Security Communications and Awareness

eLearning

OVERVIEW

Recent high-profile incidents underscore the need for security awareness training. In a world where your employees are frequently exposed to sophisticated attacks, users can be the weakest link in the security chain. By training end users, you can help protect your organization from attack.

Our engaging courses are designed to help you meet compliance requirements, minimize risks and maximize data security.

- Educate employees about how to safeguard data and protect company resources
- Reduce training and awareness costs as you streamline delivery
- Deliver consistent information to geographically-diverse users on how to identify and avoid risks users to identify and avoid risks
- Track, document and report on the impact of your program
- Assist with compliance and regulatory requirements

Our eLearning Advantage:

- ✓ Advanced reporting metrics
- ✓ Hosting options
- ✓ Mobile-friendly (html5)
- ✓ Licensing options
- ✓ Client site provisioning and support 24x7x365
- ✓ Single sign-on
- ✓ Content and site branding
- ✓ Security awareness newsletter (PDF or HTML5)
- ✓ Topic-aligned posters
- ✓ Digital security awareness vignettes
- ✓ Multi-lingual support

Typical eLearning	Optiv's Security Awareness
• Content-focused	✓ Performance-focused
• Efficient for Authors	✓ Meaningful to Learners
• Attendance-driven	✓ Engagement-driven
• Knowledge Delivery	✓ Authentic Contexts
• Fact Testing	✓ Realisitic Decisions
• One-Time Events	✓ Spaced Practice
• Incorrect/Correct Feedback	✓ Real-world Consequences

Optiv's eLearning Courses

Security Awareness

- Tier 1: Rapid Awareness
- Tier 2: CyberBOT
- Tier 3: Security Awareness Circuit Training (SACT)

Compliance

- Introduction to PCI
- Credit Card Handling

Developer

- Mobile Security Top 11
- OWASP Top 10
- Secure Coding Java/NET
- Web 2.0 Secure Coding

The Security Awareness Assessment

Provides a bird's-eye view on the state of the security awareness culture within an organization.

The Assessment

- Evaluate and define existing security awareness landscape and culture
- Inventory assets and strengths
- Define gaps and roadblocks
- Provide guidance and roadmap on implementation
- Measure the efficacy of existing program with guidance on how to improve

Security Awareness Training

Goal

Arm your employees with the knowledge and skills to protect your organization.

Available Modules

- Password security
- Email security
- Mobile security
- Social engineering
- Workplace security
- Business travel
- Malicious downloads
- Social media security
- Data privacy
- Identity theft
- Cloud security
- Insider threat
- Cyber security at home

DELIVERY DETAILS

- Optiv-hosted or client-hosted
- SCORM, Tin Can /xAPI and AICC-complaint database formats

Rapid Awareness	CyberBOT	Security Awareness Circuit Training
• Micro-learning • Informative with basic interactions • Fully-responsive • Linear path of content delivery • Includes video vignette on topic	• Interactive • Linear path to learning • End users are taught concepts up-front and then given opportunity to practice what they have learned. • Each course touches on multiple topics, with a mix of knowlege-based and behavior-based.	• Immersive • Branched paths of learning based upon user-decisions • End users learn by navigating through real-world scenarios and reviewing the consequences of their actions.
• Organizations that have limits on the amount of time employees can take on training initiatives. End users are viewing content mainly on mobile devices.	• Organizations that have experienced great success in a traditional, instructor-led style of training solutions. • End users that may need more of a traditional approach to navigation. End users that are not used to elearning as a training modality.	• Organizations looking to 'disrupt' their current training modality with a solution that challenges the end users. • End users that are familiar with eLearning as a training modality and would be comfortable with navigation that is outside the box.
• Mixture of Illustrations and Photos	• Illustrated	Photo-real
• Three multiple choice questions	• Five questions from a bank of ten • Mixture of multiple choice, true/false, and multiple select questions	• Five questions from a bank of 10 • All multiple-select questions (increases difficulty)
• 5-7 minutes	• 10-15 Minutes	• 10-15 Minutes

Compliance:
Credit Card Handling

Goal

Employees who handle customer credit cards on a daily basis are the first stop when it comes to the security of customer data. Educate them on credit card security best practices and why they matter.

