COURSE CATALOG

Security Awareness Training

PHISHINGBOX

Contents

OVERVIEW 4

CORE TIER 5

CyberBOT® Course Descriptions 6

CyberBOT Cloud Security 6
CyberBOT Data Privacy 6
CyberBOT Email Security 6
CyberBOT Identity Theft 6
CyberBOT Insider Threat 6
CyberBOT Malicious Downloads 6
CyberBOT Mobile Security 7
CyberBOT Password Security 7
CyberBOT Social Engineering 7
CyberBOT Social Media Security 7
CyberBOT Workplace Security 7

Security Awareness Circuit Training Course Descriptions 8

SACT Cybersecurity at Home 8
SACT Data Privacy 8
SACT Email Security 8
SACT Identity Theft 8
SACT Insider Threat 8
SACT Malicious Downloads 8
SACT Mobile Security 9
SACT Password Security 9
SACT Social Engineering 9
SACT Social Media Security 9
SACT Workplace Security 9

Rapid Awareness Course Descriptions 10

Rapid Awareness Attacks on Smart Phones 10
Rapid Awareness Business Email Compromise 10
Rapid Awareness Coordinated Phishing and Vishing Attacks .. 10
Rapid Awareness Cybersecurity at Home 10
Rapid Awareness Data Privacy 10
Rapid Awareness Digital Hygiene 10
Rapid Awareness Email Security 11
Rapid Awareness Malicious Downloads 11
Rapid Awareness Phishing Attachments 11
Rapid Awareness Phishing Links 11
Rapid Awareness Phishing Notifications 11
Rapid Awareness Ransomware Basics 11
Rapid Awareness Ransomware in the Workplace 11
Rapid Awareness Remote Worker Security 12
Rapid Awareness Safe Data Handling 12
Rapid Awareness Social Engineering 12
Rapid Awareness Social Media Security 12
Rapid Awareness Spear Phishing 12
Rapid Awareness Spoofed Phishing Emails 12
Rapid Awareness Wire Transfer Fraud 12
Rapid Awareness Workplace Security 13

TOTAL TIER 14

Role-Based Course Descriptions 14

Commonly Used Cloud Services & Risks 14
Credit Card Handling 14
HIPAA Privacy and Security Basics 14
Introduction to PCI 14
Protecting Privacy in Customer Service Roles 14
The GDPR: An Overview 15
Third-Party Risk Management Basics 15

Role-Based Course Collections 15

Executive Insights 15

Executive Insights Introduction 15
Executive Insights Business Information 15
Executive Insights Public Data 15
Executive Insights Social Media 16

Incident Management 16

Section 1: Introduction to Incident Management 16
Section 2: Team Mechanics 16
Section 3: Operations Support 16
Section 4: Handling Incidents 16

Security Awareness for Users With Privileged Access 16

Privileged Access: Antivirus & Antimalware 16
Privileged Access: Bluetooth Attacks & Mobile Security 17
Privileged Access: Credential Theft Prevention 17
Privileged Access: Firewalls 17
Privileged Access: IDS & IPS 17
Privileged Access: Logging & Monitoring 17
Privileged Access: Preventing IoT Vulnerabilities 17
Privileged Access: Server Security & Patch Management 17
Privileged Access: Social Engineering Prevention 17
Privileged Access: Workstation Security 17

ADVANCED TIER 18

Developer Course Descriptions 18

OWASP API Top 10 18
OWASP Mobile Top 10 18

OWASP Proactive Controls 18
Privacy by Design 18
Threat Modeling 18
Developer Course Collections **19**
Application Security **19**
Application Security: Client-Side Logic Manipulation 19
Application Security: Command Injection 19
Application Security: Cross-Site Request Forgery 19
Application Security: Cross-Site Scripting 19
Application Security: Data Modification 19
Application Security: Forceful Browsing 19
Application Security: Information Leakage 19
Application Security: Session Hijacking 19
OWASP Top 10 .... **20**
Introduction to OWASP 20
OWASP Top 10: Injection #1 20
OWASP Top 10: Broken Authentication #2 20
OWASP Top 10: Sensitive Data Exposure #3 20
OWASP Top 10: XML External Entities #4 20
OWASP Top 10: Broken Access Control #5 20
OWASP Top 10: Security Misconfiguration #6 20
OWASP Top 10: Cross-Site Scripting #7 20
OWASP Top 10: Insecure Deserialization #8 21
OWASP Top 10: Components with Known Vulnerabilities #9... 21
OWASP Top 10: Insufficient Logging and Monitoring #10 21

OVERVIEW

Plan, build and run a holistic security awareness program that meets your organization's unique needs and resonates with diverse user populations. Optiv's Security Awareness Training provides interactive, engaging and relevant options to increase awareness of the specific security concerns facing members of your team.

Optiv offers three service tiers to align with the varying levels of training complexity among organizations and the user populations within them. With a wide array of course portfolios and topics within each tier, you can tailor a program that's as simple or intricate as your organization requires.

	Core	Total	Advanced
Free Courses	5	5	5
General End User Awareness Courses	50	50	50
Role-Based Courses	0	25	25
Developer Courses	0	0	25
Newsletters (Topic-Based)	12	12	12
Digital Images	50	50	50
Total Courses	**55**	**80**	**105**

Supplemental Training Material:

Supplemental training materials are included with Core, Total and Advanced tiers of service. These supplemental training materials include:

- **Posters/Digital Images:** Optiv's topic-aligned posters/digital images are a great visual reminder of key points from the courses. Images may be printed to use within an organization's facilities, sent via email to end users, posted on internal social media platforms or implemented as screensaver or lock screen images on users' devices. Images are provided in JPEG or PDF format.
- **Newsletters:** Newsletters are an avenue to communicate important information around security awareness to your employee base. There are several ways to utilize newsletters, including digital delivery via email or link to the newsletter in corporate communications, hosting on an internal website, printing and making available in common areas like break rooms, cafeterias or copy rooms or providing a print copy to each employee for use as a desk-drop. Newsletters are provided in PDF format.

CORE TIER

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 that resonate with different organizational audiences and populations.

