# Cybersecurity Education Catalog

## Security Awareness Education (SAE)

Trustwave®

# Introduction

The human factor – what employees do or don't do – is the biggest problem to an organization's information security, yet it's often the most overlooked. Whether they are working in an office, working remotely, processing credit cards, handling clients' personal information, or developing software solutions for your business, your employees are ripe targets for information thieves seeking access to your sensitive data--unless you help them learn how to protect against and respond to security incidents.

It is vital to your organization to mitigate the human risk factor by providing a security awareness education program to your entire organization. Trustwave offers:

- Security Awareness Education (SAE)
- Security Awareness Education (SAE) with the option to add a phishing simulation plugin
- Phishing Simulation plugin standalone product

SAE courses may be hosted in the Trustwave Learning Management System (LMS). Our training content is Sharable Content Object Reference Model (SCORM) 1.2 compliant. Trustwave cloud-based courses run on all major web browsers and operating systems for desktop and mobile devices, providing anywhere, anytime access.

Use this catalog to browse the Cybersecurity Education offerings for SAE. If you have questions about SAE, reach out to your Trustwave account manager or use the Contact Us section of the Trustwave website at www.trustwave.com.

# Table of Contents

# Security Awareness Education

The Trustwave Security Awareness Education program is a cloud-based, fully automated, SaaS LMS featuring expertly curated programs that includes award-winning content in 14 languages.

How does the program work? Trustwave's program takes the heavy lifting from your organization by creating a general security awareness learning path that is automatically assigned to all new users. This learning path is based on recent cybersecurity threats.

The LMS portal allows for modification of the general awareness learning path by the organization's administrator. Modifying learning paths is easy. The organization's administrator can modify learning paths with just one drag of the mouse. Or they can create role-based learning paths using the suggested role-based learning paths included in this course catalog. Your administrator can also create other learning paths.

One license grants access to the entire library, including microlearning videos which can be scheduled at different times to reinforce your program year-round. Add the phishing plugin to test and educate your organization about phishing.

The Trustwave Security Education program is fully customizable based on your security awareness training needs. Contact your Trustwave account manager if your organization would like to receive a free trial.

### Security Awareness Education

By increasing the content by 75% and adding more engaging, interactive, and effective content our security awareness education program gives organizations the ability to educate their employees while addressing all learning styles and meeting the organization's security awareness goals. Real-life simulations and scenarios allow for the content to be more relatable to the learner. This program allows the administrator to have full control on what to assign, when to assign, and to whom.

### Phishing Simulation Plugin

Trustwave understands the importance of risk mitigation by making your employees aware of phishing and the damage it can cause. Trustwave Cybersecurity Education offers a customizable phishing simulation plugin that offers different types of phishing emails to send to different groups of your organization. If the unsuspecting employee clicks on the link embedded in the email, they will be directed to security awareness training courses presenting the dangers of phishing attacks and how to prevent them. And all in one platform!

### Courses Available in Multiple Languages

All courses are available in English. Most courses are available in translated text or translated voice/text. The default portal language is English and is available in many other languages. Available course languages are:

| | |
|---|---|
| English (US) | Spanish (EU) |
| English (UK) | Japanese |
| Chinese-Simplified | Korean |
| Chinese-Traditional | Italian |
| French (EU) | German |
| French (CA) | Russian |
| Spanish (LA) | Portuguese (LA) |

### Certified by the Texas Department of Information Resources

Our SAE courses meet the criteria required for certification by the Texas Department of Information Resources, with the end goal of providing certified content for Texas state and local government employees. If you have any questions about this certification please email trustwavesaesupport@trustwave.com.

## SAE Courses

Browse our extensive collection of security-awareness training provided by area of interest. A course code, description and learning objectives, and training duration accompany each topic. Administrators can refer to the tables if they choose to modify the default general learning path or create new role-based paths based on SAE recommendations. Additionally, custom learning paths can be created for the organization based on your organization's training needs.

