



# Buyer's Guide

## Security Awareness Training & Simulated Phishing Platform

## Buyer's Guide: Security Awareness Training & Simulated Phishing Platform

KnowBe4 is the world's largest integrated platform for security awareness training and simulated phishing. This guide explains everything that is included in the KnowBe4 platform.

### Problem

Your employees are the weak link in your IT Security. Social engineering is the number one security threat to any organization. The alarming growth in sophisticated cyberattacks makes this problem only worse, as cybercriminals go for the low-hanging fruit: employees. Numerous reports and white papers show organizations are exposed to massive increases in the number of cyberattacks over the past five years.

### Overview

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform with over tens of thousands of customers. Based on Kevin Mitnick's 30+ year unique first-hand hacking experience, you now have a platform to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks. KnowBe4 provides you with the world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters.

With world-class, user-friendly new-school Security Awareness Training, KnowBe4 gives you self-service enrollment, and both pre-and post-training phishing security tests that show you the percentage of end-users that are Phish-prone. KnowBe4's highly effective, frequent, random Phishing Security Tests provide several remedial options in case an employee falls for a simulated phishing attack.

Our platform allows you to create a fully mature security awareness program.

"People are used to having a technology solution [but] social engineering bypasses all technologies, including firewalls. Technology is critical, but we have to look at people and processes. Social engineering is a form of hacking that uses influence tactics."

– Kevin Mitnick



You also have the option to complement these phishing emails with monthly “hints and tips” to increase end user security awareness related to a variety of social engineering tactics. Executives get the insight they need to maximize training ROI and track security compliance.

The platform is created "by admins for admins", designed with an intuitive navigation and easy UI that takes minimal time to deploy and manage. The infrastructure is highly scalable and can handle 100,000+ end users with ease. For organizations with their own LMS, training can be delivered in industry standard formats such as SCORM and AICC. Our system also includes support for single sign-on so that users do not have to log in multiple times, using Security Assertion Markup Language (SAML).

### Prerequisites

No prerequisites are required other than normal end user level knowledge of email and operating an internet browser. End users need a PC with sound, however, the core training modules are fully subtitled to suit all environments in compliance with the Americans with Disabilities Act.

### Who Should Attend

All employees in your organization who use a computer, email and internet, from the mail room to the board room.

### Training Access Levels

We offer three Training Access Levels: I, II, and III depending on your subscription level. Because our library is constantly being updated, 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!

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.

## Training Modules

*The KnowBe4 content library is constantly being updated with fresh new content. Content listed below are examples from the KnowBe4 ModStore by subscription level. For the most complete list of current training content, please sign up to access the KnowBe4 Modstore here: <https://www.knowbe4.com/training-preview>*



### Kevin Mitnick Security Awareness Training *Included in Training Access Level I (Silver)*

#### Kevin Mitnick Security Awareness Training (45-min)

This fully interactive course takes you through three modules: Social Engineering Red Flags, Common Threats and Your Role\*. Recognizing the tricks and techniques hackers are using against you and your organization is critical to staying safe. Join Sparr0w (a hacker) and Kevin Mitnick (Chief Hacking Officer at KnowBe4) as they share their insider knowledge and take you behind the scenes to show you how the bad guys do what they do. Along the way, you'll become familiar with the signs of danger you should look for and the steps you can take to avoid becoming a victim of cybercrime. Additionally, you will practice your security awareness skills through a number of engaging scenarios. \*Abridged for inclusion in the 45-minute course.

#### Kevin Mitnick Security Awareness Training (15-min)

This module is a condensed version of the full 45-minute training, often assigned to management. Recognizing the tricks and techniques hackers are using against you and your organization is critical to staying safe. Join Sparr0w (a hacker) and Kevin Mitnick (Chief Hacking Officer at KnowBe4) as they share their insider knowledge and take you behind the scenes to show you how the bad guys do what they do. Along the way, you'll become familiar with the signs of danger you should look for and the steps you can take to avoid becoming a victim of cybercrime.



