Countermeasures

besecure
Managed E-Business Security™

ENTERPRISE SECURITY TOP 10 CYBER SECURITY
Consulting/Services Companies in Europe - 2018

## Learning Objectives

- Describe social engineering and identify common threats to information security and how to avoid becoming a victim.
- Describe physical security, identify common threats and list best practices.
- Describe PC security, identify common threats and list best practices.
- Describe email security, identify common threats and list best practices.
- Describe password security, identify common threats and list best practices.
- Define Web browsing security, identify common threats and list best practices.
- Define mobile device security, identify common threats and list best practices.
- Recognize the risks and threats that come with electronic banking, as well as the technology and security best practices available to help combat such threats.

## Security Awareness Platform

All organizations need to educate their employees about cyber security risks. That's why we have developed a fully functional Learning Management System to manage content and ongoing education. Our LMS was developed to reinforce the behavioral conditioning and experiential learning with the ability to expand training in areas of security and compliance important to your company. Detailed reports ensure that you always know how the awareness program is progressing.

## Competency Assessment Reports

At the end of seminar, employees are requested to fill in relevant security awareness tests that can be in the form of multiple choice questions, scenario specific questions or game-like tests like quizzes and crosswords. Results are recorded in executive reports that demonstrate the level of knowledge that has been acquired, and any likely gaps in specific training domains.

## About BESECURE

BESECURE, a leader in Governance Risk and Compliance solutions and services, provides Compliance Services based on legal and regulatory requirements, designs and implements advanced IT security solutions, delivers information Security Training Seminars, provides Managed Security services, performs Penetration Tests and Vulnerability Assessments covering all phases of the life cycle of information security. BESECURE applies a certified Quality Management System according to ISO 9001:2008 and a certified Information Security Management System according to ISO 27001. For more information, please visit http://www.besecuregroup.com

**www.besecuregroup.com**

**Greece, Southeast Europe**
19, Syngrou Ave., 117 43,
Athens, Greece
Tel. +30 210 330 7 440, Fax +30 210 330 7 441

**Cyprus, Middle East**
133B Fraglin Roosevelt Ave, 3011,
Limassol,Cyprus
Tel. +357 250 29 300, Fax +357 250 29 301

**Belgium, Western Europe**
Place Rouppe 27,
1000, Brussels, Belgium
Tel. +32 25 88 4470, Fax +32 25 88 4471