**EN** = English Only **MTL** = Multi-language, text or text/voice translated

**Security Awareness Topics** These courses present general security awareness.

| Course Code | Course Name | Course Description and Objectives | Duration |
|---|---|---|---|
| S-190-CQ-01-MTL | Security Assessment | The security assessment provides an all-new 10-question test bank giving training managers a second pre-assessment option that covers major security awareness topics, including malware, phishing, and IoT. CyQ tracks and measures the user's response to each question by category. Analytics provide a detailed profile of each user's results. | 10 minutes |
| S-202-SA-01-EN | Introduction to Security Awareness | Enhance your security awareness. This course contains up-to-date security information presenting security awareness by learning about the different types of sensitive information and how to protect it. Reviewing risks associated with mishandling sensitive information and what to do in case of a breach allows employees to become more informed and aware of the impact of their daily activities. Implementing best practices presented in this course allows the protection of sensitive data in the workplace. | 30 minutes |
| S-131-SL-02-MTL | Security Awareness - Strongest Link | Protecting your personal and company data has become a crucial part of our everyday lives, and there is more at stake than ever. Hackers and cybercriminals roam the Internet seeking both vulnerabilities to exploit and uninformed users to take advantage of. Learn the fundamentals of information security and safe computing habits, including key principles, concepts, vulnerabilities, threats, and how to counter them. | 30 minutes |
| S-141-PH-01-MTL | Security Awareness Basics | This course presents two of the most dangerous cyber-threats to any organization: malware and phishing. The importance of being "security aware" and making safe, security-conscious decisions on a day-to-day basis is reinforced to help thwart these menacing cyber-attacks. | 15 minutes |
| S-141-SA-01-MTL | Security Awareness Essentials | Employees will master the fundamentals of information security including key threats and how to counter them. By mastering the information presented in this course employees will be able to effectively defend personal and workplace data from malicious threats. | 30 minutes |
| S-161-AP-01-MTL | Defending Against Phishers | This animated course builds awareness about phishing threats with easy-to-apply best practices about how to recognize and defend against them. Whether at work or at home, people around the world are inundated with millions of phishing threats every day. And as the public grows more aware of these threats, cyber criminals evolve and look for ever-more sophisticated ways to trick would-be victims into "click the link." | 10 minutes |
| S-161-AP-07-EN | Coronavirus Phishes & Scams | As the coronavirus pandemic has spread across the globe, cyber-attacks have also been on the rise. Cybercriminals have increased their phishing attacks and are creating new scams as more and more people are staying at home and potentially working remotely for the first time. This brief course will teach learners to recognize the current patterns and elements of coronavirus based phishes and scams and provide best practices on how to avoid their traps and stay secure. | 5 minutes, 30 seconds |

## Security Awareness Topics

These courses present general security awareness.

| Course Code | Course Name | Course Description and Objectives | Duration |
|---|---|---|---|
| S-161-CS-01-MTL | Cloud Security | Cloud-based services offer incredible convenience and can help people be more productive, especially while on the go. But they also create new security challenges, because the security of any information stored on the cloud is only as good as the security of the service provider who holds it. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for cloud security. | 9 minutes |
| P-101-PB-01-EN | Privacy and Data Protection | This course will help employees understand what information is private, why it is private, and what they can do to protect it throughout the data lifecycle, which is the life of a piece of information, whether in paper or digital format, from creation to destruction within an organization. | 30 minutes |
| S-161-ES-01-MTL | Email & Instant Messaging Security | Email and instant messaging (IM) are essential communication tools that most people use just about every day. They're incredibly useful applications because they allow you to quickly and efficiently exchange messages and files with just about anyone else in the world. However, it's a two-way street, meaning that since you can connect with anyone online, anyone else, including hackers and cybercriminals, can connect with you. This course teaches employees the email and IM best practices to protect both their organization's sensitive information and their own personal information and identity from attack. | 11 minutes |
| S-161-HM-01-MTL | Security Awareness for the Home | Threats to our home network can quickly turn into threats to our workplace infrastructure and visa-versa. To combat against threats, we must learn to practice safe computing habits both in the home and in the workplace. Learners will be introduced to some key principles of safe system administration that they can use in the home that mirror techniques used in the workplace. By mastering the techniques found in this course, participants will learn to develop a regime of security-conscience behavior that will help keep important data safe from getting in the wrong hands. | 7 minutes |
| S-161-HS-01-MTL | Internet of Things & Home Security | Almost anything can be made into a "smart" device, such as security cameras and sensors, TVs, garage door openers, door locks, wearable devices, pacemakers, and even cars. These devices are what we refer to as the "Internet of Things" (IoT), which holds the promise of adding a whole new level of convenience and connectedness to everyday life. Having that many new, connected computing devices, most of which record activity, presents new challenges for security and privacy. This course teaches employees the best practices for IoT devices both at home and at work. | 10 minutes |
| S-161-IR-01-MTL | Incident Reporting | Reporting incidents of suspicious activity and the loss of assets or sensitive information is extremely important. In this module, employees will learn about common physical and information security incidents that should be reported and how to report them. | 7 minutes |
| S-161-IT-02-MTL | An Introduction to Insider Threats | Across the globe, organizations spend countless hours working to keep sensitive data out of the hands of cybercriminals. This task has become even more difficult to manage due to an increasing number of data compromises that stem from insider threats. This threat from within, or "insider threat" can be successfully addressed using the strategies shared in this module. In this module we will discuss the three types of insider threats, some recognizable behaviors associated with each type and provide simple yet effective strategies to counteract each threat. | 7 minutes |
| S-161-IT-03-MTL | Protecting Against Malicious Insiders | The threat is real. It's taking place somewhere, right now. A malicious insider has decided to mount a cyberattack against your organization from the inside out. This malicious insider will stop at nothing to get the data they need to commit theft, fraud or sabotage. By applying the strategies provided in this course and being willing to take action you can help rid the workplace of these malicious insider threats. In this module you will learn what a malicious insider does, some recognizable threat indicators and simple yet effective ways to address the malicious insider threat. | 8 minutes |
| S-161-MA-02-MTL | The Malware Threat | Malware is any type of software that is intended to damage or disable computer systems. It is often used to steal information, destroy or lock users from data, or disrupt operations. This course defines malware and the associated security threats, and describes common types of malware. By mastering the information presented in this course you will be able to help defend your personal and workplace data from these threats. | 5 minutes |

