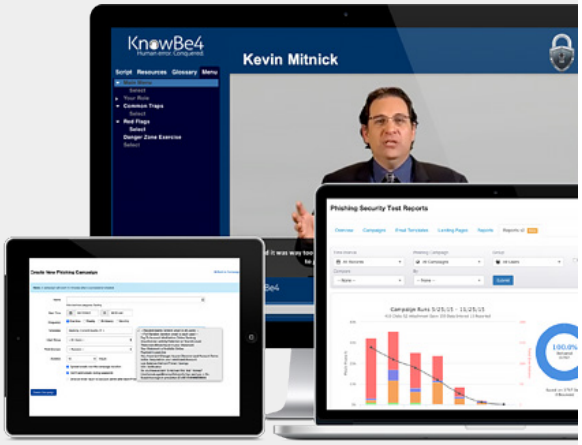
Overview of KnowBe4 Training Modules

KnowBe4
Human error. Conquered.



KnowBe4's game-changing partnerships with The Security Awareness Company, Securable.io, AwareGO, Popcorn Training, ThinkHR and exploqii 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.

If you want to get a real-time view of all the great content, sign up to access the KnowBe4 ModStore Training Preview to see our full library!

Kevin Mitnick Security Awareness Training

Included in Training Access Level I (Silver)

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 (Gold & Platinum)

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 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 - Miranda's Story

In this 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.

Common Threats, Part 2 - Miranda's Story

In this module you'll learn about strategies and techniques hackers use to trick people just like you. We introduce you to Kyle Montgomery as he deals with three real-world-based scenarios: Ransomware, Spearphishing, and a Snapchat attack to 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.

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.

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.

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.

Handling Sensitive Information

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 for compliance with regulations.

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.

KnowBe4 Training Modules

Also included in Training Access Level II (Gold & Platinum)

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, 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 our 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 Training

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

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.

Social Engineering Red Flags

This totally 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.

KnowBe4 Training Micro-modules

Also included in Training Access Level II (Gold & Platinum)

Credit Card Security (Part 1)
Credit Card Security (Part 2)
Danger Zone Exercise
Don't Be Dave
Email Spoofing
Handling Sensitive Information Securely (Part 1)
Handling Sensitive Information Securely (Part 2)
How to Stay Safe for the Holidays
Ransomware
Safe Web Browsing
Social Engineering
Social Media Best Practices
Strong Passwords
USB Attack

Executive Series Micro-modules

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
Social Media Precautions for Executives

Security Awareness Company Content Library

Also included in Training Access Level III (Diamond)

Cyber Security 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
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
OWASP Top 10
PCI DSS Retail Store Experience
Password Basics
Phishing Andrew's Inbox
Phishing Awareness
Privacy Basics
Ransomware
Secure Online Behavior
Security Awareness Fundamentals
Security Triads
Social Engineering
Social Engineering & Phishing for Executives
The Top 10 Security Awareness Fundamentals Test Out
Top 10 Security Awareness Fundamentals for New Hires
Understanding and Protecting PII
Workforce Safety & Security Awareness
Workplace Violence and Safety

Cyber Security 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)

100+ Cyber Security Awareness Newsletters & Security Docs

15+ Cyber Security Awareness Games

150+ 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
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
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 Bank
Phishing in Action
Physical Security Threats
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?
Your Security Awareness Journey

Popcorn Training Content

Also included in Training Access Level III (Diamond)

Popcorn Training Modules

Something Phishy Series Videos & Quiz (Animated)
Something Phishy Introduction
Mobile Mayhem (mobile threats)
Pass the Password (passwords, social engineering)
Break the Barrier (physical, clean desk)
Phisheous Malicious (Internet use)
Dicey Devicey (BYOD Security)
Freaky Leaky (DLP)
Cloudy with a chance of Phish (Cloud Apps)
Social Media Fever (Social Network Security)
Cyber Heroes Series Videos & Quiz (Live Action)

Cyber Heroes Introduction
Don't take the bait (spear-phishing, social engineering, vishing)
Mobile Mayhem (mobile threats)
Pass the Password (pass word, social engineering)
Phisheous Malicious (Internet use)
Dicey Devicey (BYOD Security)
Freaky Leaky (DLP)
Cloudy with a chance of Phish (Cloud Apps)
Social Media (Social Network Security)

Privacy Series Videos and Quiz (Live Action)
Personal Information–Currency of the 21st Century
Identity Theft–Protect your Personal Information
Privacy Principles–Handling Personal Information at Work
Protecting Personal Information–Security & Safeguards
General Data Protection Regulation (GDPR)–User Rights

Security Moment Short Clip Videos & Quiz (Motion Graphic)
The Big Phish 1
Ransomware
Social engineering 101
Spot the fake attachment
Spot the fake link
Privileged user access management (PAM)