# 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**

Welcome to the Danger Zone! Keep your organization safe by successfully answering questions and preventing a hacker from reaching an unlocked workstation. This gamified assessment is designed as a post-training activity, meant to be taken after completing the 2020 Your Role, 2020 Social Engineering Red Flags, and 2020 Common Threats modules.

## **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



# El Pescador Training Modules

*Also included in Training Access Level III (Diamond)*

Data Collection  
 Data Collection Quiz  
 C-Level Phishing  
 Finance Sector Phishing  
 Lei Geral de Proteção de Dados

Phishing: Why Should We Care  
 Phishing, The Major Cause of Information Leakage  
 Relationship Trust  
 The Threat May Be Closer Than You Think





# 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  
Cryptocurrency Security  
Cyberbullying

## 85 Popcorn Training Reinforcement Posters and Security Docs



## 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)

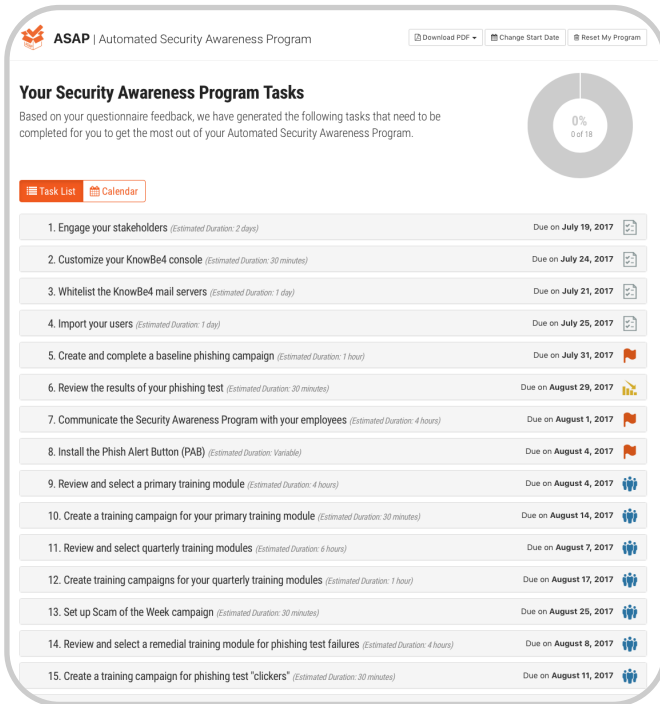
Canadian Private Sector Privacy

# Automated Security Awareness Program (ASAP)

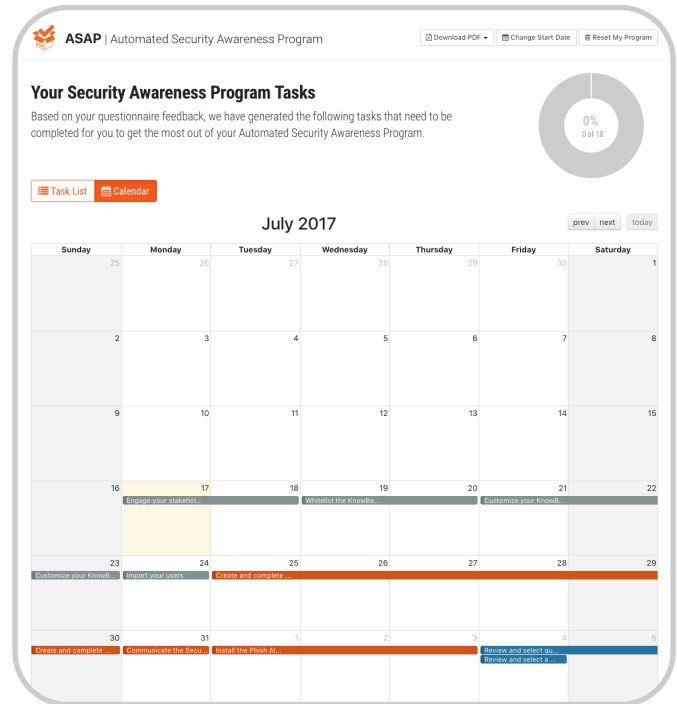
Many IT pros don't exactly know where to start when it comes to creating a security awareness program that will work for their organization.