Rapid Awareness	CyberBOT®	Security Awareness Circuit Training	SecurityBytes
Style: • Micro-learning • Informative with basic interactions • Fully responsive	**Style:** • Interactive • Linear path to learning • End users are taught concepts up front and given opportunities to practice	**Style:** • Immersive • Branched paths of learning based upon user decisions	**Style:** • Nano-learning • Non-interactive • Designed for just-in-time training for failed phishing simulations
Content: Linear path of content delivery.	**Content:** Courses touch on multiple topics, with a mix of knowledge-based and behavior-based scenarios.	**Content:** End users learn by navigating through real-world scenarios and reviewing consequences of their actions.	**Content:** Short, video-based training on focused topics.
Visual Style: Illustrated and photo-real	**Visual Style:** Illustrated	**Visual Style:** Photo-real	**Visual Style:** Illustrated and photo-real
Assessment: Three-question quiz	**Assessement:** Five-question quiz	**Assessement:** Five-question quiz	**Assessement:** Three-question quiz
Voiceover: Yes	**Voiceover:** Yes	**Voiceover:** No	**Voiceover:** Yes
Length: <5 minutes	**Length:** 10-15 minutes	**Length:** 10-15 minutes	**Length:** 60-90 seconds
Passing Score: 100%	**Passing Score:** 80%	**Passing Score:** 80%	**Passing Score:** 100%
Courses Included: • Remote Worker Security Awareness *(Free)* • Attacks on Smart Phones • Business Email Compromise • Coordinated Phishing & Vishing Attacks • Data Privacy • Digital Hygiene • Email Security • Malicious Downloads • Phishing Attachments • Phishing Links • Phishing Notifications • Ransomware Basics • Ransomware in the Workplace • Safe Data Handling • Social Engineering • Social Media • Spear Phishing • Spoofed Phishing Emails • Wire Transfer Fraud	**Courses Included:** • Cloud Security *(Free)* • Data Privacy • Email Security • Identity Theft • Malicious Downloads • Mobile Security • Password Security • Social Engineering • Social Media • Workplace Security	**Courses Included:** • Malicious Downloads *(Free)* • Cybersecurity at Home • Data Privacy • Email Security • Identity Theft • Insider Threat • Mobile Security • Password Security • Social Engineering • Social Media • Workplace Security	**Courses Included:** • Ransomware *(Free)* • Business Email Compromise • Credential Theft • Data Privacy • Email Security • Malicious Downloads • Phishing Attachments • Phishing Links & Attachments • Ransomware • Social Engineering • Spear Phishing • Spoofing • Wire Transfer Fraud

CyberBOT® Course Descriptions

Course Name	Course Description	Course Objectives	Time	Audience
CyberBOT Cloud Security (FREE COURSE)	The Masterminds have high hopes as they deploy the CyberBOTs into the cloud. Users must ensure they use only safe and approved cloud services, adequately secure data stored in the cloud and comply with their organization's cloud-based application policies to complete their mission to battle the CyberBOTs in the cloud.	• *Define "the cloud" and basic characteristics of cloud services* • *Explain what is appropriate to store in the cloud* • *Avoid common mistakes when using cloud storage and applications*	10-15 minutes	All employees and contractors
CyberBOT Data Privacy	CyberBOTs are targeting the organization's data and it's up to users to secure it against compromise. Learners explore the risk factors and best practices related to collecting, processing, storing and disposing of data as they complete missions to defeat each CyberBOT's attempt to steal sensitive information.	• *Recognize when data is considered personal information* • *Explain appropriate use and retention best practices* • *Explain best practices for collecting information and how to give notice*	10-15 minutes	All employees and contractors
CyberBOT Email Security	The CyberBOTs are at it again, this time using the tried-and-true phishing attack. Users must defeat the CyberBOTs' attempts to phish inboxes by recognizing phishing emails and detecting malicious links and attachments.	• *Filter potential phishing emails by the subject line and sender* • *Recognize common phishing signs* • *Avoid clicking links or attachments in suspicious emails*	10-15 minutes	All employees and contractors
CyberBOT Identity Theft	The CyberBOTs are seeking a new identity. End users and their customers/clients are at risk. Learners must protect their own personal information, as well as that of customers and clients. If the CyberBOTs are successful at stealing an identity, users must recognize the signs and respond appropriately to prevent further compromises.	• *Recognize the common signs of identity theft* • *Identify steps to prevent identity theft* • *Explain how identity theft can affect an organization*	10-15 minutes	All employees and contractors
CyberBOT Insider Threat	The Masterminds are sending CyberBOTs to seek out employees with an interest in harming the organization or those who are negligent for an insider threat attack. The CyberBOTs hope users won't recognize the signs and take the proper steps to report the threat.	• *Define an insider threat* • *Identify types of insider threats* • *Recognize suspicious behaviors and activities associated with insider threats*	10-15 minutes	All employees and contractors
CyberBOT Malicious Downloads	When the CyberBOTs begin sharing suspicious email attachments and links, users must learn to defend themselves against malicious downloads. Attacks carried out via phishing emails, malicious websites and malware require learners to raise their awareness of the risks, techniques and intentions of the CyberBOTs to complete each mission successfully.	• *Utilize best practices for safe web browsing* • *Recognize and avoid falling victim to scareware and ransomware attacks* • *Explain the importance of system/ software updates*	10-15 minutes	All employees and contractors

