eLearning Course Catalog

Cybersecurity Education Services

Optiv eLearning courses are licensed based upon the service tier of the engagement. This graphic shows the course types that are licensed for each tier and the remainder of this guide outlines the exact course titles that are available. The portfolio of courses is continuously being updated with new versions and new content.

- **Basic**
  - Video-based Courses
    - Optiv-Hosted Only

- **Core**
  - +General End User Awareness Training
    - Optiv-Hosted or Client-Hosted
  - +Role-based Training
    - Optiv-Hosted or Client-Hosted

- **Total**
  - +Developer Training
    - Optiv-Hosted or Client-Hosted

- **Advanced**
  - Optiv eLearning courses are licensed based upon the service tier of the engagement. This graphic shows the course types that are licensed for each tier and the remainder of this guide outlines the exact course titles that are available. The portfolio of courses is continuously being updated with new versions and new content.
# SECURITYBYTES VIDEO-BASED COURSES

The purpose of Optiv’s SecurityBytes video-based courses is to provide Clients with the opportunity to provide just-in-time training when an end user fails a simulated phishing campaign. These courses are available with Optiv-hosted engagements. The courses are comprised of 60- to 90-second videos with a 3-question quiz.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Voiceover: Yes</td>
<td>Voiceover: Yes</td>
<td>Voiceover: Yes</td>
</tr>
<tr>
<td>Quiz Questions: 3</td>
<td>Quiz Questions: 3</td>
<td>Quiz Questions: 3</td>
</tr>
</tbody>
</table>

Available Courses:
- Business Travel
- Cloud Security
- Cybersecurity at Home
- Data Privacy
- Email Security
- Identity Theft
- Information Protection
- Insider Threat
- Malicious Downloads
- Mobile Security
- Password Security
- Ransomware
- Social Engineering
- Social Media
- Workplace Security

Available Courses:
- Business Travel
- Cloud Security
- Cybersecurity at Home
- Data Privacy
- Email Security
- Identity Theft
- Insider Threat
- Malicious Downloads
- Mobile Security
- Password Security
- Social Engineering
- Social Media
- Workplace Security

Available Courses:
- Attacks on Smartphones
- Business Email Compromise
- Credential Theft
- Malware Classifications
- Malware Infections
- Phishing Attachments
- Phishing Links and Notifications
- Ransomware
- Spear Phishing
- Spoofing
- Spyware Infections
- VPN
- Wire Transfer Fraud
## GENERAL END USER AWARENESS

The goal of Optiv's General End User Awareness training courses is to arm employees with the knowledge and skills they need to protect their organization. Optiv offers different portfolios of courses that resonate with different organizational audiences and populations.

<table>
<thead>
<tr>
<th>Rapid Awareness</th>
<th>CyberBOT® Security Awareness Training</th>
<th>Security Awareness Circuit Training</th>
<th>Unpack the Hack</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Microlearning</td>
<td>• Interactive</td>
<td>• Immersive</td>
<td>• Game-based</td>
</tr>
<tr>
<td>• Informative with basic interactions</td>
<td>• Linear path to learning</td>
<td>• Branched paths of learning based upon user decisions</td>
<td>• Interactive and covering several cybersecurity awareness concepts.</td>
</tr>
<tr>
<td>• Fully responsive</td>
<td>• End users are taught concepts upfront and then given opportunities to practice what they have learned.</td>
<td>End users learn by navigating through real-world scenarios and reviewing the consequences of their actions.</td>
<td>Users will have varying experiences in the game as the culprit and clues in each game differ.</td>
</tr>
<tr>
<td>Linear path of content delivery</td>
<td>Courses touch on multiple topics with a mix of knowledge-based and behavior-based scenarios.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mixture of Illustrations and Photos</th>
<th>Illustrated</th>
<th>Photo-real</th>
<th>Illustrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three multiple choice questions</td>
<td>Five questions from a bank of ten</td>
<td>Five questions from a bank of ten</td>
<td>No formal assessment</td>
</tr>
<tr>
<td>Voiceover: No</td>
<td>Voiceover: Yes</td>
<td>Voiceover: Yes</td>
<td>Voiceover: Yes</td>
</tr>
<tr>
<td>&lt;5 minutes</td>
<td>10-15 minutes</td>
<td>10-15 minutes</td>
<td>20-30 minutes</td>
</tr>
<tr>
<td>Pass Rate: 100%</td>
<td>Pass Rate: 80%</td>
<td>Pass Rate: 80%</td>
<td>Pass Rate: Completion is marked once user submits their suspect for confirmation.</td>
</tr>
</tbody>
</table>
## CORE TIER