Course Overview

This multi-occupational, interactive security training course will educate employees on credit card security, best practices and why it matters.

Course Tracks

- Call center
- Table service
- Quick serve
- Manager

Module Outline

› Introduction to PII
› Credit card basics
› Chip and pin transaction best practices
› Why security is important
› Interactive "what would you do" scenarios

TIME FRAME

› (1) Module – 20 min

DELIVERABLES

› Improve security effectiveness between employees and customers.
› Increase retention and influence behavior.
› Give customers peace of mind their credit card data is safe when conducting business with your organization.

Compliance:
Introduction to the Payment Card Industry (PCI)

Goal

Educate employees about what the PCI is, how to interact with its regulations, the penalties for not complying and the types of data they can and cannot store.

Course Overview

The Introduction to PCI eLearning course was created for everyone who interacts with credit or debit card data in mind. This includes everyone from cashiers to traveling sales staff to system administrators.

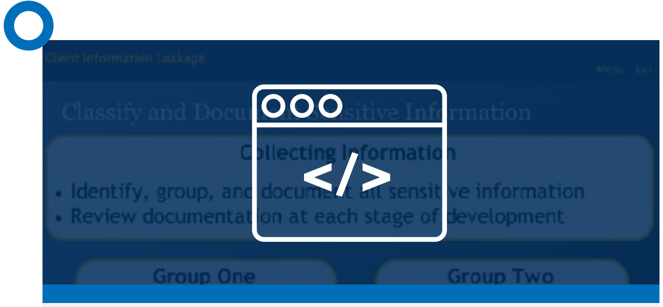
Course Outline

› Identity theft
› Data protection standards
› Data flow
› PCI council
› PCI DSS
› Classification levels
› Verifying compliance
› Card data that can be stored
› Penalties and fines
› Costs of a data breach
› Basic security guidelines

TIME FRAME

› (1) Module – 15 min

Developer:
Mobile Security Top 11



Client Information Leakage

Menu Exit

Classify and Docu sitive Inf rmation

C llecting I formatio

- Identify, group, and docume t all sensit ve information
- Review documentat on at each stage of development

Group One Group Two

In today's mobile environment, there is a drive for developers to quickly and efficiently create mobile applications for a variety of devices. As they develop the next generation of mobile applications, developers must keep security best practices at the forefront. They must know how to secure both the application that will be deployed to the mobile device and the web services that power the app. If either are left insecure, attackers will exploit any weakness they find. This 1.5-hour course covers the important security topics developers need to understand, regardless of development platform or language.

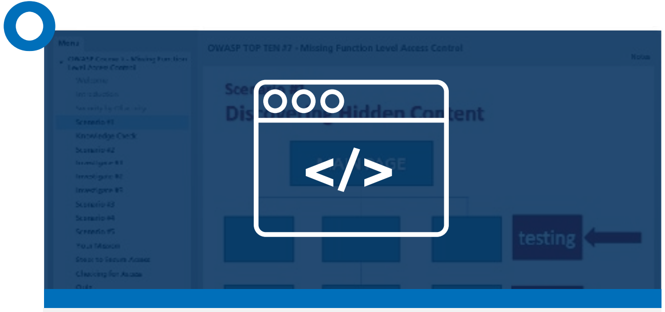
TIME FRAME

› (11) Modules – 90 min

Course Outline

- › Application error messages
- › Application response handling
- › Authentication and session management
- › Client information leakage
- › Client-side injection
- › Cross-site request forgery
- › Data storage
- › Sensitive information disclosure
- › Transport layer security
- › User account lockout
- › User input caching

Developer:
OWASP Top 10



Menu

OWASP TOP TEN #7 - Missing Function Level Access Control

Home

Sce

Dis Hidden Con ent

The Open Web Application Security Project (OWASP) Top 10 document regularly provides the 10 most frequent and dangerous security vulnerabilities organizations deal with every day. This course allows users to explore what each attack is, how each attack works, detailed examples of each attack, remediation steps and best practices that they can easily incorporate into their everyday development and coding work.