Course Name	Course Description	Course Objectives	Time	Audience
CyberBOT Mobile Security	While the CyberBOTs are on a mission to install malware on mobile devices, SMiSh unsuspecting victims and steal devices left unattended, learners are on their own mission to install safe mobile applications, recognize and respond to SMiShing attacks and keep devices secure along the way.	• *Install safe mobile applications* • *Recognize and avoid SMiShing attacks* • *Protect screens from on-lookers (data privacy, social engineering protection)*	10-15 minutes	All employees and contractors
CyberBOT Password Security	As the CyberBOTs attempt to crack passwords and gain unauthorized access to user accounts, learners discover methods for beating CyberBOTs at their own game. As part of the mission, users gain valuable knowledge about creating secure and unique passwords and how to further protect those passwords from the CyberBOTs' reach.	• *Create strong, unique passwords* • *Explain the importance of using a different password for each site/ application* • *Explain best practices related to protecting passwords*	10-15 minutes	All employees and contractors
CyberBOT Social Engineering	The Masterminds have designed undercover operations. As the CyberBOTs take on unusual disguises and methods, learners must explore the techniques and intentions of social engineers and defeat the CyberBOTs by detecting their in-person, phone (vishing) and social media attacks.	• *Recognize physical disguises social engineers use* • *Recognize how to prevent social engineering attacks* • *Recognize and combat vishing attacks*	10-15 minutes	All employees and contractors
CyberBOT Social Media Security	Nearly everyone has a social media profile today. The CyberBOTs are no exception as they scan social networks for opportunities to attack vulnerable users. Learners must succesfully defend their social media presence to complete their mission against these attacks.	• *Prevent disclosure of excessive information on social media* • *Avoid risky plug-ins and apps* • *Recognize malicious links on social media*	10-15 minutes	All employees and contractors
CyberBOT Workplace Security	CyberBOTs are attempting to infiltrate the workplace and it's up to users to keep them at bay. Whether it's gaining unauthorized physical access, stealing confidential information or installing malicious devices on the organization's network, the CyberBOTs will keep learners on their toes throughout this mission.	• *Prevent unauthorized access to physical locations* • *Recognize the benefits of keeping a secure and clean workspace* • *Describe risks of using unapproved devices on organization networks*	10-15 minutes	All employees and contractors

Security Awareness Circuit Training Course Descriptions

Course Name	Course Description	Course Objectives	Time	Audience
SACT Cybersecurity at Home	Security risks are not limited to the workplace. In a technology-driven society, threats within the home are just as relevant and concerning as those in the office. This course examines common security issues within a home environment, including WiFi network security, home networking threats, vishing attacks and safe storage and disposal of personal information.	• *Secure a home wireless network* • *Explain best practices in handling vishing attempts and contacts from unknown callers* • *Explain risks of posting information to social media and accepting connection requests from strangers*	10-15 minutes	All employees and contractors
SACT Data Privacy	Protecting organizational data is a shared responsibility among all members of the workforce. The SACT Data Privacy course explores risk factors and best practices related to collecting, processing, storing and disposing of sensitive data. Learners will consider their role in the data lifecycle and how it relates to overall organizational data protection strategies.	• *Recognize when data is considered personal information* • *Explain appropriate use and retention best practices* • *Explain best practices for collection of information and how to give proper notice*	10-15 minutes	All employees and contractors
SACT Email Security	This course examines various types of threats related to phishing emails. Users learn how to recognize and address phishing emails, review messages for potential signs of phishing and comprehend the risks of interacting with malicious email content.	• *Filter potential phishing emails by the subject line and sender* • *Recognize common phishing signs* • *Avoid clicking links or attachments in suspicious emails*	10-15 minutes	All employees and contractors
SACT Identity Theft	Identity theft affects employees and customers on a personal level, but organizations are also directly affected when an employee's or customer's identity is stolen. This course defines identity theft and shares common indicators and what users can do to protect their personal information as well as that of customers.	• *Recognize common signs of identity theft* • *Identify steps to prevent identity theft, personally and for customers* • *Explain how identity theft can affect an organization*	10-15 minutes	All employees and contractors
SACT Insider Threat	Security threats from those associated with an organization often carry the greatest risks. Easy access to data by insiders is a significant threat. This course reviews these threats and shares indicators employees should know to prevent, stop and report insider threats.	• *Define an insider threat* • *Identify types of insider threats* • *Recognize suspicious behaviors and activities associated with insider threats*	10-15 minutes	All employees and contractors
SACT Malicious Downloads (FREE COURSE)	Malicious file downloads are a direct threat to organizational devices and systems. As such, the SACT Malicious Downloads course increases user awareness regarding the risks, techniques and motivations behind attacks using malicious downloads, including email attachments, malware and malicious links and websites.	• *Use best practices when browsing* • *Recognize and avoid falling victim to scareware and ransomware attacks* • *Explain the importance of system/ software updates*	10-15 minutes	All employees and contractors

Course Name	Course Description	Course Objectives	Time	Audience
SACT **Mobile Security**	This course guides users through best practices they can employ to reduce risks related to mobile devices. The course can help learners understand how to identify and use safe mobile applications, recognize text message (SMiShing) attacks, safely use mobile devices in shared spaces and prevent device theft.	• *Install safe mobile applications* • *Recognize and avoid SMiShing attacks* • *Protect screens from on-lookers (data privacy, social engineering protection)*	10-15 minutes	All employees and contractors
SACT **Password Security**	Almost any end user will use some type of work-related account which requires a password. As such, the this course shares practical skills for creating secure passwords, protecting passwords from compromise and securing credentials on multiple accounts.	• *Create strong, unique passwords* • *Explain the importance of using unique, secure passwords* • *Define best practices related to protecting passwords*	10-15 minutes	All employees and contractors
SACT **Social Engineering**	The SACT Social Engineering course explores the techniques and intentions of social engineers during in-person, phone (vishing) and social media interactions. Since social engineering attacks can occur anywhere, this course examines attack vectors both within and outside the workplace.	• *Identify common physical disguises used by social engineers* • *Describe how to prevent social engineering attacks* • *Recognize vishing, social media threats and risks outside the office*	10-15 minutes	All employees and contractors
SACT **Social Media Security**	While social media can be a valuable communication tool when used appropriately, the risks of overexposure and threats from social engineers and malicious links present on social networks can be troublesome for users and organizations. The SACT Social Media Security course reviews these risks and provides best practices for sharing safely on social media.	• *Prevent disclosure of excessive personal or company information on social media* • *Avoid fake plug-ins and apps within social media platforms* • *Avoid clicking on malicious links within social media platforms*	10-15 minutes	All employees and contractors
SACT **Workplace Security**	The SACT Workplace Security course delves into threats affecting the workplace environment and users' responsibilities to protect organizational infrastructure and data against compromise. Topics covered include physical access by unauthorized persons, secure workspaces, unauthorized devices and shared responsibility across the workforce.	• *Prevent unauthorized individuals from physically accessing facilities* • *Recognize benefits of keeping a secure and clean workspace* • *Summarize risks of using unauthorized devices on the company's network*	10-15 minutes	All employees and contractors