**We've taken away all the guesswork with our Automated Security Awareness Program builder (ASAP).** ASAP is a revolutionary new tool for IT professionals, which builds a customized Security Awareness Program for your organization that will show you the steps needed to create a fully mature training program in just a few minutes!

The process of creating the program is simple enough, answer between 15-25 questions about your goals and organization, and a program will be scheduled for you automatically. The program tasks will be based on best-practices on how to achieve your security awareness goals.



Task	Estimated Duration	Due Date
1. Engage your stakeholders	2 days	July 19, 2017
2. Customize your KnowBe4 console	30 minutes	July 24, 2017
3. Whitelist the KnowBe4 mail servers	1 day	July 25, 2017
4. Import your users	1 day	July 25, 2017
5. Create and complete a baseline phishing campaign	1 hour	July 31, 2017
6. Review the results of your phishing test	30 minutes	August 29, 2017
7. Communicate the Security Awareness Program with your employees	4 hours	August 1, 2017
8. Install the Phish Alert Button (PAB)	Variable	August 4, 2017
9. Review and select a primary training module	4 hours	August 4, 2017
10. Create a training campaign for your primary training module	30 minutes	August 14, 2017
11. Review and select quarterly training modules	6 hours	August 7, 2017
12. Create training campaigns for your quarterly training modules	1 hour	August 17, 2017
13. Set up Scam of the Week campaign	30 minutes	August 25, 2017
14. Review and select a remedial training module for phishing test failures	4 hours	August 8, 2017
15. Create a training campaign for phishing test "clickers"	30 minutes	August 11, 2017



Day	Tasks
16	Engage your stakeholders
17	Engage your stakeholders
18	Whitelist the KnowBe4 mail servers
19	Whitelist the KnowBe4 mail servers
20	Whitelist the KnowBe4 mail servers
21	Whitelist the KnowBe4 mail servers
22	Whitelist the KnowBe4 mail servers
23	Whitelist the KnowBe4 mail servers
24	Whitelist the KnowBe4 mail servers
25	Whitelist the KnowBe4 mail servers
26	Whitelist the KnowBe4 mail servers
27	Whitelist the KnowBe4 mail servers
28	Whitelist the KnowBe4 mail servers
29	Whitelist the KnowBe4 mail servers
30	Whitelist the KnowBe4 mail servers
31	Whitelist the KnowBe4 mail servers

