SANS Security Awareness
2017 EndUser Module Descriptions

INTRODUCTION

The goal of SANS Security Awareness Training is to not only ensure you are compliant but also provide training that changes user behavior and helps your organization manage risk. We do this by using the CIS Critical Security Controls as a foundation for our training, combined with an advisory board of SANS top instructors and industry leading experts who train the world's info sec professionals. Our computer-based training package includes 38 different modules in 22 languages. This guide provides descriptions for each of the 2017 EndUser modules, as well as the features that are included in each category.

The following features are available:

- **Engagement Quizzes:** Mid-course quizzes to ensure students remain engaged throughout the curriculum.

- **End-of-Module Quizzes:** Each module concludes with an assessment to ensure the objective of the training has been met.

- **Interactivity:** Interactive modules include an activity following the video that engages Learners to apply the material. Interactivity lets Learners practice critical skills, so they can react properly when they encounter actual threats. You have the option to just assign a module with or without the interactive activity; you can also assign the interactive activity without the video.

NOTE: Interactive modules are available in English and Spanish ONLY.

- **Multiple Languages:** Videos are translated into several languages that a user can select based on his or her language preferences. Review the Languages section of this document for a complete list of available languages and details.

MODULE DESCRIPTIONS

RECOMMENDED CORE CURRICULUM

The Core Curriculum is intended to provide your entire organization with the training needed to be compliant with overall security awareness standards. The recommended modules portray realistic, memorable scenarios that are transferrable to everyday tasks. By completing the ten core training modules, Learners "build their shield" – an interactive process that balances the risks in the threat landscape with empowering and engaging messages, so Learners can protect themselves, their families, and their organizations.

Total Runtime	Engagement Quizzes	End-of-Module Quizzes	Interactivity	Available Languages
28:49	YES*	YES	ENGLISH SPANISH-LA	ALL

*The Conclusion module does not include an engagement quiz or have an interactive version.

You Are the Shield 01:05

This introduction explains how each person plays an important role in protecting your organization and how they are an information gatekeeper. In addition, we introduce the concept of creating a strong cyber shield and how this training will enable them to take control of and protect their cyber activities, both at home and at work.

Social Engineering 03:11

Social engineering is one of the most common types of cyber security attacks. This updated module explains what social engineering is, provides two different examples to demonstrate these types of attacks, and shows how people can detect and defend against them. As social engineering can take on any form, including phone calls, emails, text messages, social media, or in person, the module lays the foundation for what to do in the event of an attack.

Email, Phishing, and Messaging 04:21

Phishing is a cyber security attack that can be used to target many people at once or a small group, which is known as spear phishing. This updated module explains what generic and spear phishing are and how they work by using real-world email and text messaging examples. The module also reviews the warning signs of phishing and how employees can spot and stop such attacks.

Browsing Safely 02:16

Browsers are the primary tool people use to access the Internet. As a result, browsers and their plugins are a common target for attackers. In this module, employees learn how to browse safely, including keeping the browser and plugins updated, using HTTPS, and scanning what they download.

Social Networks 02:15

Social networking sites are a primary communication tool where people freely share information. We provide examples of the risks of sharing information online and steps that employees can take to prevent identity theft, spreading malware, scams, and targeted attacks.

Mobile Device Security 02:51

Mobile devices today have the same functionality, complexity, and risks as a computer, but with the additional risk of being highly mobile and easy to lose. Employees learn how to keep their mobile devices safe and secure, to include keeping them physically secure, using strong passcodes, and keeping the devices updated.

Passwords 03:28

Strong passwords and their safe use are some of the most effective ways to keep online accounts and information safe. This updated module explains why passwords are important, how to create a strong password using passphrases, and how two-step verification, combined with a password, increases security. The module also reviews safe password use behaviors, such as not sharing passwords, having a unique password for each account, and why using public computers for email, work accounts, and financial information is not safe.

Data Security 06:23

Safe data handling practices are critical at each step of accessing, sharing, transmitting, retaining, and destroying data. This updated module explains why it is important to only use authorized systems and only allow authorized personnel access to data. The module also describes ways to securely store or process sensitive information, restrictions on transferring or sharing information, ways to manage data retention, and how to destroy data securely. **Note: this module is required for most of the compliance videos.**

Hacked 02:25

A security incident or compromise can occur even with security controls and security awareness training in place. This updated module focuses on the warning signs that can be used to identify and report an incident. Warning signs include, but are not limited to, suspicious software, unauthorized charges to SMS numbers, unexplained data or device battery usage, pop-up messages indicating malware, anti-virus alerts, and passwords no longer working.

Conclusion 00:34

A short video wrapping up the training.