Rapid Awareness Course Descriptions

Course Name	Course Description	Course Objectives	Time	Audience
Rapid Awareness Attacks on Smart Phones	Smart phones are a growing target for cyberattackers as their features, operating systems and data storage capabilities evolve. The Rapid Awareness Attacks on Smart Phones course explores mobile devices and how they are targeted by cybercriminals through vishing phone calls, SMiShing messages and malicious apps.	• *Identify common threats for mobile devices* • *Recognize signs of vishing and SMiShing* • *Download safe applications from trusted sources*	5 minutes	All employees and contractors
Rapid Awareness Business Email Compromise	Business email compromise is a highly-sophisticated phishing threat that cost organizations in the United States more than $12 billion in the last decade. The Rapid Awareness Business Email Compromise course reveals common warning signs of these attacks, potential data and financial targets and tips for identifying and responding to potential attacks.	• *Describe why organizational funds and data are targets of BEC attacks* • *Identify common characteristics of BEC attacks* • *Respond appropriately to messages requesting payment, wire transfers or the release of sensitive data*	5 minutes	All employees and contractors
Rapid Awareness Coordinated Phishing and Vishing Attacks	While phishing emails and vishing calls are separate distinct threats, they are increasingly combined into coordinated attacks that appear more legitimate and enticing to end users. This course examines how cybercriminals utilize these combined techniques and how users can protect themselves before, during and after a combined phishing and vishing attack attempt.	• *Review phishing emails with phone numbers for signs of an attack* • *Respond appropriately to a combined phishing and vishing attack attempt* • *Explain the steps which occur during a combined attack*	5 minutes	All employees and contractors
Rapid Awareness Cybersecurity at Home	The Rapid Awareness Cybersecurity at Home course highlights the common threats and prevention strategies that affect users on home wireless networks, personal devices and phishing, vishing and SMiShing attacks at home. Users will learn how to protect against cyber threats outside the office.	• *Define common security risks within a home environment* • *Review strategies for protecting home networks and devices* • *Explain how to respond to phishing, vishing and SMiShing*	5 minutes	All employees and contractors
Rapid Awareness Data Privacy	The Rapid Awareness Data Privacy course assists users in properly handling and storing data containing personal information, responding appropriately to data privacy incidents and securely handling organizational and customer data as they complete daily job functions.	• *Define personal information* • *Report and respond appropriately to suspected data privacy incidents* • *Collect, store and process data securely*	5 minutes	All employees and contractors
Rapid Awareness Digital Hygiene	Digital hygiene is comparable to physical hygiene. In the same way that poor personal hygiene habits can lead to poor health, the health of devices, networks and data is put at risk with poor security habits. This course provides an overview of security habits to implement as part of a regular digital hygiene routine.	• *Explain security best practices, both offline and online* • *Secure accounts and devices against compromise* • *Identify safe browsing habits on the web and social media*	5 minutes	All employees and contractors

Course Name	Course Description	Course Objectives	Time	Audience
Rapid Awareness Email Security	With a focus on phishing threats, the Rapid Awareness Email Security course can help defend organizational email against phishing attacks. Learners will explore methods used in phishing attempts, understand why it is important to report suspected phishing emails and review common indicators of phishing emails.	• *Explain what a phishing email is* • *Identify common characteristics within phishing email messages* • *Explain the importance of reporting suspected phishing emails to protect other users*	5 minutes	All employees and contractors
Rapid Awareness Malicious Downloads	The Rapid Awareness Malicious Downloads course provides a quick, concise overview of threats stemming from malicious file downloads. Learners quickly review types of malware, safe browsing practices and how to identify common sources of malicious downloads.	• *Define common types of malware* • *Review apps, attachments and URLs for signs of malicious content* • *Use safe browsing practices to avoid malicious downloads*	5 minutes	All employees and contractors
Rapid Awareness Phishing Attachments	Phishing emails don't always contain malicious links. Many have malicious attachments a user may open, installing malware or running malicious macro code. This course highlights the most common types of malicious attachments and how they can install keyloggers, ransomware, botnets and macro malware.	• *Review email attachments for unusual file types* • *Describe how malicious attachments can install malware* • *Identify types of malware that can be installed via common file types*	5 minutes	All employees and contractors
Rapid Awareness Phishing Links	The Rapid Awareness Phishing Links course uses a dual approach to help users avoid phishing scams. A review of phishing email characteristics is followed by an overview of best practices for examining the links within them for unsafe destinations.	• *Recognize characteristics of suspicous links in messages* • *Examine links to reveal destinations* • *Identify potentially malicious websites that may steal information*	5 minutes	All employees and contractors
Rapid Awareness Phishing Notifications	The sense of urgency and resulting panic from false email notifications can entice users to turn over login credentials or financial account information and open malicious attachments or links. With the information in this course, users will learn how these notifications elicit an emotional response and how to research and evaluate messages before reacting.	• *Recognize characteristics of false notifications* • *Review emails from familiar sources for signs of phishing* • *Avoid providing credentials or personal information in response to false notifications*	5 minutes	All employees and contractors
Rapid Awareness Ransomware Basics	Providing an introductory overview of ransomware threats inside and outside the office, this basics course explains sources of ransomware infections on mobile and non-mobile devices. Threats from malicious websites, phishing emails, social media posts, portable storage devices and mobile applications are identified.	• *Identify sources for potential ransomware infection* • *Describe how ransomware can affect data on a device* • *Recognize the signs that a device is infected with ransomware*	5 minutes	All employees and contractors
Rapid Awareness Ransomware in the Workplace	The Rapid Awareness Ransomware in the Workplace course examines ransomware-related threats to organizational devices, networks and data. Two common types, locker and crypto ransomware, are identified and users review how ransomware infections can spread across company networks.	• *Recognize signs of a ransomware infection* • *Describe differences between locker and crypto ransomware* • *Outline how ransomware spreads across organizational networks*	5 minutes	All employees and contractors

