Standard Package Course Descriptions

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 course styles that resonate with different organizational goals and audiences.

Just-in-Time Courses

Optiv's SecurityBytes microlearning courses are designed to provide just-in-time training when an end user fails a simulated phishing campaign. These courses, are comprised of 1-3 minutes of content followed by a three-question quiz and are part of the Standard package.

Video-Based SecurityBytes

Photo-based images and design create a realistic look. **Includes Voiceover**

Available Courses:

- Business Email Compromise
- Credential Theft
- Data Privacy
- Email Security
- Malicious Downloads
- Social Engineering

Animated/Scenario-Based SecurityBytes

Videos use animated imagery to convey information. **Includes Voiceover**

Available Courses:

- Business Email Compromise
- Credential Theft
- Phishing Attachments I
- Phishing Attachments II
- Phishing Links
- Phishing Links and Notifications
- Ransomware
- Spear Phishing I
- Spear Phishing II
- Spoofing
- Wire Transfer Fraud

Standard Courses

General Security Awareness

Rapid Awareness Digital Hygiene

5 minutes

All Employees and Contractors

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

Security Awareness Training New Hire

20-25 minutes

All Employees and Contractors

An organization's new employees can be targeted because they are unfamiliar with the environment and may not know the different processes and procedures. This course is intended to prepare new employees to recognize and mitigate threats to the business, as well as to clients, associates, and fellow personnel.

- Identify email- and social media-based risks
- Define the effective use and protection of passwords
- Recognize negligent behaviors that introduce risk

Security Awareness Training Refresher

15 minutes

All Employees and Contractors

Although new hires may be easy targets, tenured employees and the valuable artifacts, access, data, or knowledge they have, are likely more lucrative. This course is intended to refresh existing employee knowledge with tips for reducing attack surfaces, working remotely, and recognizing malicious content.

- Identify risks within remote work environments like home offices
- Describe methods for reducing personal attack surfaces
- List common attack vectors used to deliver malicious content

Your Role in Cybersecurity

10 minutes

All Employees and Contractors

For organizations, cybersecurity is a complex and interdependent system of components. It requires people, process, and technology, and people are the connective mechanism that binds the collective efforts together. This course provides a high-level identification of what all organizations must do to be cybersecure, and explains why organizations ask employees to do what they're asked to do.

- Explain the interdependency of people, process, and technology in the context of cybersecurity
- Identify why employees are asked to do what they're asked to do
- Understand how individual actions enable an organization's cybersecurity mechanisms

Phishing, Vishing, and Smishing

Hannah on the Hook

5 minutes	All Employees and Contractors
While at a trade show, Hannah finds herself challenged by cleverly designed phishing emails. Will she be able to identify the tricks used to hook targets, or will she take the bait?	• Compare emails to identify those that are suspicious • Describe how common elements in emails are used to make phishing messages more convincing

Hold the Phone

5 minutes	All Employees and Contractors
Not all cybersecurity threats happen online. Sometimes, they come calling on the phone. This course reveals best practices for handling vishing attempts and unknown callers.	• Define vishing and caller ID spoofing • Describe common vishing tactics and risks • Summarize strategies to combat vishing attempts

Rapid Awareness Business Email Compromise

5 minutes	All Employees and Contractors
Business email compromise is a sophisticated phishing threat that cost organizations in the United States $12 billion in the last decade. This course reveals common warning signs, potential data and financial targets, and tips for identifying and responding to potential attacks.	• Describe targets of BEC attacks • Identify indicators of BEC attacks • Respond appropriately to messages requesting payment, wire transfers, or the release of sensitive data

Rapid Awareness Coordinated Phishing and Vishing Attacks

5 minutes	All Employees and Contractors
While phishing emails and vishing calls are distinct threats, they are frequently combined in coordinated attacks that seem more credible and enticing to end users. This course examines how these techniques are used in tandem 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 that occur during a combined attack

Rapid Awareness Email Security

5 minutes	All Employees and Contractors
With a focus on phishing threats, the Rapid Awareness Email Security course helps users defend organizational email against phishing attacks. Learners will review phishing methods, the importance of reporting suspected phishing emails, and common indicators of phishing.	• Define phishing • Identify common characteristics within phishing email messages • Explain the importance of reporting suspected phishing emails to protect other users

