SECURITY AWARENESS TRAINING MODULES

KEVIN MITNICK SECURITY AWARENESS TRAINING

Included in Training Access Level I

Kevin Mitnick Security Awareness Training

45 minutes

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. Three real-world scenarios show you strategies and techniques hackers use to take control of your computer system. Kevin Mitnick then takes you behind the scenes to see how the bad guys do what they do. You'll learn about the seven areas of an email that can contain red flags that alert you to a possible attack. The Danger Zone exercise will let you apply what you've learned when you help Jake Saunders, a typical computer user, steer clear of six real-world social engineering attacks.

Kevin Mitnick Security Awareness Training

15 minutes

This module is a condensed version of the full 45-minute training, often assigned to management. It covers the mechanisms of spam, phishing, spear phishing, spoofing, malware hidden in files, and advanced persistent threats (APTs). This module is available in 26 language versions.

Ascend TECHNOLOGIES

SECURITY AWARENESS TRAINING MODULES

Included in Training Access Level II

Security Awareness Training Course

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. Three real-world scenarios show you strategies and techniques hackers use to take control of your computer system. You'll learn about the seven areas of an email that can contain red flags that alert you to a possible attack. The Danger Zone exercise will let you apply what you've learned when you help Jake Saunders, a typical computer user, steer clear of six real-world social engineering attacks.

Basics of Credit Card Security

This 20-minute module covers the basics of credit card security. It is meant for all employees in any organization who handle credit cards in any form, whether taking orders on the phone, swipe cards on terminals or through devices connected to smart phones. It teaches employees to handle credit card information securely to prevent data breaches. Different types of cards are covered, which specific elements the hackers are after, and explains how malware like keyloggers, password crackers, and spyware can endanger credit card information. Employees are taught the rules for paper copies of credit card data, and things to remember during data entry, including things NOT to do like sending credit card information through email and text and more. A quiz ends off this module.

CEO Fraud

In this engaging and interactive module, you will learn how to defend yourself against what the FBI calls business email compromise and what is commonly known as CEO fraud. You will also learn how and why these attacks occur as well as how to protect your organization from this serious threat and then apply this knowledge in a short exercise.

Common Threats Part 1 & 2

In these modules you'll learn about strategies and techniques hackers use to trick people just like you. We introduce you to Miranda and Kyle as they each deal with three real-world-based scenarios that show you how these common threats can take place. At the end of each scenario, Kevin Mitnick will take you behind the scenes and reveal exactly how each type of hack is accomplished.

Creating Strong Passwords

In this interactive course you will learn about the important rules for creating strong passwords, you'll test a password to see how strong it is, and learn about the latest trend in password security, the passphrase, and how to create one.

GDPR

This interactive module provides an overview the General Data Protection Regulation. The goal of this module is to familiarize you with the General Data Protection Regulation, also known as the GDPR; what it means to your organization; and what it means to your job function. There are ungraded knowledge checks along the way to help you retain information for real-life scenarios, followed by a graded quiz at the end.

Handling Sensitive Information

This 15-minute module of the Kevin Mitnick Security Awareness Training series specializes in making sure your employees understand the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI), Credit Card data (PCI DSS), Controlled Unlimited Information (CUI), including your organization's proprietary information and are able to apply this knowledge in their day-to-day job for compliance with regulations. A version for Canada is also available.

Mobile Device Security

This 15-minute module specializes in making sure your employees understand the importance of Mobile Device Security. They will learn the risks of their exposure to mobile security threats so they are able to apply this knowledge in their day-to-day job.

PCI Compliance Simplified

This 15-minute module uses real examples of credit card fraud, and how to protect your organization against this by being PCI compliant. This course is for anyone that's responsible for handling credit cards in your organization and qualifies as Security Awareness Training. Especially owners, the CFO or Controller, managers and IT people in charge of credit card processing should take this course. The training covers topics like Merchant levels, Merchant types, Self Assessment Questionnaires, new changes in the industry,

SECURITY AWARENESS TRAINING MODULES *CONT.*

chip cards, TIP Program, Qualified Integrated Resellers and the key security requirements for any organization.

