# Hippogriff LLC - Awareness Training Fast Look

**The strongest AND weakest link for any organization are the people entrusted to care for it. Not only do technical staff have to keep up with changes to deployed software and hardware distributed throughout an organization, but they have to keep apprised of worker concentration lapses which are the primary cause of successful cyber intrusions.**

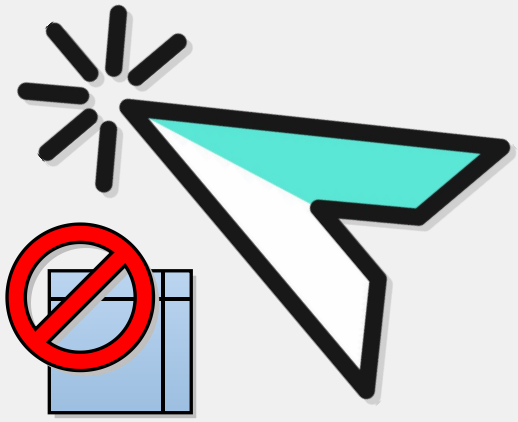

Cyber Security Awareness Training is one of the most important elements in fielding a precise and compliant approach to combating the barrage of daily malicious attempts against networks and devices. The best way to teach the skills of alertness is by personable instruction through hands-on simulations, and thus allowing for behavior modification to take hold within the minds and personalities or workers; this requires persistent thought immersion via real-world skills development.

**Training Modules**

- Malicious Hacking, Cracking, and Cyber Crime
- Proper Handling of Payment Cards
- Mobile Phone Security
- Security at Home
- Identity Theft
- Online Security and Privacy
- Phishing and Social Engineering
- Website Security
- Malicious Software
- Wireless Security
- Using Good Passwords
- Travel Security
- Interacting with Callers
- Working with Outside Vendors
- E-Mail Security and Chat Privacy
- Working Remotely
- Handling Company Information
- Data Encryption
- Desktop and Laptop Security
- Backing Up Data
- Business Continuity
- Red Flag Rules and Data Retention
- Document Handling and Privacy
- Remote Access and Working Remotely
- Device Application Integrity
- Social Networking
- Legal and Financial Consequences

Companies must assess and address the risks to customer and employee information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. Depending on the nature of their business operations, firms should also consider implementing the practice of Employee Management and Training. The success of an organization's information security plan depends largely on the employees who implement it; they must be prepared as much as possible.

In the United States, there are currently more than 8,500 Local, State and Federal standards that an organization might need to comply with, and more regulation is going into effect every quarter annually. Some of the required awareness programs that organizations must have in place within the U.S. and its territories include: PCI DSS, Sarbanes-Oxley (SOX), Health Insurance Portability & Accountability Act (HIPAA), ISO/IEC 27001 & 27002, FACTA - FTC Red Flags Rule, Gramm-Leach Bliley Act, CobiT, Federal Information Security Management Act (FISMA, NERC CIP, and a plethora of individual U.S. State Privacy Laws such as: A.R.S. § 18-551 - Arizona, Civil Code § 1798.82, 1798.84, and § 1798.29 + CaCPA - California, H.B. 15 - New Mexico, 23 NYCRR 500 - New York, CMR 17.03 - Massachusetts, etc. There are also hundreds of thousands of international rules and regulations that may apply to U.S. business operations as well; such as: GDPR, PIPEDA, ePrivacy, UKIaG, ANDBS, and more. International business operations may reversely be required to abide by U.S. standards as well.



The cost of simple lapses when interacting with data storage and processing materials can be enormous. Correct training through a combination of virtual platforms, tangible environments, educational media, interactive profiling, example demonstration, and challenging game theory is all provided through the Training Modules to garner a fun and intriguing experience for workers.

**Computer Technology Protection Services**

1-866.273.4831
inquiry@hippogriff.tech
Hippogriff.TECH • Hippogriff.IO