Rapid Awareness Phishing Attachments

5 minutes	All Employees and Contractors
Phishing emails don't always contain malicious links. Many have attachments that contain malware or malicious macro code. This course highlights the most common types of malicious attachments and how they 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

Rapid Awareness Phishing Links

5 minutes

All Employees and Contractors

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 suspicious links in messages
- Examine links to reveal destinations
- Identify potentially malicious websites that may steal information

Rapid Awareness Phishing Notifications

5 minutes

All Employees and Contractors

The sense of urgency and resulting panic from false email notifications can entice users to turn over credentials or open malicious attachments or links. This course reviews 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

Rapid Awareness Spear Phishing

5 minutes

All Employees and Contractors

The targeted nature and amount of specific detail in spear phishing attacks can fool even the most savvy and cyber aware users. This course reviews 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 suspicious messages to identify the source
- Describe how cybercriminals locate spear phishing targets

Rapid Awareness Spoofed Phishing Emails

5 minutes

All Employees and Contractors

Spoofed emails are a specific type of phishing attack that appears to be sent by a familiar contact or source. This course reviews how email addresses are spoofed, signs a received message might be spoofed, and how to respond if your own 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

Rapid Awareness Wire Transfer Fraud

5 minutes

All Employees and Contractors

Wire transfer fraud and phishing emails often go hand-in-hand. This course reviews how a simple phishing email can cause significant financial loss. Users learn how email wire transfer fraud is 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

Securing Your Inbox

10-15 minutes

All Employees and Contractors

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

The Confidential Matter (Business Email Compromise)

5 minutes	All Employees and Contractors
When your organization's CEO emails you about a very sensitive matter, you follow instructions to the letter, right? Not so fast. What if the person giving you those instructions isn't who they claim to be? In this course about business email compromise (BEC), users learn who attackers target and how they construct these types of emails. Learners also acquire tips for identifying BEC as part of the scenario.	• Explain how BEC attacks occur and who may be targeted • List common indicators present within messages involved in BEC attacks • Describe methods used to avoid falling for a BEC email

Data

Cloud Cover

5 minutes	All Employees and Contractors
Most employees would agree that it's better to work smarter, not harder. But what if that convenience and expedience comes at the cost of security? In this course, learners experience a common example of shadow IT and examine the fallout from utilizing unapproved IT resources.	• Define shadow IT • Identify risks associated with using shadow IT resources • Summarize steps for addressing shadow IT

Data Privacy Protectors

7-10 minutes	All Employees and Contractors
Join the ranks of the Data Privacy Protectors by learning to recognize the types of personally identifiable information and sensitive organization data that need special protection. Your team lead, Nina, will guide you through steps to collect, use, and dispose of sensitive information securely.	• Recognize which data is considered personally identifiable information • Define specifitypes of sensitive customer and organizational data • Collect, store, and process data securely

Processing Personal Data

10-15 minutes	All Employees and Contractors
Organizations that collect and process sensitive information are obligated to securely handle that data. This course will acquaint learners with these obligations and offer best practices for protecting the data they collect and process.	• Define personal information • Identify actions that involve the handling of personal information • List best practices for protecting personal information

Rapid Awareness Data Privacy

5 minutes	All Employees and Contractors
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

Rapid Awareness Safe Data Handling

5 minutes	All Employees and Contractors
Organizations and their employees process significant amounts of internal and external data each day. This course examines methods for protecting sensitive 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

Mobile and Devices

Antiquaman and the Mobile Menace

5 minutes	All Employees and Contractors
There's a mobile menace lurking in app stores. Superhero Antiquaman is searching for a mobile app, but he needs to be sure it's safe. In this comic book style course, users help Antiquaman select the safest app and learn common indicators that a mobile app might be malicious.	• Restate why mobile devices are targeted by cybercriminals • List elements to review when selecting mobile apps • Summarize signs that a malicious app may be installed on a device