Ransomware

This fun and engaging course will show you what ransomware is, how it works, and how to steer clear of potential threats. You'll meet Sergeant Vasquez, head of the cyber security task force as he takes you through a line-up of the top attack vectors that bad guys use to hold your computer systems hostage until you pay the ransom.

Ransomware For Hospitals

Hospitals are currently targeted by cyber criminals, penetrating their networks and locking patient files with crypto-ransomware so that no data is accessible for any hospital worker. This short (7-minute) module gives anyone working in a hospital the basics of ransomware, email security and Red Flags they need to watch out for to help prevent very expensive attacks like this.

Safe Web Browsing

This 10-minute module takes employees through the basics of safe web browsing. They will learn how to avoid common dangers and the "do's and "don'ts" of safe web browsing. This module is set up to be fully interactive and could be presented as a quiz to take and "see how much you know."

Social Engineering Red Flags

This interactive module shows you the seven areas of an email to pay attention to if you don't want to be hacked. Once you know where to look, it shows seven real-life examples, and you'll be asked to spot the red flags in each.

The Danger Zone

In this 10-minute module, you will learn to spot real-world social engineering attacks by helping to guide Jake Saunders, a typical computer user, through six potential social engineering attacks. Jake needs to make the right decisions or suffer the consequences.

Your Role, Internet Security and You

Today's threats are sleek, sophisticated, and very slippery. They can slide right through your organization's antivirus software and spam filters and go straight to your inbox. This is a high quality, 9-minute course takes you on a tour of the threat landscape and shows you some of the common ways the bad guys try to trick you.

FINANCIAL INSTITUTION TRAINING MODULES

Included in Training Access Level II

Financial Institution Physical Security

This 20-minute module covers the protection of your employees, your customers and their funds, the premises, any security devices, computers, and networks, from physical circumstances and events that could cause serious losses or damage. This includes protection from robbery, kidnap/extortion, bomb threat, fire, natural disasters, burglary, and nuclear emergencies.

GLBA Security Awareness Training

In this module, employees of financial institutions are stepped through the concepts of "Non-Public Personal Information", or NPPI, best practices for protecting customers' personal information, the employee's role in ensuring protection of NPPI, what is social engineering and how not to get tricked, how to protect against unauthorized access and misuse of protected information, and how to provide notice of an incident that may compromise customer information security.

TRAINING MICRO-MODULES

Included in Training Access Level II

Executive Series Micro-Modules

Includes: CEO Fraud, Decision-Maker Email Threats, Mobile Device Security, Ransomware and Bitcoin, Remote and Travel WiFi Dangers, Safe Web Browsing With Corporate Devices, Secure Destruction of Sensitive Information, Securely Working From Home, Social Engineering the Executive, and Social Media Precautions for Executives.

Captain Awareness Series

Includes: Be a Human Firewall, Conquer Internet Safety for Kids, Securing Your Mobile Devices, Triumph over the Reuse of Passwords, Understanding GDPR, Securely Working from Home, Be Vigilant with USB Drives, Outwit Dumpster Divers, Travel Securely, Handling Printouts, Understanding Data Breaches, Safeguard Social Media, Protect Your Web Browser, Guardians of Sensitive Information, Vanquish Malicious Attachments, Outwit Social Engineering, and more.

Credit Card Security (Parts 1 & 2)

The first 5-minute micro-module covers why it's so important to protect credit card information; what hackers are after, how employees are a key factor in keeping credit card information secure; and how malware can be used to capture this information. Next, learn the rules for safely storing (and sharing) credit card information.

Danger Zone Exercise Micro-module

This 5-minute micro-module is an interactive course all about phishing. There are four scenarios where the learner is asked to spot the potential threat. Each scenario provides valuable feedback based on the learner's responses. There are two versions of this course, one with sound and one without.

Don't Be Dave

This 90 second video shows two of the worst things you can do with your password.

Email Spoofing

This 5-minute micro-module covers the very important topic of email spoofing. It defines social engineering and shows how hackers can infiltrate an organization and create spoofed emails that trick unsuspecting employees. It also covers a real-life example of just how dangerous email spoofing can be.

