

Who's watching your back?

Foundstone[®]
Professional Services A DIVISION OF McAfee

Training Datasheet

Security Awareness Program Development & Training

Raising Information Security Awareness

DURATION

- One (1) Hour (Computer Based Training)

WHAT YOU'LL LEARN

- Understand the threats to your organization from the outside, as well as the inside
- Learn what motivates attackers and their goals
- Develop the mindset of a security conscious employee who is on the front lines of protecting your corporate assets
- Learn common attacks and the common sense defenses that all employees can use

SUGGESTED NEXT STEP(S)

- Role specific security awareness training for instance Unix or NT specifics or further advanced certifications such as CISSP and CEH

Employees are your first line of defense. They are the eyes and ears of the organization. They have access to your data and systems. They know how to distinguish between normal patterns and unusual activity. No one is better suited to protect your area of concern. We can't just rely on technology to solve all our security problems because we ultimately rely on people to install, manage and use that technology. The first step in the evolution of security in the enterprise is providing your employees with the awareness and tools they need to identify and thwart an attack.

Organizations must realize that security awareness is an ongoing process, not a one-time event. If your organization does not have a security awareness program, Foundstone can help develop one for your company. In the same way a marketing team puts together a year-long advertising campaign to increase awareness of a new product; Foundstone uses its expertise in security education to put together a year-long security awareness campaign that will deliver security messages throughout the organization. A typical campaign highlights different security messages on a periodic basis and implementing such a program complements your organization's security efforts.

Foundstone's Security Awareness Program Development is divided into seven major phases:

- Determine Major Organizational Roles
- Identify Current Awareness Issues

- Determine Topics and Identify Content (Via a Needs Assessment)
- Policy Review to Verify Compliance
- Evaluate Delivery Mechanisms
- Content Development
- Implement/Deliver Campaign Materials

Training or education can be delivered by Foundstone in variety of modes specifically targeted to each major employee role. These modes range from in-depth seminars for specific system administrators to break room posters for general staff. Executive briefings can also be developed as well as customized computer-based training that all users can participate in. We can also create customized security articles for inclusion in corporate newsletters, websites or other company-wide periodicals. Content would be developed on a regular basis so that users are given a consistent, timely and periodic security message. Depending on the audience and content, the delivery mechanism can range from one hour lunch-time brown bag seminars to multi-day workshops to "anytime" computer-based training.

Examples of techniques used for delivering Security Awareness Material:

- Portal, blogs, forums and polls
- Posters and "Do and Don't" lists
- Messages on branded trinkets (mouse pads, mugs, post-it notes, key chains, stress balls, bookmarks, calendars, buttons, t-shirts etc.)
- Screensavers and warning banners / messages
- Articles in corporate periodicals

- Special fliers - hardcopy, bright-colored one-page bulletin that is distributed through the organization's mail system
- Company-wide email / voice mail message
- Videos - especially during new employee orientation
- Computer and web based training that integrate with a SCORM compliant Learning Management System (LMS)
- Webcasts / webinars to the entire organization (video on demand)
- "IT Security Days"
- Executive-level briefings and progress reports
- Traditional in-person seminars or training sessions
- Lunch / "brown bag" seminars
- Corporate training manuals
- Executive level messages (Voice, Email, Inter-Office mail)
- Pay stub messages
- Intranet banners, messages, and animated gifs
- CD with corporate security information
- Corporate mailings to home address through USPS
- Tri-Fold pamphlet handouts
- Login banners on network systems
- Customized awareness campaign logo
- Badges of honor for training completion / belts
- Redeemable points and potential access to incentives such as the McAfee Home Use program

SECURITY AWARENESS 101 CBT

This course is designed to teach all employees of an organization their role in protecting your organization's assets from threat agents both inside and outside of the organization. Employees will learn how to protect themselves from electronic attacks, such as viruses, worms and "sniffing" communications, social engineering and physical threats.

Who Should Take This Class

All employees should take this class. No technical experience or expertise is required, although a

basic understanding of using a computer and the internet is helpful.

Course Outline

Introduction

- Why Security?
- Why Now?
- Why Me?
- What To Protect and How?

Threats to Our Data

- Outsiders: Hackers, Organized Crime and Business Competitors
- Insiders: Employees, Consultants/Contractors, Former Employees
- Accidents and Natural Phenomena

What Can Employees Do to Protect Our Data?

- Awareness of What Requires Protection
- Common Steps to Protect Information at Rest and in Transit

How is Security Compromised?

- How Attackers Gain Access, Use Their Access and Cover Their Tracks

Attacks and Defenses

- Logins and Passwords
- Social Engineering
- Viruses, Worms and Spyware
- Internet Access & Web Surfing
 - Corporate Network
 - Home Network
 - Wireless Networks
 - SSL and Encryption
 - Social Networking
- Email
- Physical Security
 - Building Access
 - Your Workspace and Computer
 - Mobile Devices and Media
- Data Backup
- Data Destruction