Security and Privacy Awareness TRAINING

Inspired eLearning
The **gold standard** in security and privacy training, for not a lot of gold…

Turn-Key Training Solution

Investing in technical security controls is essential for securing your organization's information and ensuring privacy. But technical controls are not enough.

Consider for a moment that every employee and contractor is given access through gates, locked doors, authentication systems, firewalls and encryption systems. Clearly without end-user training on security best practices, it is impossible to secure your information resources or ensure privacy.

This fact coupled with training mandates, such as **PCI, FISMA, SOX, GLBA, HIPAA,** and **Red Flag** make a turn-key security and privacy awareness training program essential to any organization's compliance and risk management initiatives.

Building a Security Conscious Culture

Our 46-course security awareness training library is designed as an enterprise-wide communications tool that fosters a security conscious culture. Our program includes unique all-employee annual training content for up to seven years, anti-phishing training, simulated phishing attacks, annual updates, a monthly eNewsletter, posters, screensavers and job aids to provide a constant stream of tips and best practices that learners can put to use immediately to enhance security.

Use our comprehensive and highly interactive program to train your workforce, comply with laws, regulations and standards and reduce the risk of security and privacy breaches.

30% of IT Security relates to technology. 70% relates to people and practice.

A turn-key, web-based training program to build, manage and maintain security awareness.

Make your end-user population a powerful defense by training them to recognize and respond to threats immediately.

Inspired eLearning's

Unique Benefits Include:

Named a Leader in Gartner's Magic Quadrant for Security Awareness

Our Security Awareness Training Platform is a recognized leader in the industry. In addition to winning numerous awards, we're very proud to have been recently named an industry leader by the world's foremost information technology research and advisory company – Gartner.

We believe this recognition comes from our unceasing focus on providing world-class IT compliance and training solutions to organizations of all sizes.

The Most Comprehensive Security and Privacy Awareness Program Available

What happens in year two of your security awareness program? Do you send out the exact same training material again, knowing that end users will complain and that it won't be nearly as effective? What about year three or four? Only Inspired eLearning has an answer to this question. We deliver unique training to your end users for seven years. Don't get caught going through a long procurement process, only to be stuck having to choose between delivering the same content all over again, or starting over from scratch. ***Do your employees prefer fresh security awareness training content every year? Choose Inspired eLearning, the only security awareness content provider that's NOT a one trick pony.***

Industry and Government Acceptance: Over 4 Million Users Worldwide

Our security awareness programs have received rave reviews from public and private organizations such as ACE Group, ADP, Banco Santander, BJ's Wholesale Club, Johnson Controls, the Securities Exchange Commission, Bridgestone Firestone, Hearst Corporation, Merck, Tenet Health Systems, Nokia, Toys-R-Us, US Air, ING, Convergys, Tata, Levis Strauss and DTE Energy, just to name a few. Don't waste time re-inventing the wheel. Plug into an existing all-inclusive solution used by some of the most respected organizations in the world.

Looking for a proven security awareness training solution? Choose Inspired eLearning.

We Change Behavior with Simulations

A purely passive video training experience might seem like a good idea, but did you know retention rates for video demonstrations are only 30%, while retention rates for simulations are 75%, which is to say 250% better? When learners actively experience simulated attacks and go through the actions required to avoid being hacked, they're more likely to do the same in the real world. In addition to eye-catching content, our courses include password construction simulations, phishing email simulations, Wi-Fi security simulations and many more.

Looking for a solution that really makes a difference? Choose our mature content to maximize learner retention and security conscious behavior.

Integrated Anti-Phishing Training & Simulated Phishing Attacks

Are your end-users susceptible to phishing or spear-phishing attacks? Check out PhishProof, our anti-phishing training and assessment service that includes iPad-compatible, simulation-focused training, free phishing assessment software, detailed analytics and reports, and complete deployment services.

Ready to make your end-users part of the solution? Contact us for more details.