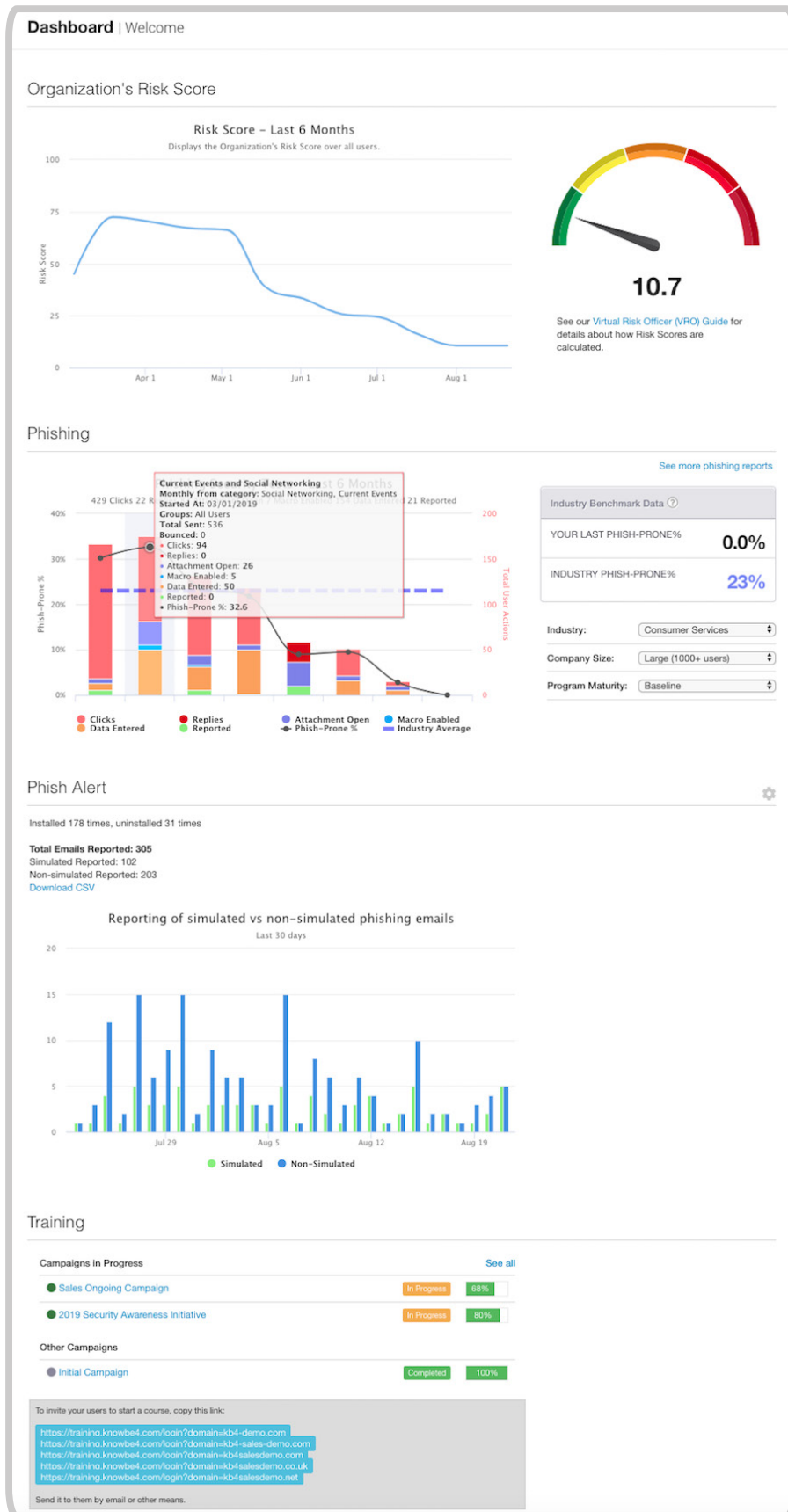
The program is complete with actionable tasks, helpful tips, courseware suggestions and a management calendar. Your custom program can then be fully managed from within the KnowBe4 console. You also have the ability to export the full program as a detailed or executive summary version in PDF format, use it for compliance requirements, and reporting to management.

You have an easy calendar view to plan and deploy your security awareness program.

## Dashboard

Our Phishing and Training Dashboard allows you to see how your end users are doing at-a-glance and in comparison to your peers across industries with **Industry Benchmarking**.

### Sample Phishing and Training At-a-glance



# Simulated Phishing

## Phishing Platform

You have the ability to schedule and send an unlimited number of Simulated Phishing Security Tests (PSTs) to your users during the subscription period.

Our extensive library of templates allows you to use the platform for “turnkey phishing”. You can be up and running in less than 30 minutes. Our library of templates includes emails in the following categories: Banking, Social Media, IT, Government, Online Services, Current Events, Healthcare, and many more. There is a community section where you can swap templates with thousands of other KnowBe4 customers.