### GENERAL END USER COURSES

#### Rapid Awareness
- Attacks on Smartphones
- Bring Your Own Threat (BYOT)
- Business Email Compromise
- Business Travel
- Cloud Basics
- Cloud Security
- Cloud Threat Actors
- Coordinated Phishing and Vishing Attacks
- Cyber Threat Actors
- Cybersecurity at Home
- Data Privacy
- Digital Hygiene
- Email Security
- Encryption Basics I
- Encryption Basics II
- Hybrid Threat Actors
- Identity Theft
- Insider Threat
- Internet of Things
- Malicious Downloads
- Malware Basics
- Malware Impact
- Mobile Security
- Multifactor Authentication
- Password Security
- Phishing Attachments
- Phishing Links
- Phishing Notifications
- Ransomware Basics
- Ransomware in the Workplace
- Remote Worker Security
- Safe Data Handling
- Social Engineering
- Social Engineering Threat Actors
- Social Media
- Spear Phishing
- Spoofed Phishing Emails
- Spyware
- Video Conferencing Security
- Vishing Explained
- Wire Transfer Fraud
- Workplace Security

#### CyberBOT® Security Awareness Training
- Business Travel
- Cloud Security
- Cybersecurity at Home
- Data Privacy
- Email Security
- Identity Theft
- Insider Threat
- Malicious Downloads
- Mobile Security
- Password Security
- Social Engineering
- Social Media
- Workplace Security
- New Hire
- Refresh

#### Security Awareness Circuit Training
- Business Travel
- Cloud Security
- Cybersecurity at Home
- Data Privacy
- Email Security
- Identity Theft
- Insider Threat
- Malicious Downloads
- Mobile Security
- Moment of Compromise
- Password Security
- Social Engineering
- Social Media
- Workplace Security
- New Hire
- Refresh

#### Unpack the Hack
- Defending Daybreak
TOTAL TIER

ROLE-BASED ELEARNING COURSES

The goal of Optiv’s Role-Based Awareness courses is to educate employees on security-aware behaviors specific to their role. Depending on the nature of the company, all employees may have a specialized role and would benefit from the applicable training.