Secure Coding 6 Module Course for Developers Video & Quiz (Animated & Motion Graphic)
Web Application Security Basics and Intro
Injection attacks and how to avoid them
Secure Session Management
Authentication and Authorisation
Secure Transactions & Secure Deployments
Data security

Compliance Series (Animated)
PCI DSS for Merchants
PCI DSS for Corporate Office
PCI DSS for Retail Stores
SupaPOPI (RSA)
Consumer Protection Act (RSA)
Treating Customer Fairly (RSA)
Conflict of interest policy
Business Continuity / Business Resilience

Popcorn Training Content

Also included in Training Access Level III (Diamond)

Popcorn Training Posters

Cyber Heroes Series
Cloudy with a Chance of Phish
Dicey Devicey
Don't Take the Bait
Freaky Leaky
Internet Threats
Mobile Mayhem
Pass the Password
Social Media Fever

Security Moments Series
Hacking Emotions
Privileged User Access Management
Ransomware
Social Engineering 101
Spot the Bad Attachment
Spot the Bad Link
The Big Phish

Something Phishy Series
Breaking the Barrier
Cloudy With A Chance of Phish
Dicey Devicey
Freaky Leaky
Mobile Mayhem
Pass The Password
Phishious Malicious
Social Media Fever
Something Phishy

Securable.io Videos

Also included in Training Access Level III (Diamond)

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 (Diamond)

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

ThinkHR Training Modules

Also included in Training Access Level III (Diamond)

A Manager's Guide to Diversity, Inclusion and Accommodation
Active Shooter
Bullying and Hazing on Campus
Bullying and Violence in the Workplace
Campus Security Obligations Under Federal Law
FERPA for Higher Education
Optimizing Your Work/Life Balance: Maintaining Your Life Balance
Optimizing Your Work/Life Balance: Taking Control of Your Stress
Pandemic Flu Awareness
Preventing Harassment in the Global Workplace - Employee Edition
Preventing Harassment in the Global Workplace - Manager Edition
Promoting a Substance-Free Workplace
Rightful Employment Termination
Sexual Harassment Prevention for Employees
Title IX for Higher Education
Wage and Hour Awareness for Managers
Workplace Harassment Prevention for Employees - Version 2.0 (Title VII)

exploqii Videos

Also included in Training Access Level III (Diamond)

Anti-Trust 1 - Basic Regulations & Risks
Basic Rules of Secure Communication
Bluetooth & WiFi
Business Partner Compliance
CEO Fraud - Fake president
Clean Desk Policy
Cloud Services
Code of Conduct
Compliance Checklist
Compliance Management System
Conflict of Interest
Corruption
Crisis Management
Data Protection
EU GDPR
Export Control
Gifts & Hospitality
Identity Theft
Industrial Espionage
Information Classification
Information Security @ Mobile Devices
Information Security @ Remote Workplaces
Information Security @ Social Media
Insider Threat
Internal Investigations
IT Security in the Workplace
Know-how Security
Money Laundering
Payment Fraud
Phishing Attacks on companies
Phone Scam
Price Rigging
Proxy Servers & Data Privacy
Ransomware Micro-module
Secure Passwords
Security-orientated Personnel Selection
Sexual Harassment
Social Engineering Micro-module
Social Media Guidelines
Threat Management
Travel Security
USB Attacks
Visitor Management
Whistleblower

Security Awareness Training Content By Subscription Level

World's largest library of security awareness training content is now just a click away!

You now really have 500+ new ways to make sure your users Think Before They Click!

KnowBe4's strategic partnerships with The Security Awareness Company, Securable.io, AwareGO, Popcorn Training, ThinkHR and exploqii allows you to significantly better manage the ongoing problem of social engineering.

In your fight against phishing and ransomware you can deploy the best-in-class phishing platform combined with the world's largest library of security awareness training content; including 500+ interactive modules, videos, games, posters and newsletters.

TRAINING CONTENT	LEVEL I	LEVEL II	MOST POPULAR LEVEL III
Training Modules	3	16	42
Videos (3-5 min)	1	1	118
Micro Modules		23	87
Compliance Modules		6	39
Games			18
Posters / Images			180
Newsletters / Security One Sheets & Digests			121

FEATURES	SILVER	GOLD	PLATINUM	MOST POPULAR DIAMOND
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
Security Roles			✓	✓
Social Engineering Indicators			✓	✓
USB Drive Test			✓	✓
Priority Level Support			✓	✓
Training Access Level III				✓
AIDA™ Artificial Intelligence-driven Agent BETA				✓

We offer three Training Access levels depending on your subscription. Training Access Levels: I (Silver), II (Gold & Platinum), and III (Diamond). We are constantly adding new training content.

Contact your account representative to get access to our Module Store to see the latest content for yourself!

For the most complete list of content training content, please visit our website at www.knowbe4.com/knowbe4-training-modules-overview/

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