TIME FRAME

› (11) Module – 90 min

Course Outline

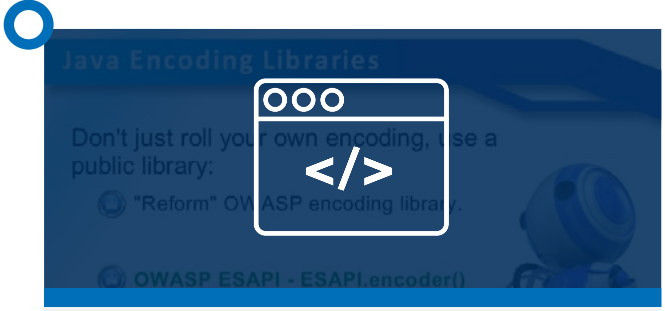
- › Introduction
- › Risk #1: Injection
- › Risk #2: Broken authentication and session management
- › Risk #3: Cross-site scripting (XSS)
- › Risk #4: Insecure direct object references
- › Risk #5: Security misconfiguration
- › Risk #6: Sensitive data exposure
- › Risk #7: Missing function level access control
- › Risk #8: Cross-site request forgery (CSRF)
- › Risk #9: Using components with known vulnerabilities
- › Risk #10: Unvalidated redirects and forwards

Developer:
Secure Coding

The Secure Coding section is composed of eight total modules: four are .NET and four are Java. Each module covers the same basic information in the first quarter before diving into language-specific content.

Course Outline

- .NET input validation
- .NET output encoding
- .NET error handling
- .NET SQL injection defense
- Java input validation
- Java output encoding
- Java error handling
- Java SQL injection defense



Java Encoding Libraries

Don't just roll your own encoding, use a public library:

- "Reform" OWASP encoding library.
- OWASP ESAPI - ESAPI.encoder()

TIME FRAME

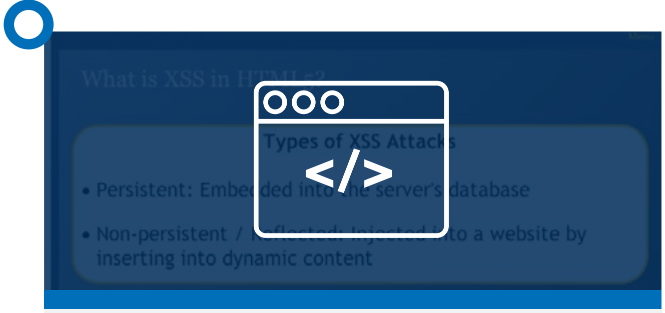
- (8) Modules – 120 min total

Developer:
Web 2.0 Secure Coding

The buzzword "Web 2.0" has been in the public vocabulary for years. As HTML5 and other new 2.0 technologies become widely implemented and draw closer to maturity, attackers are focusing their attention on finding exploits and attacking Web 2.0 services, technologies and languages. This program teaches developers how to avoid common pitfalls and follow best practices in six courses that total 45 minutes in length.

Course Outline

- AJAX / XML / JSON in Web 2.0
- Cross-origin resource sharing
- Local storage
- Web messaging
- WebSocket protocol
- XSS in HTML5



What is XSS in HTML5?

Types of XSS Attacks

- Persistent: Embedded into the server's database
- Non-persistent / Reflected: Injected into a website by inserting into dynamic content

TIME FRAME

- (6) Modules – 45 min

Get in Touch >

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896 | www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.