Standards Based Awareness Training Built for Comprehensive Compliance

Our courses have been meticulously designed to meet and exceed every topic required by **major standards and regulations.** Don't get caught with a course that doesn't offer comprehensive compliance. ***Need to survive the audit? Choose Inspired eLearning for peace of mind.***

Modular 46-Course Role-Based Library

Our 46-course role-based library is unmatched. In addition to providing seven years of unique all-user content, we include anti-phishing training and courses for managers, IT professionals and programmers, plus specific compliance training for PCI, privacy, red flag and other laws, regulations and standards. Each of our courses is built from multiple modules, which we've pre-packaged for your convenience. You can choose to deliver them in their default form or easily assemble the modules into custom courses tailored to specific audiences. In fact, just tell us how you'd like them packaged and we'll do it for you. ***Looking for lots of flexible content that can easily be mixed and matched? We've got that covered.***

7 years of unique annual content

46-course library

Security and Privacy Awareness TRAINING

100% Customizable Content. We're Not Just Talking About a Logo and Link…

Your organization is unique and your training program should be too. If you expect your end users to learn, understand and abide by your specific policies and procedures, they must be presented within the course itself and not just tacked on as a PDF at the end. We pride ourselves in fully customizing our content for our clients and producing an end product that is highly relevant and engaging for learners.

Need end users to actually understand your policies? We can help.

Above and Beyond Support: An Implementation Manager and Tech Support for Every Client

Our clients are usually small teams or individuals tasked with training thousands, tens of thousands, or hundreds of thousands of employees across the globe – every year. As you can imagine, when that's your responsibility, what you really need is a world-class service organization to back you up. That's exactly who we are. We proudly include a highly experienced Implementation Manager to work with you every step of the way. And we don't stop there. We provide a first, second and third level tech support team with deep skills in eLearning, SCORM, AICC, LMS integrations, reporting and everything else needed to ensure your program is a success.

Looking for more than just a course?
Our training comes standard with "Above and Beyond" support.

21 Languages Ready to Go

Choose Inspired eLearning to go global. Our courses are fully translated, including the on-screen text, to give your non-English audience the same high quality experience offered to your English speaking audience. Our courses are available in US English, UK English, Spanish, Latin American Spanish, German, French, French Canadian, Italian, Dutch, Japanese, Simplified Chinese, Traditional Chinese, Korean, Thai, Brazilian Portuguese, Polish, Czech, Russian, Hungarian, Greek and Bulgarian and can be translated into any other language. ***Looking for global reach? Check out our security awareness training program.***

An Enterprise-Class, Customizable Learning Management System

Many training companies tout a learning management system option, but only Inspired eLearning offers an enterprise-class LMS that can be fully customized to your needs. The iLMS offers ad-hoc reports automatically emailed to you, regularly scheduled automatic reminders for learners, automated exports to your HR system, LDAP synchronization, Single-Sign-On (SSO) and multi-server deployments capable of training hundreds of thousands of learners. Settling for anything less could leave you locked into an inflexible solution that can't meet your needs.

Need a flexible, customizable LMS that integrates into your existing infrastructure? We can help.

Broad Technical Compatibility with Courses Delivered to Millions of Learners

Delivering online security awareness training to 500, 1,000 or 10,000 people means running software on that many computers, many of which have different settings, browsers and operating systems. This is where experience really comes into play. We have delivered training to over 4 million users worldwide in 21 languages on PCs and Macs so you can be certain that our software is tested, mature and ready to go. ***Have a highly mixed client computer environment? We have the solution.***

An Engaging, Highly Interactive Program

Engaging learners and keeping their attention are essential requirements of any eLearning course. Our courses are designed to grab learners' attention with thought-provoking scenarios, simulations and real world stories and keep it with a quick pace and lots of interactivities

Looking for highly interactive and engaging security awareness courses? Check out our demos.

Low Bandwidth Requirements

A training program shouldn't drain your corporate bandwidth and affect productivity. Our courses are designed with global, enterprise-scale deployments in mind. Course can be as small as five megabytes for each learner. Don't get stuck with a high-bandwidth-only solution that doesn't always load correctly or hogs network bandwidth when it does.

Need a proven solution that scales? We have the answer.

A Monthly Newsletter with Actual News

Our monthly eNewsletters are more than just a summary of a topic we covered in a course. They include a current relevant article plucked from the headlines that proves our point about security to end-users. This approach is much more powerful and much more likely to change behavior.

Looking for an impactful eNewsletter that is timely and likely to change behavior? Contact us for a sample.

Features at a Glance

- 46-course library
- 100% customizable course content
- Annual updates
- Monthly eNewsletter
- Security awareness screensavers
- Security awareness posters
- Online testing and certification
- A comprehensive policy acceptance tool
- Your logo on every page
- An introductory message from your management team
- Automatic course bookmarking
- SCORM and AICC compliance
- Hosted on your LMS or ours
- Ad-hoc reports available in CSV, XLS, and PDF
- User data synchronization with HR systems
- Course history synchronization with HR
- Single-Sign-On (SSO) / LDAP

46 - Course Library

1. S-101: Basic Security Awareness 30-40 minutes
Protecting your personal and workplace data is as crucial as protecting your bank account. Hackers, identity thieves and malicious programs roam the Internet searching for easy targets. Learn the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. By mastering the information presented in this course you will be able to defend your personal and workplace data from malicious threats and become certified in basic security awareness.

