



PERIMETER E-SECURITY

- ▶ Providing a single, complete source for all your security needs since 1997
- ▶ Constant, around the clock monitoring with over 150 security personnel analyzing information 24/7/365
- ▶ Continuous third party assessments including an annual SAS 70 Type II and Cybertrust security audit
- ▶ Three redundant data centers and seven offices nationwide
- ▶ Servicing over 2,000 financial institutions in the United States

Call Us Toll Free: 800.234.2175

PERIMETER E-SECURITY E-SECURITY TRAINING OVERVIEW

Employees generally are unaware how easily they can be manipulated into divulging confidential information or computer system access. For example, hackers described as social engineers take advantage of human nature -- most humans want to be helpful. They use a variety of techniques to gather private information:

- **Pretexting** - using an invented scenario and a piece of known information to establish legitimacy in the mind of the target. This information is then used to obtain Social Security Number, date of birth, or mothers' maiden name as 'verification.'
- **Phishing** - creating an email that appears to come from a legitimate business, requesting verification of information and warning of a consequence if they do not comply. Usually the email contains a link to a fraudulent web page that looks legitimate.
- **Trojan Horse** - a destructive program that masquerades as a benign application

Employees may recognize some of these techniques but unfortunately not all, leaving the company and its network vulnerable. Employees need to understand the importance of network security and the key role they play in protecting company information. For example, employees may create common passwords to simplify their life and daily routines, but this also makes it simpler for hackers to gain access to the computer system.

Protecting sensitive company data as well as computer system access is one of the most important activities a company needs to address, but with hacking techniques changing daily, it is nearly impossible to accomplish.

PERIMETER E-SECURITY E-SECURITY SERVICE

E-Security & Compliance Training is an easy-to-use online training program with a wide variety of courses. This training will help your organization achieve regulatory compliance and prepare your staff for the growing challenges of protecting customer and network privacy while reducing the threat of identity theft. Our program manages the effectiveness of your employees' course performance and generates reports available for printing by management at any time.

Employees complete the training with a strong knowledge base of what is potentially dangerous activity and how important each individual is in complete company security. Available courses include Introduction to Information Security, Safe Surfing, Avoiding Identity Theft, Dealing with Spyware, Banking Information Security Introduction, HIPAA Security for Healthcare Staff, and more.

E-SECURITY TRAINING

Key Features	Benefits
Web Based Security Portal	24/7 access allows users to complete training whenever and wherever it is convenient for them, resulting in increased employee productivity
Regulatory Compliance	Assists companies with learning about and meeting regulatory compliance including: GLBA, SOX, PCI DSS, HIPAA, FISAP, COBIT, and ISO 17799
Standard Training Material	Each employee is trained on the same material in the same manner for uniform training and message
Custom Courses	Create and upload custom courses using tools such as Microsoft PowerPoint
Refresher Courses	Annual "refresher" courses include new topics, reviewing and testing all core material
Document Uploading	Administrators can upload company and HR policy documents for viewing
Cost Effectiveness	Information dissemination through computers and the Internet is extremely cost efficient
Just-in-Time	Employees can learn on an as-needed basis. Employees can also access course information at any time
Ease of Use	Taking this course requires simple log-on and click through. No special navigation is required
Learner Controlled	Technology has given the individual greater authority over the learning environment and can be used at one's own desk or at home
Subjects Cover a Full Range of Security Topics	<ul style="list-style-type: none"> ■ Passwords - how to create a strong password and the techniques hackers use to crack them ■ Data Classification - details on the different types of data and permissions associated with editing and deleting ■ Viruses & Hoaxes - malware concepts and protective controls each employee can take ■ Social Engineering - gathering of private information through conversations, and how to avoid crossing the line from helpful to harmful

Call Us Toll Free: 800.234.2175