Handling Sensitive Information Securely (Parts 1 & 2)

These 5-minute micro-modules cover the basics of safely handling sensitive information and goes into Personally Identifiable Information (PII) and Protected Health Information (PHI).

Ransomware

This powerful 5-minute micro-module takes an employee through the basics of ransomware, the different methods used to infect a machine, and how hackers trick unsuspecting users into downloading infected files.

Safe Web Browsing

This 5-minute micro-module takes employees through the basics of safe web browsing. Participants will learn how to avoid common dangers and discover the "dos and don'ts" of safe web browsing.

Social Engineering

This 5-minute micro-module defines social engineering and describes what criminals are after. It covers the three main areas of attack: digital attacks, in-person attacks, and phone attacks.

Social Media Best Practices

This 5-minute micro-module provides a brief overview of best practices that businesses and employees can implement to prevent attacks and protect sensitive information from social media hackers.

Strong Passwords

This 5-minute micro-module covers the rules of how to create and use strong passwords in both an office environment and at home. Employees learn the 10 important rules for safer passwords, minimum password length, and how to remember long passwords.

USB Attack

This 5-minute micro-module covers the risks of picking up a USB stick and plugging it into a workstation.

SECURITY AWARENESS CONTENT LIBRARY

Included in Training Access Level III

Cybersecurity Awareness Interactive Training Modules

Active Shooter & Physical Incident Response
Call Center & Help Desk Awareness
Computer Security & Data Protection
Cross Border Data Protection
Data Classification
Developing an Incident Response Plan
Empowering Your Employees for Better Security
Executive Awareness Leadership
How to be a Human Firewall
Identification & User Authentication
Identity Theft and Data Breaches
Insider Threats for Executives and Managers
Malware
Mobile Security Basics
Non-technical Security Basics
OWASP Top 10
PCI DSS Retail Store Experience
Password Basics
Phishing Andrew's Inbox
Phishing Awareness
Phishing Fundamentals
Privacy Basics
Ransomware
Secure Online Behavior
Security Awareness Fundamentals
Security Triads
Social Engineering
Social Engineering & Phishing for Executives
Social Engineering Basics
The Top 10 Security Awareness Fundamentals Test Out
Top 10 Security Awareness Fundamentals for New Hires
Understanding and Mitigating Security Risks for Executives
Understanding and Protecting PII
Workforce Safety & Security Awareness
Workplace Violence and Safety

Cybersecurity Awareness Compliance Modules

FERC/NERC for End Users
FERC/NERC for Managers and Executives
FERPA (Education)
FFIEC (Financial Compliance)GLBA (Finance)
HIPAA (Healthcare)
PCI-DSS (Retail Compliance)
Sarbanes-Oxley (Accounting)

Cybersecurity Awareness Newsletters and Security Docs

13 Habits of Savvy SM Users
5 Examples of Social Engineering
5 Steps to Prevent ID Theft
5 Steps to Prevent ID Theft
5 Traits of a Security Aware Employee
7 Tips for Travelers
A Real Life Spear Phishing Attack
Access Controls
Advanced Persistent Threats
Are Your Things Part of a Botnet?
Back to School Security Checklist
Bad Passwords
Bank Secrecy Act
Being a Human Firewall in All Three Domains
China's Cybersecurity Law
Click With Care
Confidentiality
Cross Border Data Protection Overview
DIY Home Internet Security Policy
Data Breaches and You
Data Classification at Home
Data Classification at Work
EU GDPR: The Basics
Field Guide to Phishing Emails
Following Policy and Reporting Incidents
Forms of Social Engineering
Hey! That's my pie! Oops, I mean PII
How VPNs Work
How to Identify a Social Engineering Attack
In Case of Emergency

