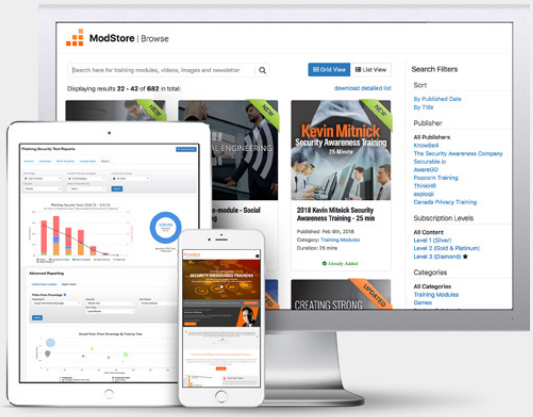
Overview of KnowBe4 Training Library

KnowBe4
Human error. Conquered.



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

- KnowBe4
- The Security Awareness Company
- Securable.io
- Popcorn Training
- ThinkHR
- Exploqii
- Canada Privacy Training
- Twist & Shout
- Teach Privacy
- Syntrio

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 850+ 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.

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 Cybersecurity Awareness Posters

Also included in Training Access Level I (Silver)

2019 Common Threats
2019 Social Engineering Red Flags
Captain Awareness
Captain Awareness: Conquering Internet Safety for Kids
Captain Awareness: Securing Your Mobile Devices
Risks of Social Media Sharing
All Your Data Are Belong To Us
Bad Rabbit: Think Before You Click
Be An Email Superhero
Burning Man
CEO Fraud
Don't Let Your Strings Get Pulled
Don't Click on Me
Email Subject Line Red Flags
Give Us the Bitcoin
It only takes one
Jaws: Don't Be a Victim
Keep Calm and Don't Click
Loose Clicks Sink Ships
Loose Lips Sink Ships
Loose Tweets Sink Fleets
Phishin' Is Easy
2019 Your Role: Internet Security and You
Captain Awareness: Triumph over the Reuse of Passwords
Ransomware Apocalypse is Calling
Ransomware Has No Borders
Ransomware Invaders
Resist the USB Attack
Stop Phishing Attacks Dead in Their Tracks
Stop, Look, Think
Stop, Look, Think Signs
The Clickers
There's Something Phishy in Your Inbox
Think Before You Click
Think Before You Click Boy
Think Before You Click Brain
Think Before You Click Eye Chart
Think Before You Click Monster
Think Before You Click Pop-Up
This is My Ransomware Killing Poster
Tron Ransomware
Uncle Sam: I Want You to Stop Clicking
Why Security Awareness Training?
You Can't Go Back

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 smartphones. It teaches employees to handle credit card information securely to prevent data breaches. A quiz ends off this module.

Risks of Social Media Sharing

This course alerts users to the security problems that can arise from common social media usage – even when posting information that is personal.

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."

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.

KnowBe4 Training Modules

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

Common Threats, Part 1 - Miranda's Story
In this module you'll learn about strategies and techniques hackers use to trick people. 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 - Kyle's Story
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.

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.

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.

Criminal Justice Information Services Security Series
These four courses, Level 1 through Level 4 are designed to satisfy the FBI/CJIS requirements for training employees based on their access to protecting criminal justice information.

Privileged User Security Series
These four courses cover important aspects of privileged access, secure database administration, secure Windows administration, and secure Linux administration.

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 with best practices for protecting customers' personal information, and the employee's role in ensuring protection of NPPI.

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 Unclassified Information (CUI), including your organization's proprietary information.

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.

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 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)
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

Captain Awareness Video Series

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
Conquer Open WiFi
Foil Phishing

KnowBe4 Video Modules

Kevin Mitnick - Two-Factor Authentication Attack
KnowBe4 Pretexting - Fake IT "Password Break-In"
KnowBe4 Pretexting - Tech Support "Social Engineering"
KnowBe4 Pretexting - Two-Factor Authentication Attack
KnowBe4 Pretexting - A Fake IT Attack
SIM Swapping - Call Center
SIM Swapping - Mobile End Users
SIM Swapping - Mobile Retail Locations

Security Awareness Company Content Library

Also included in Training Access Level III (Diamond)