Courses align with common compliance-related training obligations and/or security concerns related to specific responsibilities or positions within organizations.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Components</th>
<th>Voiceover</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>California Consumer Privacy Act (CCPA)</td>
<td>One course</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course introduces end users to the requirements and obligations of the Act as well as highlighting the limited allowed exceptions and penalties related to the Act.</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>Eight courses</td>
<td>No</td>
<td>15-30 minutes</td>
<td>These courses are designed for security professions or users with privileged access who work with the cloud. Courses include: Cloud Computing, Commonly Used Cloud Services &amp; Risks, Configuration Management in the Cloud, Container, Kubernetes &amp; Serverless Computing, IAM in the Cloud, Securing Data in the Cloud: Logging, Monitoring &amp; Storage, Securing the CI/CD Pipeline, Zero Trust.</td>
</tr>
<tr>
<td>Credit Card Handling</td>
<td>One course with four tracks: call center, table service, quick serve, management</td>
<td>Yes</td>
<td>20 minutes</td>
<td>Employees who handle credit cards on a daily basis are the first stop when it comes to data security. Educate them on credit card handling best practices and why they matter.</td>
</tr>
<tr>
<td>Detection &amp; Response Solutions</td>
<td>One course</td>
<td>No</td>
<td>15-20 minutes</td>
<td>Due to the evolving needs of threat detection and response, demand has shifted from traditional threat monitoring towards more advanced detection and response solutions like MDR, XDR, NDR and EDR.</td>
</tr>
<tr>
<td>Digital Risk Protection Management</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>Digital Risk Protection Management (DRPM) is a proactive intelligence solution that identifies, manages and remediates risks outside of an organization’s environment by monitoring its unique digital footprint.</td>
</tr>
<tr>
<td>Executive Insights</td>
<td>Four courses covering individual topics</td>
<td>No</td>
<td>5-7 minutes each</td>
<td>As a prime target for cybercrime, it’s imperative that executives are aware of the vulnerabilities specific to their position. These four courses cover threat actors, business information, social media and public data.</td>
</tr>
<tr>
<td>General Data Protection Regulation (GDPR)</td>
<td>One stand-alone overview course; Seven deep-dive courses</td>
<td>Yes</td>
<td>15 minutes 5-10 minutes each</td>
<td>For companies affected by GDPR, this course provides end users an overview of the regulation and how it may affect their daily tasks.</td>
</tr>
<tr>
<td>HIPAA Privacy and Security Basics</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>This course covers topics specific to end users that handle data covered by HIPAA, such as covered entities, business associates and PHI.</td>
</tr>
<tr>
<td>Incident Management</td>
<td>Four courses</td>
<td>No</td>
<td>5-30 minutes each</td>
<td>Proactive strategies can be critical when incidents arise. These four courses present an incident management framework for assembling teams and policies using a proactive approach.</td>
</tr>
<tr>
<td>Subject</td>
<td>Components</td>
<td>Voiceover</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Introduction to PCI</td>
<td>One course</td>
<td>Yes</td>
<td>10-15 minutes</td>
<td>Educate employees about the Payment Card Industry (PCI), how to interact with its regulations, the penalties for not complying and the types of data they can and cannot store.</td>
</tr>
<tr>
<td>MITRE ATT&amp;CK® Framework</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>The MITRE ATT&amp;CK® framework is a powerful resource used by cybersecurity professionals to better understand threat actor behavior before, during and after attacks. This course describes components of the framework and outlines its various use cases.</td>
</tr>
<tr>
<td>OWASP IoT Top 10</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>The adoption of internet of things (IoT) technology is a trend that continues to grow. Unfortunately, there are few standards in place for IoT security. This course highlights common IoT security issues.</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Seven courses</td>
<td>No</td>
<td>10-20 minutes each</td>
<td>This series is designed to increase awareness of the current PCI standard 3.2.1 and its various requirements for leaders, developers and service personnel.</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>One course</td>
<td>No</td>
<td>5 minutes</td>
<td>This course provides an overview of techniques used in penetration testing to identify potential security vulnerabilities.</td>
</tr>
<tr>
<td>Personal Information Protection and Electronic Documents Act (PIPEDA)</td>
<td>One course</td>
<td>Yes</td>
<td>15 minutes</td>
<td>For companies affected by PIPEDA, this course provides end users an overview of the regulation and how it may affect their daily tasks.</td>
</tr>
<tr>
<td>Protecting Privacy in Customer Service Roles</td>
<td>One course</td>
<td>No</td>
<td>10 minutes</td>
<td>Designed for individuals in customer-facing roles, this course outlines specific risks and best practices for protecting customer information in person, online and on the phone.</td>
</tr>
<tr>
<td>Security Awareness for Users with Privileged Access</td>
<td>Ten courses</td>
<td>No</td>
<td>5 minutes each</td>
<td>The security of networks and devices grows more challenging with each new technology or threat. These courses cover ten important security topics relevant to administrators or elevated access users.</td>
</tr>
<tr>
<td>SIEM Management Best Practices</td>
<td>One course</td>
<td>No</td>
<td>15-20 minutes</td>
<td>Security Information and Event Management (SIEM) is a security tool that consolidates and correlates data from multiple sources to help security teams detect and respond to threats. Unfortunately, a poorly configured SIEM can be ineffective. As such, this course examines best practices for optimizing SIEM as a cybersecurity tool.</td>
</tr>
<tr>
<td>Third-Party Risk Management Basics</td>
<td>One course</td>
<td>Yes</td>
<td>15 minutes</td>
<td>Risks introduced by third-party business relationships can present a significant threat. This course describes a lifecycle for recognizing, prioritizing and reducing risks introduced by these relationships.</td>
</tr>
<tr>
<td>Understanding Cyber Risk Management</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>Managing cyber risk is a critical component in any organization’s security program. This course examines the differences between risks, threats and vulnerabilities and outlines the risk management ecosystem for a deeper understanding of risk components.</td>
</tr>
<tr>
<td>Understanding SecOps</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>SecOps is a collaborative strategy between security and operations teams to prevent, detect and respond to attacks, intrusions and threats. This course defines the roles and models used with SecOps and how they contribute to improved security visibility.</td>
</tr>
<tr>
<td>Understanding Threat Management</td>
<td>One course</td>
<td>No</td>
<td>15-20 minutes</td>
<td>Threat management is a proactive strategy to identify vulnerabilities, assess threats, prevent attacks and prepare for incidents. This course defines threat management and explores processes and characteristics of effective programs.</td>
</tr>
</tbody>
</table>
### ADVANCED TIER

## DEVELOPER TRAINING

The goal of Optiv's Developer courses is to provide advanced, focused training on specific security concerns related to the development of applications, websites and APIs.