Course Name	Course Description	Course Objectives	Time	Audience
Rapid Awareness Remote Worker Security (FREE COURSE)	As the world shifts from on-premise to remote workforces, it is imperative that individual contributors practice secure behaviors relevant to work-from-home environments. This course provides users with general awareness for maintaining an organization's security when its workplace is everywhere.	• *Connect securely to organizational networks and applications* • *Maintain security during web and video conferences* • *Mitigate vulnerabilities of home workspaces*	10 minutes	All employees and contractors
Rapid Awareness Safe Data Handling	Organizations and their employees process significant amounts of internatl and external data each day. The Rapid Awareness Safe Data Handling course examines methods for protecting sensitive customer/client and organizational data. In addition to instructional content, users apply concepts in engaging practice scenarios.	• *Explain best practices related to data handling* • *Define types of sensitive customer and organization data* • *Analyze scenarios to identify methods for protecting data*	5 minutes	All employees and contractors
Rapid Awareness Social Engineering	As a concise introduction to social engineering methods, this course provides users with a high-level overview of tactics involved in this type of attack. Users gain knowledge regarding social engineering targets, the psychological manipulation employed and steps to identify and report social engineering attempts.	• *Explain methods used by social engineers* • *Identify common targets for social engineering* • *Recognize and respond correctly to social engineering attempts*	5 minutes	All employees and contractors
Rapid Awareness Social Media Security	The Rapid Awareness Social Media Security course covers the basics of using social media platforms securely, including safe sharing, best practices for privacy and security settings and identifying malicious links in posts and notifications.	• *Identify information that is safe to share via social media* • *Configure social media privacy settings to limit sharing* • *Avoid malicious social media links*	5 minutes	All employees and contractors
Rapid Awareness Spear Phishing	The targeted nature and amount of detail in spear phishing attacks can fool even the most savvy users. The Rapid Awareness Spear Phishing course helps to reduce these instances by making learners aware of how well-researched and highly-focused phishing attempts are designed to gain a sense of trust.	• *Summarize how spear phishing messages are tailored to users* • *Review senders of suspicious messages to identify the source* • *Describe how cybercriminals locate spear phishing targets*	5 minutes	All employees and contractors
Rapid Awareness Spoofed Phishing Emails	Spoofed emails are a specific types of phishing attack and appear to be sent by a familiar contact or source. The Rapid Awareness Spoofed Phishing Emails course reviews how email addresses are spoofed, signs a received message might be spoofed and how to respond if the user's email address is spoofed by another party.	• *Identify messages sent from spoofed email addresses* • *Explain how spoofing is different from account compromise* • *Define common sources used to locate email addresses for spoofing*	5 minutes	All employees and contractors
Rapid Awareness Wire Transfer Fraud	Wire transfer fraud and phishing emails often go hand-in-hand. This course reviews how a simple phishing email can result in significant financial loss to an organization. Users learn how email wire transfer fraud schemes are carried out, consequences of successful attacks and how to verify the legitimacy of requests.	• *Identify red flags in wire transfer fraud email attempts* • *Review requests for wire transfers or financial information* • *List methods other than email used for wire transfer fraud*	5 minutes	All employees and contractors

Course Name	Course Description	Course Objectives	Time	Audience
Rapid Awareness Workplace Security	Unauthorized workplace visitors, workspaces that reveal too much information and company network vulnerabilities threaten almost all workplaces. The Rapid Awareness Workplace Security course examines these risks and quick and easy methods to protect against them.	• *Recognize individuals accessing secure areas without authorization* • *Describe how to secure physical workspaces* • *Explain how approved devices and services protect company networks*	5 minutes	All employees and contractors

TOTAL TIER

Role-Based Training

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

Role-Based Course Descriptions

Course Name	Course Description	Course Objectives	Time	Audience
Commonly Used Cloud Services & Risks	Organizations utilizing the cloud have access to a variety of additional services that can enhance security, user experience and performance. Unfortunately, they can also introduce threats to the environment. This course examines six categories of common services, their related risks and best practices for their use.	• *Identify the six categories of common cloud services* • *Paraphrase one risk introduced by the services within each category* • *Describe best practices to mitigate services-related risks*	10-15 minutes	Cloud Administrators, IT Staff, Security Staff, Developers
Credit Card Handling	Credit card handlers need cardholder security awareness when conducting card-based transactions. By understanding the personally identifiable information contained on a credit card and how to secure it, credit card handlers can perform safer transactions. This course helps every entity type efficiently discover obligations for secure transactions.	• *List the personally identifiable information stored on a credit card* • *Locate the security features present on modern credit cards* • *Compare and contrast handling requirements for contact and contactless credit cards*	10-15 minutes	Credit Card Handlers
HIPAA Privacy and Security Basics	The Health Insurance Portability and Accountability Act requires businesses handling Electronic Patient Health Information to take steps to keep this data secure. This introductory course, presented in a framework of cybersecurity, is intended for general end users.	• *Define protected health information* • *Recognize entities covered by HIPAA* • *Identify key HIPAA requirements*	15 minutes	All employees and contractors of organizations required to comply with HIPAA
Introduction to PCI	The Intro to PCI course guides your users through the complicated world of the Payment Card Industry. The program educates employees with a wide, yet focused, range of knowledge that covers everything from identity theft and fraud to types of cardholder data and basic security guidelines.	• *Identify cardholder information that can be stored by an organization* • *Summarize the six objectives of the PCI Data Security Standards* • *Order the flow of cardholder data in a credit card transaction*	10-15 minutes	End users in organizations that are subject to PCI compliance
Protecting Privacy in Customer Service Roles	Individuals in customer service roles often collect or have access to a vast amount of customer information. This access can make employees in these roles a prime target for information theft. The Protecting Privacy in Customer Service Roles course outlines specific risks and best practices for protecting customer information in person, online and on the phone.	• *Paraphrase why customer service roles are targets for information theft* • *Analyze methods used to obtain customer information fraudulently* • *Restrate best practices to protect customer information*	10 minutes	All employees and contractors in customer-facing roles