## Samples of System Phishing Templates

### Email Preview

**From:** CEO@kb4-demo.com  
**Reply-to:** [Send me a test email](#)  
**Subject:** Urgent Request

I need the list of W-2s of employees wage and tax statements for 2015, I need them in PDF file type but I need it [uploaded here](#) for security purposes. Kindly prepare the lists and upload them for me asap.

[Close](#)

### Email Preview - Generic Debit/Credit Card Blocked (Link)


**From:** Security Team <cardsecurity@fraudinvestigation.gov>  
**Reply-to:** Security Team <cardsecurity@fraudinvestigation.gov>  
**Subject:** Urgent Alert  
[Send me a test email](#)  
[Toggle Red Flags](#)  
SuspiciousATMWithdrawal.pdf

We have detected a suspicious money ATM withdrawal from your card.

For your security, we have temporarily blocked the card. All the details are in the attachment. Please open it when possible.

Sincerely,

Card Security and Services



### Email Preview - Account Recovery (Link)

**From:** AccountRecovery@noreply.accountreset.com  
**Reply-to:** [Send me a test email](#)  
**Subject:** Please Initiate a Password Reset - Suspected Hacking Attempt

This email is to notify you that your google account has been disabled because we suspect a hacker has compromised it.

In order to unlock your account, you must initiate a password reset.

To initiate the password reset process to re-activate your Google Account, click the link below:

<https://www.googleaccount.com/recovery/srp?test=o2#3e9wxe0>

Sincerely,  
Goog1eApps Security

Note: This email address cannot accept replies.

### Email Preview - Generic Online Order Receipt (Link)

**From:** Ordering <Orders@OnlinePurchases.net>  
**Reply-to:** Ordering <Orders@OnlinePurchases.net>  
**Subject:** Your Online Order Receipt  
[Send me a test email](#)  
[Toggle Red Flags](#)

**Thanks for your order**

**Want to manage your order online?**  
If you need to check the status of your order or make changes, please visit our home page.

**Order Summary:**

<b>Shipping Details : (order will arrive in 1 shipment)</b>	
<b>Order #:</b>	842JSO-HPP830D-FFFF011
<b>Shipping Method:</b>	Overnight Shipping
<b>Shipping Preference:</b>	Fastest Delivery Time
Subtotal of Items:	\$269.81
Shipping & Handling:	\$43.56
	*****
<b>Total for this Order:</b>	<b>\$313.37</b>

**Delivery estimate:** Tomorrow  
**3"D-Link DIR-655 Extreme N Gigabit Wireless Router"**  
Misc.; \$89.94

Sold by: D-Link Electronics

**Didn't place this order?**  
Click on the Order Number to view details about this order

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks again for shopping with us.

**From:** IT@kb4-demo.com  
**Reply-to:** [Send me a test email](#)  
**Subject:** Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.


Please click here to do that:

[Change Password](#)

Please do this right away. Thanks!

Sincerely,  
 IT

**From:** Tracking@pak-express.com  
**Reply-to:** [Send me a test email](#)  
**Subject:** A Delivery Attempt Was Made



\*\*\*Do not reply to this e-mail. PAK will not receive your reply.

**Important Delivery Information**

<b>Delivery Status:</b>	Could not deliver package due to invalid information.
<b>Fix Errors:</b>	<a href="#">HERE</a>
Please click the above link to correct the errors and we will attempt to re-deliver your package	
<b>Driver Release Location:</b>	COULD NOT DELIVER

**Shipment Detail**

<b>Number of Packages1</b>	
<b>PAK Service:</b>	1 DAY OVERNIGHT - URGENT
<b>Weight:</b>	2.8 LBS

**From:** AccountRecovery@noreply.accountreset.com  
**Reply-to:** [Send me a test email](#)  
**Subject:** Please Initiate a Password Reset - Suspected Hacking Attempt

This email is to notify you that your google account has been disabled because we suspect a hacker has compromised it.