2. S-102: Advanced Security Awareness 20-30 minutes
Learn the advanced security awareness topics needed to complete your training and be a human firewall. By mastering the information presented in this course you will be able to defend your personal and workplace data from malicious threats and become certified in information security awareness and literacy.

3. S-103: Security Awareness and Literacy 50-70 minutes
This course combines S-101 and S-102 into a single training program for organizations who would like to deploy one training program that covers every topic required by **major standards and regulations.**

4. S-105: Security Awareness Refresher 15-25 minutes
Review the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. Each topic is followed by an interactive quiz.

5. S-110: Security Awareness for Managers 20-30 minutes
Your managers are in a unique position to influence the success or failure of your security awareness program. Because they are the voice of your organization to their direct reports, their behavior and buy-in is a critical component of ensuring your cultural transformation to a security conscious organization. Therefore, training them to lead by example and encourage their teams to conduct everyday business in a responsible and secure way that reduces organizational risk, increases productivity and complies with policies, laws and regulations is critically important. This security awareness course is designed to do just that and is part of Inspired eLearning's role-based enterprise wide security awareness training program.

6. S-111: Privileged User Security 20 minutes
Hackers and cybercriminals specifically target privileged users. After all, they have access to an organization's most prized data. This course will teach privileged users the security best practices they're expected to follow in order to defend against hackers.

7. S-120: Security Awareness Challenge for I.T. Pros 20-30 minutes
Hackers. Fraudsters. Spammers. Phishers. Social Engineers. Malicious insiders. They're out there, trying to get in and it's your job to stop them and keep the systems that power your organization humming along. This course is meant to refresh your knowledge and raise your awareness of security issues. The bulk of the course is an interactive exam called the Security Awareness Challenge with questions similar to what you might find in an entry level security certification exam.

8. S-125: Baseline Information Security Training for IT Professionals 75-90 minutes
To ensure enterprise security it is important to establish a baseline of fundamental information security knowledge that every single employee in the IT department must have. And the best way to ensure this baseline is to regularly train all current employees and new hires. This course is designed to provide that baseline of knowledge to any organization and to be easily customized to fit your particular policies, procedures, best practices and guidelines.

9. S-126: Introduction to the OWASP Top 10 20 minutes
The Open Web Application Security Project (OWASP) is a global community focused on improving the security of web application software. The OWASP Top Ten list is highly respected and has been adopted by, among other organizations, the Payment Card Industry (PCI) Security Standards Council. This short lesson reviews the top ten list to ensure all web application developers in your organization are exposed to it.

10. S-131: Basic Security Awareness 35 minutes
This is part of our second all-user security awareness training course, which is designed to provide a fresh training experience in year two or three of your program. The theme of this course is “the strongest link.” It covers the same topics as S-101, such as physical security, social engineering, phishing, malware, password management, privacy, incident response and acceptable use.

11. S-132: Advanced Security Awareness 25 minutes
This is part of our second all-user security awareness training course, which is designed to provide a fresh training experience in year two or three of your program. The theme of this course is “the strongest link.” It covers the same topics as S-102, such as legal issues, what is information security, threats and vulnerabilities, storage and transmission, mobile data, telecommuting and travel safety.

12. S-133: Security Awareness and Literacy 60 minutes
This is our second all-user security awareness training course, which is designed to provide a fresh training experience in year two or three of your program. The theme of this course is “the strongest link.” It covers the same topics as S-131 and S-132 and is a follow up to S-103.

13. S-135: Security Awareness Refresher 20 minutes
This is our second all-user security awareness refresher course and is a companion to S-133. It reviews the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. Each topic is followed by an interactive quiz.

14. S-141: Security Awareness 30 minutes
This is our third all-user security awareness training course, which is designed to provide a fresh training experience in year three, four or five of your program. It is designed to cover all of the essential topics in 30 minutes or less such as password management, identity theft, malware, social engineering, phishing, physical security, travel safety, mobile data, privacy and acceptable use.