Course Name	Course Description	Course Objectives	Time	Audience
The GDPR: An Overview	Organizations subject to GDPR requirements should ensure that all employees, regardless of their role in compliance, have a basic understanding of the regulation. As such, this concise overview course summarizes key obligations and data subject rights while highlighting individual employee contributions to compliance.	• *Paraphrase business obligations to comply with the GDPR* • *Recognize individual roles in complying with regulation requirements*	15 minutes	End user in organizations subject to GDPR compliance
Third-Party Risk Management Basics	Risks introduced into an organization by business relationships with vendors can be just as damaging and costly as internal risks. The Third-Party Risk Management Basics course describes a framework for organization to recognize, prioritize and reduce risks introduced to an organization by third parties.	• *Define third-party risk management and its lifecycle* • *Summarize the third-party risk management framework* • *Identify methods for classifying and tiering third-party risks*	15 minutes	Executives, Risk Managers, Finance, Supply Chain and Logistics, Systems Administrators, IT Staff

Role-Based Course Collections

Collection Name	Collection Description	Time	Audience
Executive Insights	Personal success and organizational access make an executive a uniquely attractive target of cybercriminals. This series is designed to improve awareness of the readily available information attackers can use to cause physical, cyber or financial harm to the executive or their organization.	20-32 minutes (4 5-8 minute courses)	Executives and Executive Support Staff

Course Name	Course Description	Course Objectives
Executive Insights Introduction	Certain categories of threat actors may focus their efforts on executives within an organization. Criminals of opportunity, hacktivists, competitors, state-sponsored actors and insider threats often target executive-level individuals specifically. This course introduces and explores common motivations and techniques used by these threat actors.	• *Identify types of threat actors that may target executives* • *Describe factors that motivate executive-focused efforts*
Executive Insights Business Information	Organizations often publish information about executives as a normal business practice. Executive biographies, speaking itineraries, press releases and social media often contain small details that a threat actor can combine and exploit. This course examines sources of organizationally-disclosed information and actionable steps to minimize exposure.	• *Recognize potential sources of publicly available executive information disclosed by organizations* • *Evaluate organizational processes and personal awareness to reduce exposure*
Executive Insights Public Data	While executives can exercise some level of control over the information disclosed by their organization, uncontrolled information sources like mass media, data aggregation sites, real estate data, educational information and social media can threaten privacy. This course reveals potential uncontrolled sources and methods for mitigating the risks they present.	• *Discover potential sources of uncontrolled information disclosure* • *Apply mitigation steps to reduce or respond to exposure by uncontrolled sources*

Course Name	Course Description	Course Objectives
Executive Insights Social Media	Social media can be a valuable tool for threat actors seeking the personal information of executives and other high-profile individuals. This course increases awareness of the risks presented by social media exposure and best practices related to privacy settings, location sharing and photo or video content.	• Review privacy settings on social media accounts to limit information visibility • Analyze personal social media profiles and posts to locate sources of sensitive information

Collection Name	Collection Description	Time	Audience
Incident Management	While many organizations take a reactive approach to incidents, true incident management involves proactive steps. The Incident Management program examines incident management best practices, including recommendations for assembling incident management teams, policy and planning considerations and a four-step process for incident handling.	70 minutes (4 5-30 minute courses)	Risk Management, IT Staff, Incident Management and Response Teams

Course Name	Course Description	Course Objectives
Section 1: Introduction to Incident Management	The main difference between incident response and incident management is the approach. Incident management involves proactive, well-planned steps to prepare for incidents. This course provides a brief introduction to incident management best practices as well as terminology and concepts detailed in subsequent courses.	• *Define the term "incident"* • *Summarize differences between incident response and incident management and benefits of each*
Section 2: Team Mechanics	Building a successful incident management capability within an organization requires a strong team effort. This course outlines the mechanics of assembling and preparing an incident management team poised to respond to incidents in a timely and effective manner.	• *Describe common team models utilized in incident management teams* • *Identify leadership and membership roles within an incident response team*
Section 3: Operations Support	Advanced planning and operational support allows organizations to transform reactive incident response measures into stronger proactive incident management capabilities. This course outlines how policies, plans and proper communication support an effective, well-designed approach.	• *Explain elements that should be present in incident response policies* • *Describe communication practices that support incident management*
Section 4: Handling Incidents	Once incident management preparations are in place, teams can move on to actually handling incidents. This course walks learners through the four-step incident response life cycle and provides relevant resources, including checklists and data sheets, that can be utilized prior to, during and after incident handling.	• *Outline the four-step incident handling lifecycle* • *Identify and assemble the resources needed to handle incidents effectively*

Collection Name	Collection Description	Time	Audience
Security Awareness for Users with Privileged Access	The security of networks and devices grows more challenging with each new technology or threat. This series covers 10 important security topics relevant to IT administrators or anyone with elevated access to an organization's infrastructure and data.	50 minutes (10 5 minute courses)	Systems Administrators, IT Staff, Users with Privileged Access

Course Name	Course Description	Course Objectives
Users with Privileged Access: Antivirus & Antimalware	Network environments are under constant threat from viruses and other types of malware. This course compares different forms of antivirus and antimalware technologies and their function in protecting networks and data. Best practices are recommended for configuring these applications in a network environment.	• *Contrast the three detection methods used by antivirus and antimalware* • *Summarize how antivirus/antimalware updates enhance network security*