Rapid Awareness Attacks on Smart Devices

5 minutes	All Employees and Contractors
Smart devices are a growing target for cyberattackers as their features, operating systems, and data storage capabilities evolve. This course explores vulnerabilities common in smart devices, potential indicators of compromise, and steps users can take to protect devices.	• Define what constitutes a smart device • Identify common attack vectors for smart devices • Describe potential indicators of compromise on smart devices

Outside the Office

Feeding Habits of CyberBOTs

5 minutes	All Employees and Contractors
Created in a sinister laboratory, the CyberBOTs are formidable creatures that feed on sensitive information and data. This parody of a nature documentary reviews potential CyberBOT "feeding sources" common in modern homes, and learners identify potential sources of exposure.	• Identify potential sources of data exposure in homes • Describe home workspace layouts conducive to protecting data • Summarize how smart home devices can introduce data risks

Rapid Awareness Social Media Security

5 minutes	All Employees and Contractors
The Rapid Awareness Social Media Security course covers the basics of using social media 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 privacy settings to limit sharing • Avoid malicious social media links

The Moving Target

5 minutes

Social media allows you to invite people into your world. But oversharing information or posting photos that reveal too many details could expand that invitation too far. In this course, learners will review how certain social media posts and interactions can threaten privacy.

All Employees and Contractors

- Explain risks of posting personal details on social media
- Detail what photos posted on social media can reveal
- Describe how threat actors can use information posted on social media for an attack

Passwords and Authentication

Identify Yourself

10 minutes

Password recovery questions are a useful security feature, but they can also serve as an entry point for unauthorized users. This course teaches how to choose strong password recovery questions and answers to protect against compromise.

All Employees and Contractors

- Identify characteristics of strong recovery questions
- Contrast weak and strong recovery questions
- Describe how threat actors discover answers to password recovery questions

Paul's Password Problem

8 minutes

Almost any end user will need to choose or update their password to meet specific criteria. This course shares practical skills for creating secure passwords, protecting them from compromise, and securing credentials for multiple accounts.

All Employees and Contractors

- Define best practices for protecting passwords
- Explain why each accounts needs a unique password
- Summarize strategies for choosing strong security questions

Rapid Awareness Multifactor Authentication

5 minutes

While strong, unique passwords are key to securing accounts, if credentials are compromised, a secure password alone cannot provide adequate protection. This course examines steps involved in multifactor authentication, types of additional authentication and advantages of authentication methods.

All Employees and Contractors

- Explain the process which occurs during a multifactor authentication
- Secure accounts using a multifactor authentication method
- Describe the pros and cons of different additional factor types

SACT Password Security

10-15 minutes

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.

All Employees and Contractors

- Create strong, unique passwords
- Explain the importance of using unique, secure passwords
- Define best practices related to protecting passwords

The Problem with Popular

5 minutes	All Employees and Contractors
When it comes to passwords, you do not want to be popular. This course examines how attackers leverage some of the most commonly used passwords to compromise accounts in password spray attacks. Users also learn best practices for selecting unique, secure passwords.	• Describe how popular passwords lead to compromised accounts • Summarize processes involved in password spray attacks • Define secure password strategies

Malware and Malicious Downloads

Malicious Macros: Malware in Office Apps

5 minutes	All Employees and Contractors
Often spread through phishing email attachments, macro malware is embedded in common file types used with office productivity applications. This course explores how macro malware is spread and identifies best practices for recognizing and responding to it.	• Describe the concept of macro malware • Identify the consequences of interacting with macro malware • List best practices for addressing macro malware if/when you encounter it

Ransom Note

5 minutes	All Employees and Contractors
Phishing emails continue to be the primary threat vector for the distribution of malware. In this course, learners will gain a basic understanding of common malware types and how to recognize indicators of a potentially malicious email.	• Identify and define four common types of malware • Summarize indicators of a potentially malicious email • List best practices for responding to a potentially malicious email and malware infection

Rapid Awareness Malicious Downloads

5 minutes	All Employees and Contractors
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

Rapid Awareness Ransomware Basics

5 minutes	All Employees and Contractors
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