## Security Awareness Topics

These courses present general security awareness.

| Course Code | Course Name | Course Description and Objectives | Duration |
|---|---|---|---|
| S-161-MA-03-MTL | Ransomware: How to Defend Yourself | Ransomware is a type of malicious software used by hackers to encrypt files and other functions from a user until the victim pays a "ransom." This form of cyberattack has become one of the most used and most costly threats to businesses and individuals alike. By mastering the information presented in this course you will be able to help defend your personal and workplace data from ransomware threats. | 4 minutes |
| S-161-MA-05-MTL | Preventing Malware: Mobile Devices | This course acknowledges the commonplace usage of mobile devices at work and explains key vulnerabilities that users must be aware of. By mastering the information presented in this course you will be able to help defend your mobile devices from security threats. | 7 minutes |
| S-161-MD-01-MTL | Protecting Mobile Data and Devices | Because today's smartphones and tablets can not only act as a phone, but also as an email client, mobile Internet device, camera, GPS navigation system, entertainment console, and platform for any number of applications (apps), they can be exposed to many of the same risks as a desktop computer. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for mobile security. | 8 minutes |
| S-161-PM-01-MTL | Password Management | Passwords are the keys to our digital lives and protect us from hackers and cybercriminals, but how exactly could a hacker crack your password and what can you do to protect it? This HTML5-based, iPad-compatible password management course uses high-quality video and real-world simulations to show the tactics hackers use to compromise accounts and the password security best practices that can help prevent that from happening. | 15 minutes |
| S-161-PS-01-MTL | Physical Security | Your personal safety at work is of paramount importance. This course is designed to teach employees how to protect an organization from criminals, espionage, workplace violence, natural disasters, and other threats. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach physical security best practices. | 15 minutes |
| S-161-SE-02-MTL | Defeating Social Engineers (Advanced) | With increasingly sophisticated technical defenses for networks and computer systems, hackers often decide that it's much easier to simply go around these perimeter defenses by attacking the end user. After all, end users have what they want – a computer that's behind the network firewall, a network username and password, and possibly access to trade secrets, confidential information, and bank accounts. This course will teach end users how to identify and avoid giving away sensitive information to these hackers. | 17 minutes |
| S-161-SM-02-EN | Appropriate Use of Social Media | Social media can be an excellent tool to connect and interact with customers, show thought leadership, and build a brand, but it also poses unique security, HR, and public relations challenges. This course covers social media best practices including secure use, accountability, harassment, how to spot scams, secure passwords, and advanced security features. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for social media | 14 minutes |
| S-161-WR-01-EN | Working Remotely | Mobile computing devices like laptops, smartphones, and tablets can be found everywhere – at home, in the office, and everywhere in between. These devices, combined with high speed wireless connections, make working remotely easier than ever. However, working outside of a company's secured facilities expose an organization's physical and information assets to additional threats. This course gives the best practices for working remotely. | 8 minutes |
| S-161-WR-02-MTL | Working Securely from Home | Mobile computing devices combined with online workplace collaboration platforms and video conferencing make working from home easier than ever. However, working outside of an organization's secured facilities can expose a remote worker and his/her workplace's assets to additional cyberthreats. This course will provide the best practices to working securely from home and help one to defend against these threats. | 9 minutes |