Cyber Security Awareness Interactive Training Modules

Call Center & Help Desk Awareness
Computer Security & Data Protection
Data Classification
Developing an Incident Response Plan
Empowering Your Employees for Better Security
Executive Awareness Leadership
How to be a Human Firewall
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 Security
Phishing Andrew's Inbox
Phishing Fundamentals
Privacy Basics
Ransomware
Restricted Privileged Access
Secure Online Behavior
Social Engineering & Phishing for Executives
Social Engineering Basics
Security Awareness Fundamentals
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

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 Newsletters and Security Docs

10+ Cyber Security Awareness Games

150+ Cyber Security Awareness Posters & Artwork

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
Is Free Wifi Really Free
Jasper the Disaster in Travel Security Awareness
Jasper the Disaster in Workplace Physical Security
Jasper the Disaster in Workplace Policy
Low-Tech Hacks to Steal Your ID
Mouse Overs
NIST Password Guidelines
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
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 Series Introduction
Breaking the Barrier
Cloudy With A Chance of Phish
Dicey Devicey
Freaky Leaky
Mobile Mayhem
Pass The Password
Phishious Malicious
Social Media Fever

Cyber Heroes Series Videos & Quiz (Live Action)
Cyber Heroes Introduction
Breaking the Barrier
CEO Scams
Cloudy with a Chance of Phish
Dicey Devicey
Don't Take the Bait
Freaky Leaky
Internet Threats
Mobile Mayhem
Pass the Password
Passwords
Social Media Fever

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

Standups 4 Security Series: (Live Action)
Cybercrime Promo
A Goliath Hack
Behind the Scam with Loyiso Madinga
Open Secrets - A Password Exhibition
Spearphishing - Catching the Big Phish
Don't Trust Anybody - CEO Scam
Social Media Oversharing
The Dark Web Pop-up

Security Moment Short Clip Videos & Quiz (Motion Graphic)
Hacking Emotions
Privileged User Access Management
Ransomware
Social Engineering 101
Spot the Bad Attachment
Spot the Bad Link
The Big Phish

Building Secure Software Series
Ep 1 - Very Early and Often
Ep 2 - Leverage Security Frameworks and Libraries
Ep 3 - Secure Database Access

Secure Coding 6 Module Course for Developers Video & Quiz (Animated & Motion Graphic)
Secure Transactions and Secure Deployments
Authentication and Authorization
Data Security
Injection Attacks and How to Avoid Them
Introduction to Web Application Security
Secure Session Management

Compliance Series (Animated)
Acceptable Use Policy
Business Continuity Management
Conflict of Interest Policy
Consumer Protection Act (RSA)
PCI DSS for Corporate Office
PCI DSS for Merchants
PCI DSS for Retail Stores
SupaPopi (RSA)
Treating Customers Fairly (RSA)

Cyber Essentials Series
Information Security 101
Cryptocoin Security
Cyberbullying

85 Popcorn Training Reinforcement Posters and Security Docs

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

ThinkHR Training Modules

Also included in Training Access Level III (Diamond)

A Manager's Guide to Discipline and Documentation
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
EEO and Lawful Hiring
FERPA for Higher Education
FMLA Leave and More: An Overview of Legally Protected Leave
HIPAA - Privacy Essentials
HIPAA - Privacy Rules for Business Associates
HIPAA - Security Rules for Business Associates
HIPAA for Non-Medical Employees
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, State of New York
Workplace Harassment Prevention for Managers, State of New York
Workplace Harassment Prevention for Employees (Title VII)
Workplace Harassment Prevention for Managers - Multi-State Edition, V3.0
Workplace Management: Employment Laws and Regulations

exploqii Videos

Also included in Training Access Level III (Diamond)

Anti-Trust 1 - Basic Regulations & Risks
Anti-Trust 2 - Industry Events
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
Disinformation
EU GDPR
Export Control
Fairness & Respect in the Workplace
Gifts, Hospitality & Anti-Bribery
IT Security in the Workplace
Identity Theft
Industrial Espionage
Information Classification
Information Security @ Mobile Devices
Information Security @ Remote Workplaces
Information Security @ Social Media
Insider Threat
Internal Investigations
Know-How Security
Microphone, Camera & Selfies
Money Laundering
Payment Fraud
Phishing Attacks on Companies
Phone Scam
Price Rigging
Proxy Servers & Data Privacy
Ransomware Micro-module
Secure Passwords
Security-Oriented Personnel Selection
Sexual Harassment
Social Engineering Micro-module
Social Media Guidelines
Threat Management
Travel Security
USB Attacks
Visitor Management
Whistleblower