In order to unlock your account, you must initiate a password reset.

To initiate the password reset process to re-activate your Google Account, click the link below:

<https://www.googleaccount.com/recovery/srp?test=02h3e9wx0>

Sincerely,  
 GoogleApps Security

Note: This email address cannot accept replies.

## Phishing Template Customization

You also have the ability to customize any system template as well as include simulated attachments and macros.

### Sample of Creating Custom Phishing Templates

## Sample Landing Pages

**KnowBe4**  
Human error. Conquered.

### Oops! You clicked on a simulated phishing test.

Remember these three 'Rules To Stay Safe Online'

- ✓ **RULE NUMBER ONE:**
  - Stop, Look, Think!
  - Use that delete key
- ✓ **RULE NUMBER TWO:**
  - Do I spot a Red Flag?
  - Verify suspicious email with the sender via a different medium
- ✓ **RULE NUMBER THREE:**
  - "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: Stay alert as YOU are the last line of defense!



**PLEASE NOTE:**  
This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

**KnowBe4**  
Human error. Conquered.

### Oops! You clicked on a phishing email!

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

To: admin@kb4-demo.com  
From: IT <IT@kb4-demo.com>  
Reply-to: IT <IT@kb4-demo.com>  
Subject: **Change of Password Required Immediately**

We suspect a security breach happened earlier this week. **In order to prevent further damage, we need everyone to change their password immediately.**

**Please click here to do that**

**Change Password**

Please do this right away. Thank!

Sincerely,  
IT

**Please Note:**  
This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

## Scheduling Phishing Security Test

Scheduling a Phishing Security Test is incredibly easy; everything is designed to mimic real-world phishing attacks.

## Sample Phishing Campaign Creation

### Create New Phishing Campaign

[← Back to Campaigns](#)

**Note:** A campaign will start 10 minutes after it is activated or created.

Name:

Deliver To:

Frequency:  One time  Weekly  Bi-Weekly  Monthly  Quarterly

Start Time:   (GMT-05:00) Eastern Time (US & Canada)

Sending:  Send all emails when the campaign starts

Send emails over

**Define Business Days & Hours**

to  (GMT-05:00)

Sun  Mon  Tues  Wed  Thur  Fri  Sat

Track Activity:  days after sending is complete

Track replies to phishing emails

Categories:   [Preview](#)

Difficulty Rating:

Phish Link Domain:

Landing Page:

Add Exploit:

Add Clickers To:

Send an email report to account admins after each Phishing Security Test

[Create Campaign](#)

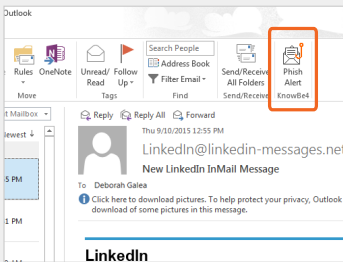


## Phish Alert Button Employees Report Phishing Attacks With One Click

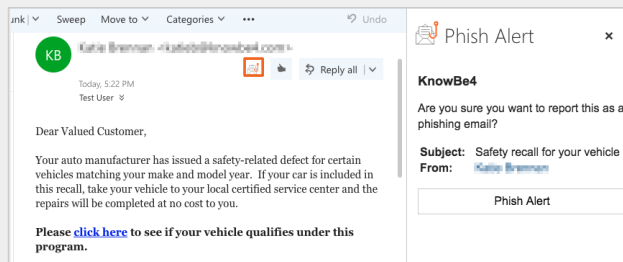
KnowBe4's Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis and deletes the email from the user's inbox to prevent future exposure. All with just one click!