## Best Practices for Job Roles

These courses target specific job roles within an organization. Each curriculum you create should contain one of these JRT (Job Role Training) lessons, depending on your role and industry.

| Course Code | Course Name | Course Description and Objectives | Duration |
|---|---|---|---|
| S-203-RA-01-EN | Secure Practices for Retail Associates | Recognize the security awareness responsibilities of retail associates. This course presents laws, regulations, and acts, PCI DSS, as well as the methods of attack to prepare you to recognize a threat and what to do in case of a breach. Keep sensitive information secure by implementing suggested best practices into your everyday activities. | 20 minutes |
| S-204-RM-01-EN | Secure Practices for Retail Managers | Be able to implement security awareness and best practices to your organization to assist employees in protecting sensitive information. Information security is important, and this course presents the security responsibilities of retail managers or business owners that impact the retail environment. | 20 minutes |
| S-205-CC-01-EN | Secure Practices for Call Center Associates | Recognize the security awareness responsibilities of call center associates. This course presents laws, regulations, and acts, PCI DSS, as well as the methods of attack to prepare you to recognize a threat and what to do in case of a breach. Keep sensitive information secure by implementing suggested best practices into your everyday activities. | 20 minutes |
| S-206-CM-01-EN | Secure Practices for Call Center Managers | Be able to implement security awareness and best practices to your organization to assist employees in protecting sensitive information. Information security is important, and this course presents the security responsibilities of call center managers or business owners that impact the call center environment. | 20 minutes |

## Compliance Topics

These courses present the basic principles of various compliance standards and information security measures.

| Course Code | Course Name | Course Description and Objectives | Duration |
|---|---|---|---|
| PCI-202-IP-01-EN | Introduction to PCI DSS | Business today face many risks that can lead to security incidents. Introduction to PCI DSS reviews the Payment Card Industry Data Security Standards (PCI DSS), laws, regulations, and secure practices. This course provides you with the information you need to protect cardholder data. | 10 minutes |
| PCI-200-PB-01-EN | Incorporating PCI DSS into BAU | Discover how to incorporate the PCI DSS six best practices into your business. This course reviews the Payment Card Industry Data Security Standards (PCI DSS) and presents best practices of how to incorporate PCI DSS into Business-as usual (BAU) and provides the information needed to protect cardholder data. | 20 minutes |
| PCI-101-CS-01-EN | PCI Essentials for Account Data Handlers and Supervisors | This course teaches employees and supervisors what PCI DSS is, how it affects your organization and the best practices they should follow to protect cardholder data and detect and prevent fraud. | 20 minutes |
| PCI-120-IT-01-EN | PCI DSS Requirements Overview for IT Professionals | This course teaches IT professionals what PCI DSS is, how it affects your organization, how to comply with the 12 requirements and the best practices that front line staff should follow to protect cardholder data and detect and prevent fraud. | 45 minutes |
| PCI-201-RA-01-EN | PCI DSS for Retail Associates | Become PCI DSS compliant. This course reviews the Payment Card Industry Data Security Standards (PCI DSS) and provides best practices to implement in everyday activities in the retail environment. Reviewing case studies allows you to assess vulnerabilities and be aware of how data is stolen and what you can do to protect sensitive information in the workplace. | 20 minutes |

