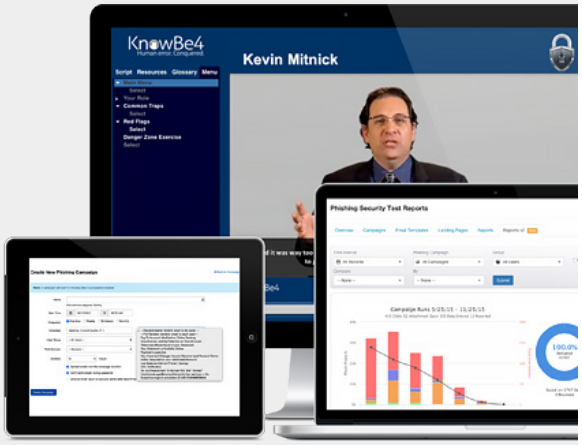
Overview of KnowBe4 Training Modules

KnowBe4
Human error. Conquered.



KnowBe4's game-changing partnerships with The Security Awareness Company, Securable.io, and AwareGO allows you to significantly better manage the ongoing problem of social engineering. We offer you the best-in-class phishing platform combined with the world's largest library of always-fresh security awareness training content; including interactive modules, videos, games, posters and newsletters.

To easily deliver this content library to customers, KnowBe4 has a 'Module Store'. As a customer, you can use the ModStore to search, browse, and preview content and -- depending on subscription level -- move modules to your KnowBe4 account.

We offer three Training Access Levels: I, II, and III, giving you access to a constantly updated content library of 500+ items based on your subscription levels.

Kevin Mitnick Security Awareness Training

Included in Training Access Level I

Kevin Mitnick Security Awareness Training (45-min)

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. This module is available in six additional language versions: French - European, French - Canadian, German, Polish, Spanish, and British English.

Kevin Mitnick Security Awareness Training (25-min)

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. You'll learn how to spot red flags that alert you to possible danger in an email and then you'll help Jake Saunders, a typical computer user, steer clear of six real-world social engineering attacks.

Kevin Mitnick Security Awareness Training (15-min)

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.

KnowBe4 Training Modules

Also included in Training Access Level II

KnowBe4 Basic Security Awareness Training Course (30-min)

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 Sanders, 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.

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.

Handling Sensitive Information Securely

This 15-minute module 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.

Mobile Device Security

Hackers want to use your mobile device as a gateway to your organization's data. This interactive module puts the power in your hands so you can protect that data. You will learn about the dangers surrounding Bluetooth, WiFi, apps, and even human error. You will also learn how to protect your organization from these threats, then apply this knowledge in three real-life scenarios.

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.

Safe Web Browsing

In this fun, fully interactive course you will learn about interesting facts about the World Wide Web, how to avoid common dangers, and the "do's and "don'ts" of safe web browsing.

Ransomware

This fun and engaging course will show you what ransomware is, how it works, how to steer clear of potential threats, and how to identify the top attack vectors that bad guys use to hold your computer systems hostage.

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.

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. After the training, you are able to download essential references regarding being or becoming PCI compliant.

GDPR

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.

KnowBe4 Training Modules

Also included in Training Access Level II

Common Threats

In this 15-minute module you'll learn about strategies and techniques hackers use to trick people just like you. We provide you 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.

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.

Financial Institution Physical Security (for Financial Institutions only)

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.

Your Role

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 that takes you on a tour of the threat landscape and shows you some of the common ways the bad guys try to trick you.

Red Flags: Warning Signs that Alert You

This fully interactive 8-minute 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.

GLBA Compliance Course (for Financial Institutions only)

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.