ADDITIONAL SECURITY AWARENESS VIDEOS

The following modules can be added to your curricula to provide information on security awareness topics relevant to your organization.

Total Runtime	Engagement Quizzes	End-of-Module Quizzes	Interactivity	Available Languages
44:05	NO	YES	NO	ALL

Targeted Attacks 03:51

Targeted attacks, such as spear phishing and CEO Fraud, involve extensive research on the target before the attack is launched. This NEW module provides a real-world example of how a targeted attack works and how everyone in an organization can protect against them.

Encryption 02:00

Encryption is a security control that protects the confidentiality and integrity of information. This updated module explains what encryption is and how an encryption key works to encrypt and decrypt information.

Insider Threat 03:32

Insider threats are trusted employees, contractors, or third-party members who exploit their insider status and maliciously cause harm to an organization. This updated module explores new examples of insider threats, warning signs of an insider threat, and how to reduce the likelihood of an attack by using strong organizational security practices.

Malware 02:51

Malware is software that is used to perform malicious actions. This NEW module explains what malware is and how it works, to include two examples: keyloggers and ransomware. The module also reviews misconceptions about malware, the importance of backups, and the need to report an infection as soon as it happens.

Creating a Cyber Secure Home 03:29

Effective cyber security practices are important both at work and at home. This NEW module describes the steps that can be used at home to protect personal devices, Wi-Fi networks, and online accounts. It also covers the importance of information backups, such as Cloud services or external hard drives, in the event of an attack, theft, or loss of a device. Secure behaviors at work often start at home.

Protecting Your Kids Online 04:37

Kids' social lives and future depend on their ability to use technology safely and securely, and as a parent, you want to give them freedom while protecting them. This module is not specific to securing organizations, but it is a powerful way to engage employees and promote your awareness program by focusing on online safety at home.

Physical Security 02:51

Physical security is an important component of information security. We explain how attackers will attempt to trick and fool their way into restricted areas. We also discuss how employees can protect the physical security of your facilities, the importance of proper information disposal, and maintaining physical control of any devices while traveling.

SANS Security Awareness
2017 EndUser Module Descriptions

Working Remotely 02:43

For many organizations, employees no longer work at the office. As a result, working remotely securely is more important than ever whether traveling, working from a local cafe or at home. In this updated module, we review how employees can protect themselves by using secure network connections, managing laptop and device security, and following workplace policies to keep them and your organization safe.

Cloud Services 02:28

Cloud services enable data storage and sharing, potentially increasing employee productivity while reducing organizational costs. However, employees must understand that authorized use of Cloud services must occur safely and securely. This module explains these risks to employees and shows them how to safely use authorized Cloud providers in your organization.

Help Desk 03:40

The help desk is often a targeted group within an organization. These people are trained to communicate with and assist a variety of strangers over the phone. As such, additional steps must be taken to both educate and protect these individuals.

Information Technology Staff (IT Staff) 04:20

Your IT staff has privileged access to your critical systems, and it is very important that they are secure. We discuss how your IT staff can protect themselves and your organization, including proper use of privileged accounts, limiting the information they share, and how they can detect if a system is compromised.

Senior Leadership 04:56

Senior leaders and their staff are a primary target, especially in today's world of targeted attacks. This module covers important concepts, such as how to be secure when traveling, proper mobile device use and security, the most common indicators of targeted attacks, and how to set the example to help build a secure culture.

International Travel 02:47

This module explains the risk while traveling internationally and steps employees can take to protect themselves and their information.

COMPLIANCE VIDEOS - INTERNATIONAL

The following modules review a variety of compliance standards. **Note: Some compliance videos build upon information covered in the Data Security core curriculum module. Employees will need to watch Data Security prior to watching the associated compliance module.**

Total Runtime	Engagement Quizzes	End-of-Module Quizzes	Interactivity	Available Languages
19:38	NO	YES	NO	ALL

Payment Card Industry Data Security Standard (PCI DSS) 03:46

Prerequisite: Data Security

If your organization stores, transmits, or processes any cardholder data, it is required to follow PCI DSS. This updated module can be used to comply with updated PCI DSS version 3.2 standards.

EU Data Protection 03:45

The European Union's Data Protection Directive is concerned with any information that, either by itself or used with other pieces of information, could identify a living person. This module explains what EU protected data is and the EU guidelines on how it should be collected, handled, protected, and disposed.

EU General Data Protection Regulation 03:54

The European Union's standards for General Data Protection will be changing in 2018 and this NEW module explains the expanded requirements for data collection, handling, protection and disposal.

Privacy 02:16

This module explains what privacy is, why it's important (including respecting the privacy of others), and steps people should take to protect it. This module does not apply to any specific law, regulation, or standard. Instead, it is an overview of privacy concepts and their importance.