| Compliance Topics | These courses present the basic principles of various compliance standards and information security measures. | | |
|---|---|---|---|
| P-151-CP-01-EN | California Consumer Privacy Act (CCPA) Essentials | The California Consumer Privacy Act, or CCPA, has created many new individual consumer rights as well as responsibilities with which businesses must now comply. When it takes effect in January 2020, every business that gathers and sells California consumers' personal information must comply with the privacy protections required under the CCPA. This module will provide learners with an overview of the act, including five consumer privacy rights it provides and the types of businesses that must comply. | 10 minutes |
| P-131-GD-01-MTL | GDPR: Introduction and Overview | This comprehensive course is delivered in a series of short, concise modules targeted to specific areas of the law and targeted to defined roles contained within the GDPR. Participants will learn the fundamentals of the new regulations and the key concepts behind them. By the end of this course series, learners will be able to recognize situations where the GDPR comes into play and what to do when they do encounter data that falls under GDPR regulations. | 20 minutes |
| P-131-GD-02-MTL | GDPR: Key Principles of the GDPR | This comprehensive course is delivered in a series of short, concise modules targeted to specific areas of the law and targeted to defined roles contained within the GDPR. Participants will learn the fundamentals of the new regulations and the key concepts behind them. By the end of this course series, learners will be able to recognize situations where the GDPR comes into play and what to do when they do encounter data that falls under GDPR regulations. | 15 minutes |
| P-131-GD-03-MTL | GDPR: Transfers of Data Outside of the EU | This course is one of a multi-part series that covers the fundamentals of the EU's General Data Protection Regulation, or GDPR, as well as its origins and key concepts. The GDPR contains principles for protecting the privacy of EU citizens' personal data. When it takes effect in 2018, every organization, worldwide, that gathers, stores, or processes this data in any way, must comply with the strong data protections required under the GDPR. In this module, you learn how the GDPR affects our organization when transferring or receiving EU citizens' private information outside the borders of the UK and EU. | 15 minutes |
| P-131-GD-04-MTL | GDPR: Navigating GDPR with our US Partners | The European Union's General Data Protection Regulation (GDPR) takes effect May 25th, 2018, ushering in sweeping changes to requirements for any EU organization that collects, maintains, or processes the personal data of EU citizens, and exchanges of that data with organizations outside the EU will be significantly impacted. Since data transfers with the US represent a major share of these cross-border activities, this course will focus on a comparison of the differences between EU and US privacy laws, as well as exploring avenues by which EU-US information exchanges can be conducted. | 10 minutes |
| P-131-GD-05-MTL | GDPR: GDPR for Data Handlers | The European Union's General Data Protection Regulation (GDPR) takes effect in May 2018, ushering in sweeping changes to requirements for any organization that collects, maintains, or processes the personal data of individuals residing in the EU. Compliance with the GDPR will affect all our organization's data handling activities, either directly or indirectly, and all staff whose responsibilities include use of PII will be expected to operate in accordance with the regulation's safeguards. This course will provide employees a general awareness of the GDPR's requirements and how they affect our day-to-day data processing activities, as well as helping them to recognize potential problems should they arise. | 8 minutes |
| P-141-GD-01-EN | GDPR: How to Comply with GDPR in the US | The General Data Protection Regulation, or GDPR, contains principles for protecting the privacy of EU citizens' personal data. When it takes effect in 2018, every organization, worldwide, that gathers, stores, or processes this data in any way, must comply with the strong data protections required under the GDPR. Upon completion of this module, learners will be able to recognize situations where the GDPR comes into play and what to do when they encounter data that falls under GDPR regulations in the US. | 10 minutes |

## Microlearning Videos

These microlearning vidoes reinforce knowledge training, increse knowledge retention, and improve overall performance. All videos are in English.