KnowBe4 Training Micro-modules

Also included in Training Access Level II (and each around 5 minutes)

Credit Card Security (Part 1)
Credit Card Security (Part 2)
Danger Zone Exercise Micro-module
Email Spoofing
Handling Sensitive Information Securely (Part 1)
Handling Sensitive Information Securely (Part 2)
Ransomware
Safe Web Browsing
Social Engineering
Social Media Best Practices
Strong Passwords
USB Attack

Executive Series Micro-modules

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

Security Awareness Company Content Library

Also included in Training Access Level III

Cyber Security Awareness Interactive Training Modules

Call Center and Help Desk
Computer Security and Data Protection
Data Classification
Identity Theft and Data Breaches
Insider Threats for Executives and Managers
OWASP Top 10
Phishing Andrew's Inbox
Phishing Awareness Pre-Assessment
Phishing Awareness Post-Assessment
Privacy Basics
Ransomware
Security Awareness Fundamentals
Security Awareness Fundamentals Post-Assessment
Security Awareness Fundamentals Pre-Assessment
Understanding and Protecting PII
Welcome to Security Awareness Training - Animated

Cyber Security Awareness Compliance Modules

FERPA (Education)
FFIEC (Financial Compliance)
GLBA (Finance)
HIPAA (Healthcare)
HIPAA for Non-Medical Professionals (Healthcare)
PCI-DSS (Retail Compliance)
Sarbanes-Oxley (Accounting)
Workforce Safety & Security Awareness

Cyber Security Concepts Training Modules

Active Shooter and Physical Incident Response
Call Center and Help Desk Awareness
Computer Security and Data Protection
Data Classification
Executive Awareness and Leadership Module
How to be a Human Firewall
Identification and User Authentication
Malware
Mobile Security Basics
Non-Technical Security
Password Basics
Phishing Awareness
Privacy
Secure Online Behavior
Security Triads
Social Engineering
The Top 10 Security Awareness Fundamentals
Top Ten Security Awareness Issues for New Hires
Understanding and Protecting PII
Workplace Violence and Safety

20+ Cyber Security Awareness Games

140+ Cyber Security Awareness Posters

Cyber Security 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
APTs
Back Up
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 Insider
Definition of Social Engineering
Dumpster Diving
Email Spoofing
Examples of Insider Jobs
Examples of Phishing
Firewalls
Free Wifi
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
Making Strong Passwords
Mobile Cyber Crime
Mobile Security Overview
Mouse Overs
Non-Technical Security Skills
Non-Technical and Physical security tips and tricks
Password Security
Phishing Contest Winner
Phishing From Facebook
Phishing From Netflix
Phishing From Your Bank
Phishing in Action
Physical Security Threats
PII and Compliance
Pretexting 1 (Fake Fraud Protection)
Pretexting 2 (Fake Help Desk)
Pretexting From Fake I.T.
Pretexting: Fake Employee to Help Desk
Pretexting: Fake Executive to I.T.
Pretexting: From Fake Credit Card Company
Privacy Vs. Security
Proper Hard Drive Disposal
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't's
Spam
The CIA Triad
The Domains Triad
The Human Firewall's Top Concerns in All Three Domains
The Many Lives of PII
The Many Lives Triad
Types of Social Engineering
Understanding Encryption
What Does a Social Engineer Look Like?
What is I.D. Theft
What is PII?
Why Executives Need Awareness
Why Security Awareness?
Your Security Awareness Journey

Securable.io Videos

Also included in Training Access Level III

FISMA- Federal Information Security Management Act
Intro to Phishing
LinkedIn Security
Monitoring Facebook Services
Protect Your Kids Online
Public WIFI Safety
Ransomware Attacks
Traveling Abroad
Twitter Security
USB Safety

AwareGO Videos

Also included in Training Access Level III

CEO Scam
Chain Mail
Clean Desk
Dumpster Diving
Free WiFi
Handling Confidential Material
Home WiFi
HTTPS
Keylogger
Malicious Attachments
Password Handling
Passwords
Phishing
Pop Ups
Printouts
Removable Media
Shoulder Surfing
Social Engineering
Software Installs
Spear Phishing
Spyware
Tailgating
Think Twice
USB Key Drop

Security Awareness Training Content By Subscription Level

TRAINING CONTENT	SILVER	GOLD	PLATINUM	MOST POPULAR DIAMOND
Training Modules	3	21	21	53
Micro Modules		23	23	50
Compliance Modules		6	6	16
Games				26
Videos (3-5 min)				84
Posters / Images				171
Newsletters / Security One Sheets & Digests				126

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com