Course Name	Course Description	Course Objectives
Users with Privileged Access: Bluetooth Attacks & Mobile Security	The mobile devices of users with privileged access are particularly vulnerable to attackers hoping to leverage elevated access to their advantage. This course examines the mobile information targeted by cybercriminals and methods for securing against common threats like Bluetooth exploits and device compromise.	• *Restate secure device settings for evading Bluetooth exploits* • *Describe methods to secure devices against theft, damage or compromise*
Users with Privileged Access: Credential Theft Prevention	The authorization rights to networks and sensitive files for users with privileged access makes their credentials a prime target for cybercriminals. This course reviews the most common attack methods for credential theft and best practices for credential requirements, policies and processes.	• *Identify two methods used by cybercriminals to steal user credentials* • *Categorize common user access credentials behaviors as secure or risky*
Users with Privileged Access: Firewalls	Protecting networks requires the use of security technologies, one of the most basic being firewalls. This course provides an in-depth look at the types of firewalls available and compares the functionality and level of security provided by each. Recommendations for firewall configuration best practices are also provided.	• *Generalize how firewalls examine data moving through networks* • *Compare the functionality and security provided by the five types of firewalls*
Users with Privileged Access: IDS & IPS	Intruder prevention and detection systems are tools for thwarting and discovering threats on a network. Understanding how they function supports good security decisions when building, provisioning and protecting network infrastructures. As such, this course analyzes these technologies in detail to reveal their security capabilities.	• *Distinguish between IDS and IPS and unified threat management* • *Summarize best practices when using IDS, IPS and UTM devices*
Users with Privileged Access: Logging & Monitoring	Log files and consistent monitoring allow privileged access users to check the health of networks and validate proper security protections are in place and functional. This course reviews appropriate logging and monitoring habits that can be used to evaluate network activity, identify inconsistencies and allow more efficient incident response.	• *Identify locations and activities that should be monitored in network environments* • *Describe three or more best practices for monitoring logs and alerts*
Users with Privileged Access: Preventing IoT Vulnerabilities in the Workplace	As the use of internet of things (IoT) devices like smart TVs, personal assistants, thermostats and wearable technologies increases within the workplace, unfamiliar devices may be used to compromise networks. This course describes threats presented by these devices and examines best practices for limiting potential risks.	• *Define threats to networks presented by IoT devices in the workplace* • *Generalize best practices for network access limitations for IoT devices*
Users with Privileged Access: Server Security & Patch Management	Server maintenance is a critical link in your organization's security cycle. This course details best practices for maintaining application servers, web servers and domain controllers to secure networks from compromise. Change management policy recommendations are also offered as a strategy for accountability and troubleshooting.	• *List best practices for maintaining the security of application servers, web servers and domain controllers* • *Explain how change management processes contribute to security*
Users with Privileged Access: Social Engineering Prevention	Social engineers use manipulation tactics to gather information about and access to organizations and their data. Users with privileged access are particularly desirable targets for these techniques. This course explores why privileged access users are at an increased risk and methods used in these types of attacks.	• *Name common methods used in social engineering attacks* • *Infer why users with privileged access are prime targets for social engineers*
Users with Privileged Access: Workstation Security	Failure to secure workstations within an organization can create widespread endpoint vulnerabilities. This course identifies common security tools used to prevent, identify and respond to vulnerabilities present on user workstations, including command line utilities and operating system policies.	• *Identify common command line utilities to secure and test workstations* • *Describe operating system policies that can enhance workstation security*

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.

Developer Course Descriptions

Course Name	Course Description	Course Objectives	Time	Audience
OWASP API Top 10	Application programming interfaces (APIs) are an increasingly common way to connect systems, applications and services. This course highlights common API security mistakes and recommends secure coding practices. A general understanding of coding practices and APIs is strongly recommended.	• *Explain the 10 most prevalent API vulnerabilities* • *Understand the risks of unsecure APIs* • *Detect and mitigate API vulnerabilities*	10 minutes	Developers
OWASP Mobile Top 10	In today's increasingly mobile environment, there is a drive for developers to quickly and efficiently create mobile applications for a variety of devices while following security best practices for the next generation of mobile applications. This course covers 10 important security topics that apply regardless of development platform or programming language.	• *List OWASP's top 10 mobile application security risks* • *Summarize threats presented by each risk type* • *Recall strategies that protect against risks identified in the course*	10-15 minutes	Developers of mobile applications
OWASP Proactive Controls	OWASP Top 10 Proactive Controls describe the ten most critical security concerns for software developers. Complementing the risk mitigation focus of OWASP Web/Mobile Top 10, these controls contribute to an informed foundation for a secure development process.	• *Identify the 10 most critical security concerns for software developers* • *Connect OWASP risk categories with proactive development strategies that protect applications*	15 minutes	Developers
Privacy by Design	The concept of Privacy by Design requires that technology designers and developers consider data privacy implications during the planning phase of development. The Privacy by Design course highlights common considerations that should occur before and during development to protect the privacy of data subject information.	• *Define Privacy by Design* • *Implement Privacy by Design concepts into planning and development of applications* • *Identify key questions and considerations of the Privacy by Design model*	5 minutes	Developers, Application Designers, UI/UX Designers
Threat Modeling	Developers must be cognizant of the security of every project they work on. Threat modeling is a systematic, structured and comprehensive way to identify and remediate security problems early in the process. Integrating effective threat modeling practices provides developers a consistent avenue for addressing their obligation to secure systems and data within a project.	• *Outline the threat modeling framework and related questions* • *Construct threat modeling diagrams to identify security concerns and focus* • *Utilize the "STRIDE" mnemonic to guide threat discovery*	15 minutes	Developers

Developer Course Collections

Collection Name	Collection Description	Time	Audience
Application Security	Uncovering, mitigating and improving the security of applications is paramount. These courses provide methods and strategies for protecting applications during development and once deployed.	80-120 minutes (8 10-15 minute courses)	Developers

