



SECURITY DIRECTIONS™ 101: Awareness

Designed for all employees, Security Directions™101 is a 30 minute online awareness course that provides the foundation of critical security principles. It is intended to help sharpen employees' existing knowledge of security as well as present new information that impacts the entire organization.

Using a stimulating and creative approach that engages and challenges the learner, the course builds awareness of security policies and processes. Realistic examples are presented that add relevance for learners from different departments and levels within the organization. The objective is to create informed employees who make better decisions and lower risk.

Outline of Key Topics

Welcome

- Message from key security leader (optional)

Lesson 1: Understanding Security Threats

The security threats that face organizations and what employees can do to prevent them.

- Security threats (including social engineering, malware, misuse of authorized access and mishandling of data assets)
- Social engineering examples (including information requests, phishing, pharming and physical access violations)
- Preventing social engineering attacks
- Malware examples (including worms, viruses, Trojan horses and spyware)
- Preventing malware

Lesson 2: Practicing Safe Computing

The best practices for safe use of passwords, e-mail and the Internet. This lesson is *customizable* to include company policies related to passwords, email and Internet usage.

- Password guidelines
- Secure and confidential e-mail
- Secure Internet use
- Safe Instant Messenger practices (optional topic)
- FTP best practices (optional topic)
- Back-up procedures (optional topic)
- Virus protection, spyware and pop-up blocker software (optional topic)

Lesson 3: Protecting Data

The best practices concerning the secure handling of client and employee data. This lesson is *customizable* to include company guidelines.

- Data classifications
- Data transmission guidelines
- Data storage and retention guidelines
- Data destruction guidelines (including paper documents, media and computer files)

Lesson 4: Practicing Safe Remote & Mobile Computing

The guidelines for working remotely or connecting via mobile devices.

- Tips for working in public places (including discussions of shoulder surfing and eavesdropping)
- Protecting your mobile computing devices (including laptops, PDAs, cell phones, etc...)
- Remote access to corporate network (optional topic)
- Security trips for travel (including securing baggage, electronic devices, data, etc...)

Lesson 5: Protecting Physical Security

The importance of securing the physical environment. This lesson is *customizable*.

- Securing offices and service areas (including work space, documents, media and badges - if applicable)
- Access control (including visitor procedures)
- Emergency preparation (including emergency contact information, evacuation procedures, etc...)

Lesson 6: Using Security Resources

The resources available to employees at the time of a security incident or as a reference material. This lesson will be *highly customizable* to your organization.

- Security checklists
- Links and documents
- Security contacts (phone numbers, e-mail, etc...)

Optional Customization – Lesson 3

MediaPro can add content to the courses specific to your security people, policies, procedures and technology. This can include links to specific resources.

Tracking Course Usage

MediaPro courseware is compliant with the industry standard SCORM 1.2.6. Our courses have been certified and used on many different standards-based Learning Management Systems (LMS) to manage module delivery and to integrate with a SCORM compliant LMS.

Hosting Options

The courseware can be hosted on the client's intranet and integrate with an existing Learning Management System, or MediaPro can provide an Internet hosting service on its e-Learning platform. The MediaPro Platform will provide the functionality to enable users to access courses via the internet, and to enable the client organization to track progress and monitor the results of users taking the courses.

Our Experienced Expert:

Richard Purcell

Corporate Privacy Group
Director, TRUSTe

Mr. Purcell has served as a director of TRUSTe, the independent trust authority for Web site privacy for over three years. He has also served as a director of the International Association of Privacy Professionals. In addition, he has served on the Federal Trade Commission's Advisory Committee on Security and Access and is now serving on the Advisory Committee of the Department of Homeland Security.



Sample screen from the Security Directions™101 course

Client Workstation Requirements -

CPU:

PII 450 or greater

Memory:

64 Meg or greater (128 Meg rec.)

Operating System:

Windows 2000 or XP

Screen Resolution

800 x 600 (or higher)

Browser:

Internet Explorer 5.5 (or higher)

Flash Player:

Version 6 (or higher)

Color:

16 bit (or higher)

Bandwidth:

256 Kbps

Cookies:

Must be enabled

Javascript:

Must be enabled

Server Requirements -

CPU:

PIII 1.26 GHz or greater

Memory:

512 Meg or greater

Operating System:

NT 4.0 or Windows 2000 (fully patched) or Unix

Disk Space

500 Meg

Domain

Same network domain as LMS system (rec.)