Personally Identifiable Information (PII) 03:14

Prerequisite: Data Security

This module explains what PII is and the extra steps employees must take to protect it and other types of confidential information. Examples include the use of encryption and personal email accounts, the sharing of sensitive information, using only authorized systems to store or process sensitive information, and securely disposing of sensitive data.

Ethics 02:43

Ethics is about doing the right thing even when it's difficult. This updated module describes challenging situations employees may be confronted with, such as managing unexpected gifts or related conflicts of interest, how to manage uncertain behavior, and knowing when to approach a supervisor or human resources with concerns.

COMPLIANCE VIDEOS - UNITED STATES

The following modules review different United States compliance standards. **Note: Some compliance videos build upon information covered in the Data Security core curriculum module. Employees will need to watch Data Security prior to watching the associated compliance module.**

Total Runtime	Engagement Quizzes	End-of-Module Quizzes	Interactivity	Available Languages
36:58	NO	YES	NO	SPANISH-LA

Health Insurance Portability and Accountability Act (HIPAA) 02:57

Prerequisite: Data Security

This module explains what Protected Healthcare Information (PHI) is and covers the steps required to store, process, and use it. If your organization stores, transmits, or processes any PHI, it is required to follow this standard.

Family Educational Rights and Privacy Act (FERPA) 04:37

Prerequisite: Data Security

The Family Educational Rights and Privacy Act, also known as FERPA, is a federal law that protects the privacy of student education records. In this updated module, we review the rules and regulations all school faculty, staff, contractors, and student employees should follow when handling student information.

Gramm-Leach-Bliley Act (GLBA) 02:28

Prerequisite: Data Security

This module explains what GLBA is, what nonpublic personal information (NPI) is, and the steps that employees must take to protect it to ensure your organization remains compliant. The focus of the module includes both educational and financial examples.

International Traffic in Arms Regulations (ITAR) 05:30

The U.S. government enforces a complex regime of export controls, trade sanctions, and other requirements to prevent certain items, including data, software, and technology, from going to unauthorized people, entities, and countries. This module covers guidelines on when ITAR applies to your organization and its research, along with the steps needed to protect it.

Foreign Corrupt Practices Act (FCPA) 03:45

The Foreign Corrupt Practices Act applies to any organization that does business in the U.S. or has stocks, bonds, or other securities traded in U.S. markets. This module explains what FCPA is, why it's important, and the rules and processes that employees are expected to follow in order to be in compliance with it.

Federal Personally Identifiable Information (Federal PII) 03:32

Any Personally Identifiable Information (PII) that comes from federal agencies is protected by federal law. This data has special and very specific policies on how it must be protected. This module explains what Federal PII is and the steps people need to take to protect it.

Federal Tax Information 03:44

Any organization working with federal tax information is regulated by federal law and required to take specific steps to protect that data. This module explains what federal tax information is and details the steps that must be taken to protect data in order to keep your organization compliant.

Criminal Justice 03:27

The criminal justice and law enforcement communities have several unique requirements for the use and handling of information they collect in their daily jobs and activities. This module explains those requirements, including authorized and unauthorized information sharing, data access, and how to avoid unsafe behaviors.

Red Flags Rule 04:11

The Red Flags Rule is a federal regulation that requires organizations to implement an Identity Theft Prevention program designed to detect the warning signs of identity theft. This module explains what these red flags are, what to look for, and the actions to be taken for data protection.

Client Confidentiality in Law Offices 02:47

This module gives an overview of how client data is at risk in law firms, why lawyers need to protect it, and key steps they need to take to do so. This module is unique in that it uses terminology specific to the legal industry.

LANGUAGES

The following is a list of supported content languages. Modules can be viewed in the languages listed within each module's description.

Languages	Notes
Arabic	
Chinese Simplified / Mandarin	Videos are spoken in Mandarin with subtitles in Simplified Chinese
Chinese Traditional / Cantonese	Videos are spoken in Cantonese with subtitles in Traditional Chinese
Czech	
Dutch	
English-UK	British English
English-US	American English
Finnish	
Flemish	
French	International/European French
French-CA	Canadian French
German	
Hungarian	
Indonesian	
Italian	
Japanese	
Portuguese-BR	Brazilian Portuguese
Russian	
Spanish-LA	Latin American Spanish
Thai	
Subtitles Only	
Korean	Videos are spoken in US English with subtitles in Korean
Polish	Videos are spoken in US English with subtitles in Polish
Spanish-International/European	Videos are spoken in US English with subtitles in Spanish
Swedish	Videos are spoken in US English with subtitles in Swedish