This course library offers training specific to commonly used programming languages as well as language-agnostic topics.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Components</th>
<th>Voiceover</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>Eight courses</td>
<td>No</td>
<td>10-15 minutes each</td>
<td>Improving the security of applications is paramount. These courses present strategies for protecting applications during development and once deployed.</td>
</tr>
<tr>
<td>OWASP API Top 10</td>
<td>One course</td>
<td>No</td>
<td>10 minutes</td>
<td>APIs are an increasingly common way to connect systems and services. This course highlights common API security mistakes and secure coding practices.</td>
</tr>
<tr>
<td>OWASP Mobile Top 10</td>
<td>One course with ten different topics</td>
<td>No</td>
<td>20 minutes</td>
<td>Developers must keep security best practices at the forefront as they develop the next generation of mobile applications. Educate your developers on important security topics.</td>
</tr>
<tr>
<td>OWASP Proactive Controls</td>
<td>One single course</td>
<td>No</td>
<td>15 minutes</td>
<td>Complementing the risk mitigation focus of OWASP Web/Mobile Top 10, these controls contribute to an informed foundation for the secure development process.</td>
</tr>
<tr>
<td>OWASP Top 10</td>
<td>One course with ten different topics or ten separate courses</td>
<td>No</td>
<td>60 minutes</td>
<td>This course explores each of the top 10 most critical security risks to web applications as outlined by the OWASP community.</td>
</tr>
<tr>
<td>Privacy by Design</td>
<td>One course</td>
<td>No</td>
<td>5 minutes</td>
<td>Privacy by design requires designers and developers to consider privacy implications in development planning. This course highlights considerations for protecting the privacy of data.</td>
</tr>
<tr>
<td>Secure Coding Java/.NET/Python</td>
<td>Four Java courses Four .NET courses Four Python courses</td>
<td>No</td>
<td>15 minutes each</td>
<td>Educate your Java, .NET and Python developers on topics such as input validation, output encoding, error handling and SQL injection defense.</td>
</tr>
<tr>
<td>Web 2.0 Secure Coding</td>
<td>Six courses</td>
<td>No</td>
<td>5-10 minutes each</td>
<td>Each of the topics covered helps developers learn how to avoid common pitfalls and how to follow best practices for HTML5 development.</td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>One course</td>
<td>No</td>
<td>15 minutes</td>
<td>Integrating effective threat modeling practices provides developers a consistent avenue for addressing their obligation to secure systems and data within a project.</td>
</tr>
</tbody>
</table>
FOR SECONDARY-LEVEL EDUCATIONAL INSTITUTIONS

ACADEMIC CYBERBOT

Cyber threats targeting educational institutions and their populations are increasingly common. The Academic CyberBOT program combines instruction for both students and school staff with six courses for students in secondary grades and two courses to assist staff in understanding data privacy and workplace security within school environments.

This program includes the courses listed below.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Components</th>
<th>Voiceover</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic CyberBOT Cyber Threat Actors</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course defines the four types of cyber threat actors, describes how they carry out attacks and explains the motivations behind their actions.</td>
</tr>
<tr>
<td>Academic CyberBOT Email Security</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This interactive course engages learners in recognizing common characteristics of phishing emails and respond appropriately.</td>
</tr>
<tr>
<td>Academic CyberBOT Password Security</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course outlines steps for creating strong passwords as well as ongoing best practices for keeping credentials secure.</td>
</tr>
<tr>
<td>Academic CyberBOT Mobile Security</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course examines how malicious apps, SMiShing, insecure WiFi and device theft threaten smartphones and tablets and presents actionable steps to reduce risks.</td>
</tr>
<tr>
<td>Academic CyberBOT Social Media Security</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course explores how oversharing, inadequate privacy settings, malicious links and unsafe apps on social media put personal information at risk.</td>
</tr>
<tr>
<td>Academic CyberBOT Cyber Security Outside of School</td>
<td>Students</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course reviews how vulnerabilities in public spaces and at home can create security risks and examines how up-to-date software, secure connections and safe browsing can combat this.</td>
</tr>
<tr>
<td>Academic CyberBOT Workplace Security for Educators</td>
<td>Staff</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course details methods used by cybercriminals to enter school facilities or remotely access school data and best practices for a secure workplace.</td>
</tr>
<tr>
<td>Academic CyberBOT Data Privacy for Educators</td>
<td>Staff</td>
<td>Yes</td>
<td>15 minutes</td>
<td>This course examines unintentionally negligent behaviors that put data at risk and recommends best practices to avoid inadvertent exposure of sensitive student and staff information.</td>
</tr>
</tbody>
</table>