15. S-151: Security Awareness: Rise of the Singularity 35 minutes
This is our fourth all-user security awareness training course, which is designed to provide a fresh training experience in year four, five or six of your program. This dramatic movie-like course uses a “spy thriller” theme. Learners use security best practices to defend a new super-computer from “the foundation,” which is determined steal it.

16. S-155: Security Awareness: Rise of the Singularity (Refresher Version) 25 minutes
This refresher version of our dramatic movie-like security awareness course uses a “spy thriller” theme. It reviews the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them.

17. S-161: Security Awareness iModules

S-161-MD Protecting Mobile Data and Devices 8-9 minutes
Because today's smartphones and tablets can not only act as a phone, but also as an email client, mobile Internet device, camera, GPS navigation system, entertainment console, and platform for any number of applications (apps), you can be exposed to many of the same risks as a desktop computer. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices or mobile security.

S-161-PS Physical Security 8 minutes
Your personal safety at work is of paramount importance. This course is designed to help employees protect an organization from criminals, espionage, workplace violence, natural disasters, and other threats. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach physical security best practices.

S-161-SE Defeating Social Engineers (Advanced) 20 minutes, (Standard) 11 minutes
With increasingly sophisticated technical defenses for networks and computer systems, hackers often decide that it's much easier to simply go around these perimeter defenses by attacking the end user. After all, end users have what they want – a computer that's behind the network firewall, a network username and password, and possibly access to trade secrets, confidential information, and bank accounts. This course will teach end users how to identify and avoid giving away sensitive information to these hackers.

S-161-SM Appropriate Use of Social Media 8-12 minutes
Social media can be an excellent tool to connect and interact with customers, show thought leadership, and build a brand, but it also poses unique security, HR, and public relations challenges. This course covers social media best practices including secure use, accountability, harassment, how to spot scams, secure passwords, and advanced security features.
This HTML5-based, iPad-compatible courses uses high-quality video and real-world simulations to teach best practices for social media.

18. AP-101: PhishProof Training 12 minutes
Because today's computers and networks are heavily defended from a direct assault, hackers are now much more likely target end-users when trying to break in. If hackers can trick you into divulging your username and password or inadvertently infecting your computer with malicious software, they can use your computer as a launching point to further penetrate your organization's network.

This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for recognizing and preventing both phishing and spear-phishing attacks.

19. PCI-101: PCI Essentials for Cardholder Data Handlers and Supervisors 25 minutes
This course teaches employees and supervisors what PCI DSS is, how it affects your organization and the best practices they should follow to protect cardholder data and detect and prevent fraud.

20. PCI-120: PCI Requirements Overview for I.T. Professionals 45 minutes
This course teaches I.T. professionals what PCI DSS is, how it affects your organization, how to comply with the 12 requirements and the best practices that front line staff should follow to protect cardholder data and detect and prevent fraud.

21. HH-102: HIPAA HITECH Security 30-40 minutes
This course covers information security awareness topics from the point of view of protecting medical records and all Protected Health Information (PHI). It includes similar topics as those found in S-101 in order to comply with the **HIPAA Security Rule.**

22. P-101: General Privacy Awareness 45 minutes
Protecting customer, organization, and employee private data is not just a core organizational value, it's the law. This course will help employees understand what information is private, why it is private, and what they can do to protect it throughout the data lifecycle, which is the life of a piece of information, whether in paper or digital format, from creation to destruction within an organization.

23. GLBA-101: GLBA Privacy Awareness 45 minutes
Protecting Nonpublic Personal Information (NPI) is more than just a core organizational value. Because of the Financial Services Modernization Act of 1999, also referred to as the U.S. Gramm Leach Bliley Act (GLBA), it's the law. This privacy course is specifically tailored to help financial services employees understand what information is private, why it is private, and what they can do to protect it throughout the data lifecycle, which is the life of a piece of information, whether in paper or digital format, from creation to destruction within an organization.

24. HH-101-BA: HIPAA / HITECH Privacy for Business Associates 45 minutes

Training employees to safeguard Protected Health Information (PHI) is a requirement of all "business associates" based on the Health Insurance Portability and Accountability Act (HIPAA), as ammended by the HITECH Act. This privacy course is specifically tailored to help employees of business associates understand what information is private, why it is private and what they can do to protect it.

25. HH-101-CE: HIPAA / HITECH Privacy for Covered Entities 45 minutes

Training employees to safeguard Protected Health Information (PHI) is a requirement of all "covered entities" based on the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act. This privacy course is specifically tailored to help healthcare employees understand what information is private, why it is private and what they can do to protect it.