Cybersecurity Awareness Newsletters and Security Docs *Cont.*

Incident Response in Action
Incident Response in All Three Domains
Integrity
IoT Gone Rogue
Keeping Kids Safe on Social Media + 10 Tips for Parents
LinkedIn Scams & It's a Spammer's World
Malware on the go!
Non-technical Security in ALL THREE DOMAINS
PHI stands for Protected Health Information
PII: To Prominent Constant of Information Security
Passphrases: The Smart Alternative
Phishing In Action
Privacy vs. Security
Proven Password Policies
Ransomware Security One Sheet
Redefining What it Means to be a Human Firewall
Regulations Near and Far
Respecting Privileged Access
Securing Mobile Devices
Securing Smart Devices
Security Incidents and Where to Report Them
Shipshape SM Behavior
Simple Steps to Online Safety
Smishing: Phishing Gone Mobile
Spam Emails vs Phishing Emails
The CIA Triad: Security to the Power of Three
The Cloud Is Not Yours
The Domains Triad: Mind, Body, and Soul
The Future of Identification and Authentication
The Horrors of Malware
The Importance of Data Classification
The Internet of Things and the Concerns of Convenience
The Journey to Being Anonymous on the Internet
The Many Lives Triad
The Many Lives of PII
The Physical Side of Security Awareness
The Rule of Three
The Three Domains of Social Engineering
The Three Lives of Incident Response
The Underground Marketplace and Common Cyber Attacks
Tis the Season..... for Scams
Top 10 Security Practices for Work
Top 10 Ways to Stay Safe at Home
Top 10 Ways to Stay Secure on the Go
Understanding BEC
Understanding Compliance Standards
Understanding Insider Threats
Understanding Insider Threats & Offboarding
Understanding the Attackers
Whale and Spear Phishing
What is A Human Firewall?
What is NIST Cybersecurity Framework?
What is Privacy Shield?
What's the WiFi Password?
Where Do You Hide Your Passwords?
Where in the World is Ransomware
Where's the Remote
Who are Cybercriminals
Why Does Compliance Matter
You Need a PW Manager

Cybersecurity Awareness Videos (2-5 mins)

10 ways to avoid phishing scams
10 ways to keep PII private
10 ways to stay safe on social media
A Day of Bad Passwords
Backup
Being a Human Firewall
Beyond Phishing
Catching Malware
Cyber Crime Starts with You
Dangers of USBs
Data Breach Overview
Data Breaches and You
Data Classification Overview
Data Loss and Insiders
Definition of Social Engineering
Dumpster Diving
Email Spoofing
Executives Mitigating Insider Threats
Hide your passwords
Human Firewall and Data Classification
Incident Response 101
Introduction to Ransomware
Introduction to the cloud
Low-Tech Hacks to Steal Your ID
Mouse Overs
Non-Technical Security Skills
Non-Technical and Physical security tips and tricks
PII and Compliance
Phishing Contest Winner
Phishing From Facebook
Phishing From Netflix
Phishing From Your Ban
Phishing in Action
Physical Security Threats

Cybersecurity Awareness Videos (2-5 mins) *Cont.*

Pretexting: (Fake Fraud Protection)
Pretexting: (Fake Help Desk)
Pretexting: Fake Employee to Help Desk
Pretexting: Fake Executive to I.T.
Pretexting: From Fake Credit Card Company
Pretexting: From Fake I.T.
Privacy Vs. Security
Protecting Data
Road Warriors
Safe Surfing 1 - HTTP vs HTTPS & Online Authentication
Security Myths Busted
Social Media
Social Media Data Mining
Social Networking Do's and Don'ts
The CIA Triad
The Domains Triad
The Human Firewall's Top Concerns in All Three Domains
The Many Lives Triad
The Many Lives of PII
Understanding Encryption
Welcome to Security Awareness Training
Welcome to Security Awareness Training - Animated
What Are APTs
What Does a Social Engineer Look Like?
What is I.D. Theft
What is PII?
Why Executives Need Awareness Training
Why Security Awareness?
Workplace Physical Awareness
Your Security Awareness Journey

Cybersecurity Awareness Games

End of the Day Security Challenge
Human Firewall Big Business
Human Firewall Trivia
Human Firewall World Race
Password Big Business Game
Password World Race Game
Phishing Awareness Big Business
Phishing Awareness Trivia
Phishing Awareness World Race
Security Awareness World Race
Security Awareness Big Business
Security Awareness Card Stack
Security Awareness Casino Challenge
Security Awareness Trivia
Social Engineering & Phishing Millionaire Challenge
Social Engineering Big Business Game
Social Engineering Trivia
Social Engineering World Race Game

Also includes over 120+ Security Awareness Posters