| Course Code | Video Name | Video Description and Objectives | Duration |
|---|---|---|---|
| S-162-BE-01-EN | The Business Email Compromise | Be able to implement security awareness and best practices to your organization to assist employees in protecting sensitive information. Information security is important, and this course presents the security responsibilities of call center managers or business owners that impact the call center environment. | 1 minute, 38 seconds |
| S-162-ET-01-EN | Evil Twin | "Evil Twin" is a technique hackers use gain to access your information through phony Wi-Fi access points that appears to be legitimate. Evil Twins can be difficult to spot because they often have names very similar to authentic access points. This short instructional video highlights simple steps you can take to evade an Evil Twin attack. | 1 minute, 36 seconds |
| S-162-FA-01-EN | Fake App Trap | Many of your favorite retailers and service providers have developed mobile apps so you can conveniently purchase goods and services, directly from your mobile device. But did you know that cybercriminals are also hard at work cooking up fake apps, using a recipe that often contains pop-up ads and malware? The good news is that you can avoid the Fake App Trap by applying the strategies outlined in this video. | 1 minute, 21 seconds |
| S-162-FN-01-EN | Fake News | Chances are you've seen sensationalized news headlines aimed at luring consumers through a rabbit hole of clickbait and misinformation. This false information phenomenon, known as "fake news," has quickly become a part of our daily reality, with no signs of slowing down. Fortunately, this video provides some strategies you can take to help keep fake news in check. | 1 minute, 52 seconds |
| S-162-HS-01-EN | Home Cybersecurity | Securing your home Internet experience can be like steering a ship through stormy seas. Inspired eLearning can help you navigate the perils of securing your home network. The trick is to make sure that you Isolate, Update and Defend. Watch this video to learn more about how to protect your home Internet service and devices. | 1 minute, 11 seconds |
| S-162-IO-01-EN | Home Invasion: The Internet of Terrors? | It is projected that by 2025, there will be over 75 billion "things" connected to the Internet, otherwise known as the Internet of Things (IoT). Such massive connectivity will make life much more convenient for you, but potentially for criminals as well. Many of these devices do not use current security features and are very susceptible to hackers. Watch this video to learn more about what you can do to help protect yourself from IoT threats. | 1 minute, 36 seconds |
| S-162-MS-01-EN | Living Mobile Secure | Attacks on mobile devices, mobile apps, and mobile carriers are rising fast. How can you ensure your device is secure? What happens if your phone or tablet is breached? Watch this video to learn more about what you can do to help protect yourself from mobile security threats. | 63 seconds |
| S-162-PH-01-EN | Phishing Defense Best Practices | Hackers are increasingly targeting individuals by sending emails that appear to come from a trusted source such as a bank, social network, or popular website. These emails include links and attachments that, if clicked, install malicious programs that compromise computer security. Watch this video to learn more about how you can protect yourself from phishing attacks. | 52 seconds |
| S-162-PH-02-EN | Protecting Against Spear Phishers | Spear phishing attacks target individuals with highly tailored emails that appears to be coming from a co-work or someone they know and trust, making it difficult to avoid opening attachments, clicking on infected links, or replying to attackers with personal or confidential information. Learn how to protect yourself by applying the strategies learned from this short video. | 49 seconds |
| S-162-PH-03-EN | SMiShed! | Inspired by true events, SMiShed! recalls a recent SMS phishing (or SMiShing) attack that scammed several bank customers out of tens of thousands of dollars. By applying the best practices outlined in this Microlearning video, you can avoid being victimized by a SMiShing attack. | 1 minute, 38 seconds |
| S-162-PH-04-EN | Dial V for Vishing | Vishing is a form of phishing in which a malicious hacker uses the phone to launch targeted attacks. In this special episode of Cybercrimes and Mysteries, you'll see a dramatic reenactment of what can happen to someone who falls victim to such an attack. This short video concludes with steps you can take to evade a vishing attack. | 2 minutes, 35 seconds |

## Microlearning Videos

These microlearning vidoes reinforce knowledge training, increse knowledge retention, and improve overall performance. All videos are in English.

| Course Code | Video Name | Video Description and Objectives | Duration |
|---|---|---|---|
| S-162-PW-01_EN | Password Strong | Passwords are the keys to our digital lives and allow us access to our many personal and work accounts. But how easy would it be for a hacker to crack your password? This video covers tips for creating strong passwords, and how you can protect yourself. | 1 minute, 24 seconds |
| S-162-RW-01-EN | Defending Against Ransomware | Ransomware is malicious software that prevents or restricts users from accessing computer systems or files until a ransom is paid. Computers typically become infected by ransomware when the user clicks on a malicious link or opens an infected attachment in an email. In addition to computers, ransomware can target mobile devices, smart TVs, and other Internet of Things (IoT) devices. This short video will provide the necessary information you need to help defend against ransomware. | 1 minute, 16 seconds |
| S-162-SE-01-EN | How to Defeat Social Engineers | Social engineers use deception to manipulate people into divulging confidential or personal information that may be used for fraudulent purposes. And you could be their next target. Protect yourself from a social engineering attack by applying the strategies learned from this short instructional video. | 54 seconds |
| S-162-SE-02-EN | The In-Personator: A Social Engineering Threat | Social engineers prepare themselves by thoroughly researching their targets before launching an in-person attack. They will often go as far as disguising themselves as a repair person, or maybe even impersonating a uniformed worker. Although social engineers can be tricky, you can prevent an in-person attack by following the tips outlined in this social engineering training video. | 1 minute, 21 seconds |
| S-162-SM-01-EN | Before You Post | Meet Bob. He's ready to take some much-needed vacation time. Before he starts his week-long adventure, he leaves a quick post on Facebook. Unfortunately, when Bob returns home, he finds that things are not quite the same. Watch this video to find out what happened to Bob and learn about social media best practices to follow when traveling. | 1 minute, 29 seconds |
| S-162-US-01-EN | USB Baiting: Don't Take the Bait | Compromised USB drives can be used to inject malicious code, redirect you to phishing websites, or give a hacker remote access to your computer. In this video, an employee is faced with a decision that could ultimately decide the fate of his organization. Watch to find out what he does (or doesn't do) to protect himself and what you can do to avoid being victimized by an uncanny social engineering attack. | 1 minute, 25 seconds |