Rapid Awareness Ransomware in the Workplace

5 minutes	All Employees and Contractors
The Rapid Awareness Ransomware in the Workplace course examines ransomware-related threats to organizational devices, networks, and data. This course examines two common types, locker and crypto ransomware.	• Recognize signs of a ransomware infection • Describe differences between locker and crypto ransomware • Outline how ransomware spreads across networks

Web Woes

5 minutes	All employees and contractors
Malware often lurks in the places we least expect to find it. This course educates users about the prevalence of malware in search results and websites and common misconceptions about certain safeguards when browsing online.	• Identify indicators of malicious links in search results • Describe the limitations of certain safeguards when browsing websites • List general best practices for safe browsing

Social Engineering and Workplace Security

Rapid Awareness Social Engineering

5 minutes	All Employees and Contractors
As a concise introduction to social engineering tactics, this course provides a high-level overview of this type of attack. Users gain knowledge regarding potential 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

SACT Insider Threat

10-15 minutes	All Employees and Contractors
Security threats from those within an organization often carry the greatest risks. Easy access to data by insiders is a significant threat. This course reviews these threats and enables employees 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

SACT Social Engineering

10-15 minutes	All Employees and Contractors
This course explores the techniques and intentions of social engineers during in-person, phone, and social media interactions. Since social engineering attacks can occur anywhere, this course examines attack vectors 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

The Help Desk

5 minutes	All Employees and Contractors
We're all on the lookout for cyberattacks, but what about the threat before the attack? In this course, users experience a real example of pretexting to learn how threat actors use this technique in the early stages of an attack.	• Define pretexting • Identify potential sources an attacker might use to obtain information for pretexting • Summarize strategies to identify and combat pretexting

Workplace Security Sabotage

6-8 minutes

A career cybercriminal has targeted an organization with plans to enter the organization's facilities, infect the network with malware, and steal files—all while cautiously bypassing security. Follow along to learn common workplace security mistakes that could result in a successful attack.

All Employees and Contractors

- Explain how to prevent unauthorized access to physical locations
- Summarize benefits of keeping a secure workspace
- Describe risks of using unapproved devices on the organization's network

Connections

No Place Like Home

5 minutes

You secure your home, but what about you connect from home? This course reviews how vulnerable home networks impact the security of personal devices and data and provides best practices for securing these connections.

All Employees and Contractors

- Identify risks of using unsecured network connections
- Explain the importance of securing home networks with a secure password
- Summarize details to exclude from home network names

Artificial Intelligence (AI)

Quinn Has a Question

5 minutes

These days, a simple phone call from a colleague may be much more than meets your ears. This course examines how deepfake audio is used in vishing attacks. Learners will discover simple and creative ways to challenge callers, verify identities, and detect synthetic audio over the phone.

All Employees and Contractors

- Identify indicators of deepfake vishing
- Describe how vishing has evolved into a sophisticated threat vector
- Summarize prevention strategies to combat deepfake vishing attacks

Responsible Use of AI

5 minutes

Understanding how to use AI tools securely is imperative to the security of individuals and organizations. This course equips all employees with a base knowledge of AI and an understanding of the guidelines and boundaries that ensure safe, responsible, and ethical use of AI in the workplace.

All Employees and Contractors

- Identify popular AI technologies
- Explore recent developments in AI technology
- Identify risks to individuals and organizations who use AI technology

Shadow AI

5-7 minutes

Tony is a virtual healthcare provider looking for a way to increase efficiency, and it seems like an AI tool is the perfect solution. But what if that tool isn't approved by the organization? This course examines the impact of "shadow AI," the use of unapproved AI technology in the workplace.

All Employees and Contractors

- Define shadow AI
- Summarize common data integrity and privacy risks of shadow AI
- List best practices for securely using AI in the workplace

Using AI Securely

10-15 minutes	All Employees and Contractors
As artificial intelligence (AI) systems and tools gain popularity, many users are interacting with them for the first time. While the technology itself can be useful, it also poses a number of cybersecurity and privacy risks. This course helps users understand these risks and the best practices they can employ to interact with AI systems and tools in more securely.	• Describe what happens when users provide an input (query, command, or data) to an AI system or tool • Identify risks and threats specific to AI devices, services, and apps • List best practices for using AI systems and tools securely