Course Name	Course Description	Course Objectives
Application Security Client-Side Logic Manipulation	When attackers can alter client-side data, applications and the data within them are at risk. This course identifies client-side technologies and vulnerabilities and explains remediation strategies.	• *Describe how client-side logic manipulation works* • *State prevention best practices*
Application Security Command Injection	Command injection is one of the more serious types of attacks facing developers today. This course outlines types of injection attacks and details steps for prevention.	• *Outline dangers of command injection* • *Recall prevention best practices*
Application Security Cross-Site Request Forgery	Criminals can exploit login procedures to compromise an application. This course explains how cross-site request forgery is executed and how to prevent it.	• *Comprehend how cross-site request forgery attempts work* • *Utilize prevention best practices*
Application Security Cross-Site Scripting	Without the proper handling of user input, the potential exists for an attacker to insert malicious code. This course describes the types of cross-site scripting attacks and strategies for mitigation.	• *Understand how cross-site scripting attempts work* • *Employ prevention best practices*
Application Security Data Modification	Cybercriminals compromise the information associated with an application for a variety of nefarious endeavors. This course identifies the ramifications of data modification, explains how it works and provides prevention techniques.	• *Determine how data modification occurs* • *Implement prevention best practices*
Application Security Forceful Browsing	Attackers use forceful browsing to reveal an application's infrastructure, enabling a deeper compromise of the application. This course explains how forceful browsing happens and how to prevent it.	• *Explain how forceful browsing is used to identify directory structures* • *Identify details that may enable attacks*
Application Security Information Leakage	Under the right, albeit undesirable, conditions, an application can leak information that an attacker can use to exploit the application. This course addresses information leakage from its types and sources to prevention techniques.	• *Detail the dangers of information leakage* • *Integrate prevention best practices*
Application Security Session Hijacking	Cybercriminals can exploit an application's vulnerabilities to obtain user credentials and, thus, access the application. This course explores variations of session hijacking and how to prevent them.	• *Illustrate how TCP and cookie hijacking occur* • *Apply prevention best practices*

Collection Name	Collection Description	Time	Audience
OWASP Top 10	OWASP, the Open Web Application Security Project, regularly lists the 10 most frequent and dangerous security vulnerabilities and attacks being used on the internet. This program covers each of the attacks on OWASP's list by exploring examples, remediation and best practices to incorporate into development and coding work.	60 minutes (1 single course or 11-part program)	Developers
Course Name	**Course Description**	**Course Objectives**	
Introduction to OWASP	The developer's role in securing applications is critical, especially in today's vulnerable web environment. Fortunately, trusted resources are available to guide secure development, regardless of the programming language used. This course introduces learners to the Open Web Application Security Project (OWASP) and its resources.	• *Recognize threat actors who may target web applications* • *Summarize the resources offered to developer by OWASP*	
OWASP Top 10: Injection #1	Injection attacks are the most common and dangerous attacks on the web today. This course examines why untrusted data compromises unsecure web applications and how separated data, trusted libraries, whitelisting and SQL controls can prevent successful injection attacks.	• *Describe how injection attacks are used to exploit databases* • *Identify four secure coding methods to prevent successful injection attacks*	
OWASP Top 10: Broken Authentication and Session Management #2	Broken authentication can expose passwords, account credentials, tokens and session IDs. This course explores flaws in authentication and session management that can be used to exploit user identities. Prevention techniques cover authentication management standards, two-factor authentication, random session IDs and timeouts.	• *Illustrate a scenario where broken authentication allows improper access* • *Defend recommended prevention techniques to secure web applications*	
OWASP Top 10: Sensitive Data Exposure #3	Failure to encrypt sensitive data or using weak encryption methods risks exposing data to cybercriminals. This course outlines processes to classify and handle sensitive data, outlines encryption methods and reviews configurations to protect data.	• *Classify sensitive data for encryption* • *Recall unsecure encryption methods*	
OWASP Top 10: XML External Entities #4	Malicious XML documents sent to an application can wreak havoc when an outdated or defective XML processor is used. This course illustrates how XML external entity (XXE) attacks contribute to denial-of-service and data theft. Recommended prevention techniques include input validation, proper data encryption and formatting and manual code review.	• *Outline how malicious XML documents enable denial-of-service and data theft* • *Identify application frameworks that use XML and may be a target of cyber attacks*	
OWASP Top 10: Broken Access Control #5	Flawed access controls do not properly govern what authenticated users may or may not do within an application. This course analyzes common flaws which may allow access to the application or functionality by unauthorized users. The course also recommends tips for reviewing access controls and implementing reference maps.	• *Diagram steps for reviewing access controls in an application* • *Reference recommended resources for eliminating direct object references*	
OWASP Top 10: Security Misconfiguration #6	Security misconfigurations are easily exploitable and frequently allow attackers unauthorized access to systems or data beyond the scope of a single application. This course details specific attack vectors and weaknesses that can be exploited and examines how repeatable security configuration processes and security hardening can reduce risk.	• *Explain how repeatable security hardening prevents misconfiguration* • *Describe a scenario in which an application security misconfiguration allows access to the entire web server*	
OWASP Top 10: Cross-Site Scripting #7	Untrusted data on web pages can introduce cross-site scripting flaws that allow attackers to execute scripts in a user's browser to hijack sessions, deface websites or send the user to a malicious website. This course reviews common targets for these attacks, contrasts server-side and client-side flaws and explores prevention methods.	• *Recognize common user types that may be targeted for XSS attacks* • *List OWASP cheat sheets and anti-XSS libraries that assist in sanitizing content*	

Course Name	Course Description	Course Objectives
OWASP Top 10: Insecure Deserialization #8	Insecure deserialization can lead to remote code execution, injection attacks and other serious threats when an attacker enters malicious content in the application. This course explores how malicious content can allow attackers to tamper with data during deserialization to exploit flaws and prevention techniques that can limit attack success.	• *Summarize how malicious content can modify data during deserialization* • *Discern why manual reviews are needed to identify deserialization flaws*
OWASP Top 10: Using Components with Known Vulnerabilities #9	Vulnerable components are easily located and exploited by attackers with threats ranging from minor damage to full server takeover. This course identifies potential areas of vulnerability and offers best practices for locating and documenting all components (software and hardware) to identify and secure vulnerable components.	• *Describe how inventory and tracking can uncover vulnerable components* • *List vulnerability report resources that can identify vulnerable components*
OWASP Top 10: Insufficient Logging and Monitoring #10	Inadequate monitoring of an application for unusual events or patterns can allow attacks to go unnoticed and hinders mitigation efforts. This course outlines appropriate logging and monitoring practices to alert for suspicious activity, identify potential malicious users and document vulnerability resolutions.	• *Summarize how logging and monitoring can prevent or limit attacks* • *Relate why contingency and incident response plans are critical to monitoring*