# Suggested Role-Based Security Awareness Education Learning Paths

Each user is automatically assigned the general security awareness learning path. The organization's administrator can modify that learning path, or create a custom role-based learning path using the sugggested paths below. Or, if your organization prefers, create your own learning paths with a custom set of courses and microlearning videos. One license gives full access to our entire collection.

### Security First Learning Path

This learning path is designed for general office staff and employees who have access to sensitive information and includes a mixture of courses and microlearning videos.

- S-190-CQ-01-MTL Security Assessment
- S-202-SA-01-EN Introduction to Security Awareness (30 minutes)
- S-161-AP-07-MTL Coronavirus Phishes and Scams (5 minutes, 30 seconds)
- S-161-AP-01-MTL Defending Against Phishers (10 minutes)
- S-161-MD-01-MTL Protecting Mobile Data and Devices (8 minutes)
- S-161-ES-01-MTL Email & Instant Messaging Security (11 minutes)
- S-161-SM-02-EN Appropriate Use of Social Media (14 minutes)
- S-161-MA-03-MTL Ransomware: How to Defend Yourself (4 minutes)
- S-162-BE-01-EN The Business Email Compromise (1 minute, 38 seconds)
- S-162-RW-01-EN Defending Against Ransomware (1 minute, 16 seconds)
- S-161-MA-02-MTL The Malware Threat (5 minutes)
- S-161-PM-01-MTL Password Management (15 minutes)
- S-161-IR-01-MTL Incident Reporting (7 minutes)

### PCI Fundamentals

This learning path is designed for general or management staff tasked with compliance or risk program management responsibilities.

- P-101-PB-01-EN Privacy and Data Protection (30 minutes)
- PCI-202-IP-01-EN Introduction to PCI DSS (20 minutes)
- PCI-200-PB-01-EN Incorporating PCI DSS into BAU (20 minutes) (optional based on role)
- PCI-101-CS-01-EN PCI Essentials for Account Data Handers and Supervisors (20 minutes)
- PCI-201-RA-01-EN PCI DSS for Retail Associates (30 minutes) (optional based on role)
- PCI-120-IT-01-EN PCI SDD Requirements for IT Professionals (45 minutes) (optional based on role)

### Security and Privacy Awareness for Executives and Managers

This learning path is designed for executives who want an overview of security awareness and information privacy.

- S-202-SA-01-EN Introduction to Security Awareness (30 minutes)
- P-101-PB-01-EN Privacy and Data Protection (30 minutes)
- S-161-PS-01-MTL Physical Security (15 minutes)
- S-162-BE-01-EN The Business Email Compromise (1 minute, 38 seconds)
- S-161-AP-07-EN Coronavirus Phishes & Scams (5 minutes, 30 seconds)
- S-161-CS-01-MTL Cloud Security (9 minutes)
- S-161-IT-02-MTL Introduction to Insider Threats (7 minutes)
- S-161-WR-01-EN Working Remotely (8 minutes)

### Remote Worker

This learning path is designed for the remote worker and addresses risk connecting remotely.

- S-161-WR-01-EN Working Remotely (9 minutes)
- S-161-HS-01-MTL Internet of Things & Home Security (10 minutes)
- S-162-PW-01-EN Password Strong (1 minute, 24 seconds)
- S-161-ES-01-MTL  Email & Instant Messaging Security (11 minutes)
- S-161-AP-01-MTL Defending Against Phishers (10 minutes)
- S-162-HS-01-EN Home Cybersecurity (1 minute, 11 seconds)
- S-161-WR-02-MTL Working Securely from Home (9 minutes)

### Security and Privacy Awareness for Retail

This learning path is designed for retail managers and associates who have access to sensitive information.