26. PS-103: Physical Security 30-45 minutes

Train your employees to recognize and respond to physical security issues in the workplace, including workplace violence, theft and emergencies.

27. DR-101: Data and Records Retention 35 minutes

Electronic and hardcopy data is growing at a rate of about 125% per year and yet only 20% of that data is actually used to conduct business. Your employees need to be trained to only create the data they need, as well as how to properly and legally dispose of it when it is no longer required. This will not only lower your administrative burden, but will also make electronic discovery much less costly in the event of a lawsuit.

28. S-107: Red Flag Identity Theft Prevention 25 minutes

This course helps employees understand your Identity Theft Prevention Program and how they can help prevent identity theft by recognizing Red Flags and responding appropriately. It includes coverage of laws, regulations, definitions, identity theft prevention program details, detection, response, and handling address discrepancies.

ThreadStrong Secure Coding

29. TS-101: Intro to Web App Security 1 hour

This course provides students with the basic concepts and terminology for understanding application security issues. It provides a definition of application-level security and demonstrates how these concerns extend beyond those of traditional infrastructure security. It also provides an explanation of common application security vulnerabilities such as SQL injection, Cross Site Scripting (XSS) and authorization issues. Armed with this knowledge, developers, QA testers and security personnel can understand and start to be able to address application-level threats.

30. TS-102: Secure Coding for Java 4 hours

Once developers understand the basics, they are in a position to start learning more specific secure design and coding techniques. This course steps through the OWASP Top 10 as well as other common application security issues to demonstrate how applications are compromised and the design and coding practices that can help to secure applications from the Inside out. This version of the course is designed for the professional Java developer and teaches them platform-specific concerns and countermeasures.

31. TS-103: Secure Coding for .NET 4 hours

Once developers understand the basics, they are in a position to start learning more specific design and coding techniques for .NET application security. This course approaches application security practices and associated vulnerabilities as part of nine domains. Trust Boundaries covers essential principles regarding the treatment of application inputs from any source. In the Authentication and Authorization domains, we discuss application approaches to verifying a user is who they claim to be, and that that user is allowed to do what they attempt to do. Input Validation covers approaches to validating application input as well as what inputs should be subject to validation. With Information and Error Handling, Non-Repudiation and Auditing, Data Protection, and Configuration and Deployment, we discuss a wide range of practices that apply to applications and web applications in general, as well as recommended approaches for more distinct application features. This course is also available in a Java security training version so that developers learn platform-specific concerns and countermeasures.

32. TS-104: Threat Modeling 1 hour

Threat Modeling is a key practice for organizations wanting to design and develop secure applications as it helps to identify potential security vulnerabilities early in the process when they are inexpensive to fix. This course walks through the Threat Modeling process step by step so that students understand the value of Threat Modeling and can build threat models for their own systems.

33. TS-105: Software Security Remediation Basics 1 hour

Learn the key phases of a Software Remediation Project, how to structure them into a logical and formal process, and the inherent challenges found in each phase.

34. TS-106: Cross-Site Request Forgery Explained 20 minutes

Cross-Site Request Forgery (CSRF) is a serious and often-misunderstood web application vulnerability. This course goes into detail about the anatomy of a CSRF vulnerability as well as how security analysts can identify CSRF vulnerabilities and how developers can design and build applications resistant to CSRF attacks. Interactive examples and videos demonstrate the subtleties of CSRF vulnerabilities and how malicious attackers exploit them.

35. TS-107: Mobile Security 30 minutes

An introduction to the basic concepts and best practices of secure development for mobile devices, concentrating on Android and iOS. This is the first in our series of Topics in Mobile Application Security courses, which will provide a deeper look into the security issues surrounding mobile devices. Each course will concentrate on a top mobile application vulnerability, using examples from each platform to demonstrate the flaw and approaches to mitigation.

36. TS-108: Authentication and Authorization - Android 30 minutes

Examines issues in session management, transport layer security and other challenges facing developers of mobile applications. Platform-specific code examples demonstrate secure approaches to development for Android devices. This is the second in our series of Topics in Mobile Application Security courses, which will provide a deeper look into the security issues surrounding mobile devices. Each course will concentrate on a top mobile application vulnerability, using examples from each platform to demonstrate the flaw and approaches to mitigation.

37. TS-109: Authentication and Authorization - iOS 30 minutes

Examines issues in session management, transport layer security and other challenges facing developers of mobile applications. Platform-specific code examples demonstrate secure approaches to development for iOS devices. This is the second in our series of Topics in Mobile Application Security courses, which will provide a deeper look into the security issues surrounding mobile devices. Each course will concentrate on a top mobile application vulnerability, using examples from each platform to demonstrate the flaw and approaches to mitigation.