Teach Privacy Training Modules

Also included in Training Access Level III (Diamond)

California Health Privacy
Canadian Anti-Spam Legislation (CASL)
Data Breach
Data Disposal
Data Retention
Encryption
FERPA (K-12)
General Data Protection Regulation (GDPR)
Global Privacy and Data Protection
Secure Workspaces Game
The Privacy Act

Syntrio Training Modules

Also included in Training Access Level III (Diamond)

Avoiding Antitrust Violations
Avoiding Conflicts of Interest
Avoiding Insider Trading Risk
Back Injury Prevention
California Workplace Harassment Prevention for Employees
California Workplace Harassment Prevention for Managers
Connecticut Sexual Harassment for Managers
Controlling Workplace Exposure to Bloodborne Pathogens
Delaware Sexual Harassment for Employees
Delaware Sexual Harassment for Managers
Disability Discrimination and Accommodation
Employee Privacy: Balancing a Manager's Right to Know
ErgoNet: A Training Guide for Healthy Office Workers
Ethics and Code of Conduct
FCPA Anti-Corruption and Bribery
Global Anti-Corruption
Maine Sexual Harassment for Employees
Maine Sexual Harassment for Managers
New York Preventing Sexual Harassment for Employees
New York Preventing Sexual Harassment for Managers
Personal Protective Equipment: A General Awareness
Preventing Unlawful Retaliation in the Workplace
Slip, Trip, and Fall Prevention
Understanding the Family and Medical Leave Act
Valuing Diversity for Managers

Twist & Shout Video Modules

Also included in Training Access Level III (Diamond)

Restricted Intelligence Series *-Season 1*

Episode 1:The Test (passwords and passes)
Episode 2: Browsing (safe surfing)
Episode 3: A Cry for Help (email hacking and phishing)
Episode 4: The Journey (portable storage devices)
Episode 5: The Leak (beware what you share
Episode 6: The Lesson (mobile devices)

Restricted Intelligence Privacy Edition -*Season 2*

Episode 1: Nothing To Do With Me (What Is PI?)
Episode 2: Nobody Reads That Stuff (Privacy by Design)
Episode 3: Once More Unto the Breach (Retention & Disposal)
Episode 4: The Heart of the Matter (Purpose & Minimisation)
Episode 5: Mr. Cellophane (Transparency)
Episode 6: Partners (Third Party Partners)
Bonus - GDPR Intro (GDPR is Coming)

The Inside Man Series *-Season 1*
Episode 1: The New Guy (Social Engineering)
Episode 2: Social Hour (Social Media)
Episode 3: On Our Side (Phishing Attacks)
Episode 4: Surprise (Document Disposal)
Episode 5: Takeaways (Clear Desktop Policy)
Episode 6: Masquerade (Cloud Services)
Episode 7: Buying Time (Passwords)
Episode 8: Taken (Ransomware)
Episode 9: Where The Wild Things Are (Travel)
Episode 10: Keep Your Friends Close (App security and permissions)
Episode 11: The Sound Of Trumpets (External Devices)
Episode 12: Checkmate (Insider Threats)

40 Twist & Shout Reinforcement Posters and Promotional Graphics

Canada Privacy Training Modules

Also included in Training Access Level III (Diamond)

Canadian Private Sector Privacy

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 850+ new ways to make sure your users Think Before They Click!

KnowBe4's game-changing partnerships with The Security Awareness Company, Securable.io, Popcorn Training, ThinkHR, exploqii, Canada Privacy Training, Twist & Shout, Teach Privacy and Syntrio 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 850+ interactive modules, videos, games, posters and newsletters.

TRAINING CONTENT	LEVEL I	LEVEL II	MOST POPULAR LEVEL III
Training Modules	5	30	83
Micro Modules	2	23	67
Videos (90 sec-5 min)	1	27	187
Compliance Modules		15	80
Posters / Images	37	44	293
Newsletters / Security One Sheets		6	191
Games			15

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	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓	✓
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

April 2019