- S-202-SA-01-EN Introduction to Security Awareness (30 minutes)
- P-101-PB-01-EN Privacy and Data Protection (30 minutes)
- S-161-PS-01-MTL Physical Security (15 minutes)
- S-161-PM-01-MTL Password Management (15 minutes)
- PCI-201-RA-01-EN PCI DSS for Retail Associates (30 minutes)
- S-203-RA-01-EN Secure Practices for Retail Associates (20 minutes) OR S-204-RM-01-EN Secure Practices for Retail Managers (20 minutes)
- PCI-200-PB-01-EN Incorporating PCI DSS into BAU (20 minutes) (optional based on role)

### Security and Privacy Awareness for Call Center

This learning path is designed for managers and employees of card-not-present environments.

- S-202-SA-01-EN Introduction to Security Awareness (30 minutes)
- S-205-CC-01-EN Secure Practices for Call Center Employees (20 minutes) OR S-206-CM-01-EN Secure Practices for Call Center Managers (20 minutes)
- P-101-PB-01-EN Privacy and Data Protection (30 minutes)
- S-161-PM-01-MTL Password Management (15 minutes)
- S-161-PS-01-MTL Physical Security (15 minutes)
- S-161-ES-01-MTL Email & Instant Messaging Security (11 minutes)
- S-162-PH-01-EN Phishing Defense Best Practices (52 seconds)
- S-162-PW-01-EN Password Strong (1 minute, 24 seconds)
- S-161-MA-02-MTL The Malware Threat (5 minutes)
- S-162-RW-01-EN Defending Against Ransomware (1 minute, 16 seconds)

### Security and Privacy Awareness for Compliance Managers

These learning paths are designed for compliance or risk program management responsibilities.

- P-101-PB-01-EN Privacy and Data Protection (30 minutes)
- S-202-SA-01-EN Introduction to Security Awareness (30 minutes)
- S-162-SE-01-EN How to Defeat Social Engineers (54 seconds)
- S-162-PW-01-EN Password Strong (1 minute, 24 seconds)
- S-161-ES-01-MTL Email & Instant Messaging Security (11 minutes)
- S-162-PH-01-EN Phishing Defense Best Practices (52 seconds)
- S-162-BE-01-EN The Business Email Compromise (1 minute, 38 seconds)
- S-161-MA-02-MTL The Malware Threat (5 minutes)
- S-162-RW-01-EN Defending Against Ransomware (1 minute, 16 seconds)
- S-162-MS-01-EN Living Mobile Secure (63 seconds)
- PCI-200-PB-01-EN Incorporating PCI DSS into Business As Usual Compliance (20 minutes)

Advanced:

- S-161-SE-02-MTL Defeating Social Engineers (Advanced) (17 minutes)
- S-161-PM-01-MTL Password Management (15 minutes)
- S-162-PH-02-EN Protecting Against Spear Phishers (49 seconds)
- S-162-PH-03-EN SMiShed! (1 minute, 38 seconds)
- S-162-PH-04-EN Dial V for Vishing (2 minutes, 35 seconds)
- S-161-AP-01-MTL Defending Against Phishers (10 minutes)
- S-161-MA-03-MTL Ransomware: How to Defend Yourself (4 minutes)
- S-161-PS-01-MTL Physical Security (15 minutes)
- S-161-MD-01-MTL Protecting Mobile Data and Devices (8 minutes)
- S-161-MA-05-MTL Preventing Malware: Mobile Devices (7 minutes)
- S-161-HS-01-MTL Internet of Things & Home Security (10 minutes)

### General Data Protection Regulation (GDPR)

This learning path is designed for general staff who require a general knowledge of GDPR.

- P-131-GD-01-MTL GDPR: Introduction and Overview (20 minutes)
- P-131-GD-02-MTL GDPR: Key Principles of the GDPR (15 minutes)
- P-131-GD-03-MTL GDPR: Transfers of Data Outside of the EU (15 minutes)
- P-131-GD-05-MTL GDPR: GDPR for Data Handlers (8 minutes)
- P-131-GD-04-MTL GDPR: Navigating GDPR with our US Partners (10 minutes)
- P-141-GD-01-EN GDPR: How to Comply with GDPR in the US (10 minutes)