38. TS-110: Data Protection for Android

Explains the different types of local storage available on the Android platform, configuration and encryption for locally stored data, and secure network connections between the Android device and web services. This is the fourth in our series of Topics in Mobile Application Security courses, which will provide a deeper look into the security issues surrounding mobile devices. Each course will concentrate on a top mobile application vulnerability, using examples from each platform to demonstrate the flaw and approaches to mitigation.

39. TS-111: Validation and Encoding: Android

This course examines best practices for input validation and output encoding on the Android platform. You will learn to identify common vulnerabilities of the Android platform that validation and encoding can address. The forth in a series of Topics in Mobile Application Security courses, this course is intended for Mobile App Developers, Software Developers, Security Professionals, and Penetration Testers. Each course in the series focuses on the top mobile application vulnerability of the platform. In this course, users will learn from Android-specific examples that demonstrate vulnerabilities and the best approaches to mitigation.

40. TS-112: C/C++ Memory Management

C and C++ are widely-adopted, deeply influential, and supported by a tremendous variety of frameworks and development environments. This speaks to the diversity of C/C++ developers and applications. It should also remind developers that C/C++ security risks and exploits are well-known among attackers. Memory management is the most well-known risk with C/C++, and for good reason.

This course will cover memory management fundamentals and common coding flaws that open an application to buffer overflow exploits and other attacks. The course will cover secure coding practices throughout, providing fixes to coding flaws as well as recommendations for comprehensive memory management solutions.

41. TS-113: Application Security Testing

Application security testing is a way for organizations to identify and mitigate security vulnerabilities in their applications. This course covers the general approach used in a security assessment; the lessons identify the steps that take place and the activities that are performed during an assessment. The course covers the tools and techniques that are used to identify and follow-up on vulnerabilities discovered during the baseline and targeted testing steps of an assessment; the following assessment activities are explained: static analysis, dynamic analysis, forensic analysis, penetration testing, and code review. The lessons also describe how to rate vulnerabilities observed during an assessment according to the DREAD rating system and how to explain remediation recommendations in an assessment report.

42. TS-114: Secure Architecture and Design

Security testing and remediation are important in a software project to protect the organization; however, these measures are reactive and can be costly. This self-paced, e-Learning course covers the general concepts and approach to designing secure software architecture from the ground-up. We will discuss finding appropriate solutions for functional security requirements such as authentication, access control, and secure storage. The course also explains how to analyze the architecture for business policy needs and risks from external dependencies. The final section of this course discusses data flow and control flow analysis – data flow diagrams and control flow graphs are explained and utilized.

43. TS-115: Introduction to PCI DSS For Developers

This course will expose application developers to the Payment Card Industry (PCI) Data Security Standard (DSS). The course will provide background and context on why organizations must be PCI compliant, the risk of and penalties for non-compliance, and developer responsibilities associated with PCI DSS requirements. The course will include examples of threats to PCI cardholder data, an overview of PCI-relevant secure coding practices, and methods to maintain PCI compliance over an extended period. This course is designed for developers at all levels of experience and is programming language agnostic. Upon successful completion of this course, students should be able to discuss PCI DSS requirements, apply relevant knowledge to their roles, and be able to demonstrate to PCI assessors that they have completed a basic overview of PCI DSS and secure coding techniques, which partially fulfills PCI DSS Requirement 6.5.

Information Security Training

44. Certified Information Security Manager
IS-110: CISM TrainingIS-110: CISM Training 6 hours

The CISM certification program was designed specifically for experienced information security managers and those who have information security management responsibilities. The credential is meant for those who design, build and manage enterprise information security programs.

45. Certified Information Systems Security Professional
IS-115: CISSP® Training 25 hours

The CISSP credential is one of the most highly regarded information security certifications available. It is meant for professionals who develop and maintain information security policies and procedures and requires five full years of experience in information security. The CISSP is accredited by the ANSI (American National Standards Institute) to ISO (International Organization for Standardization) Standard 17024:2003.

46. IS-120: CompTIA Security+ Training 21.5 hours

The CompTIA Security+ vendor-neutral certification designates knowledgeable professionals in the field of information security. Security+ certified professionals can anticipate security risks, guard against them and properly respond to security incidents when they occur. This training program is meant for the following job roles: security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator and network administrator.