- When the user clicks the Phish Alert button on a simulated Phishing Security Test, this user's correct action is reported.
- When the user clicks the Phish Alert button on a non-simulated phishing email, the email will be directly forwarded to your Incident Response team.
- Has fully customizable button text and user dialog boxes.
- Clients supported: Outlook 2010, 2013, 2016 & Outlook for Office 365, Exchange 2013 & 2016, Outlook on the web (Outlook.com), the Outlook Mobile App (iOS and Android), Chrome 54 and later (Linux, OS X, and Windows)

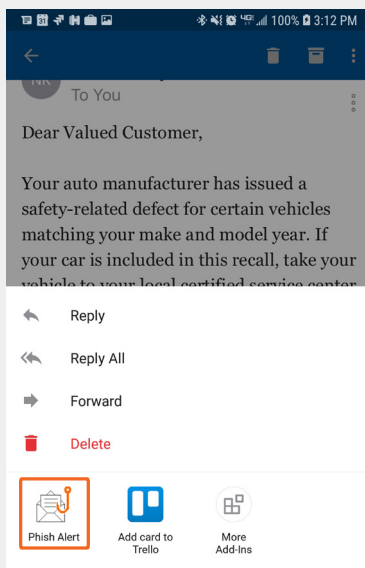
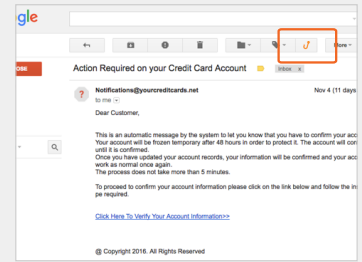
### Outlook Toolbar Adds a Phish Alert button for your users



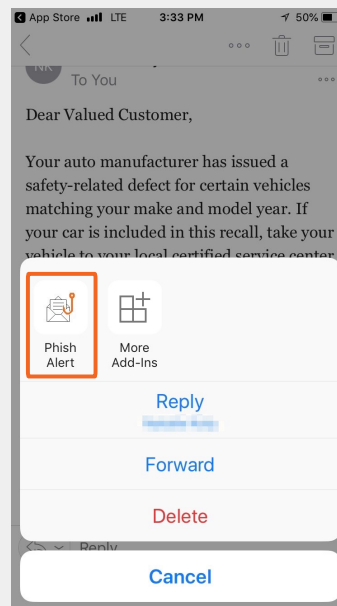
### Office 365 Add-in Pane Adds a Phish Alert button for your users



### Gmail Extension Adds a Phish Alert button for your users



Outlook Mobile  
(Android)

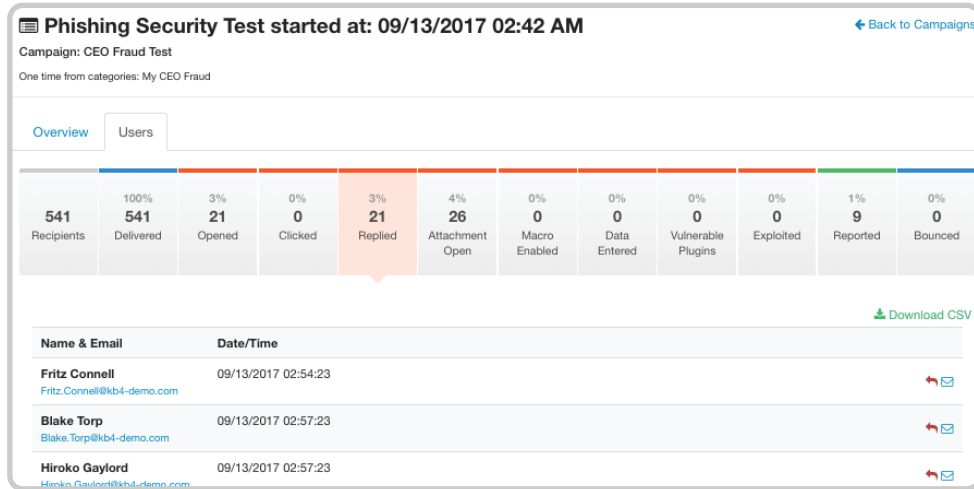


Outlook Mobile  
(iOS)

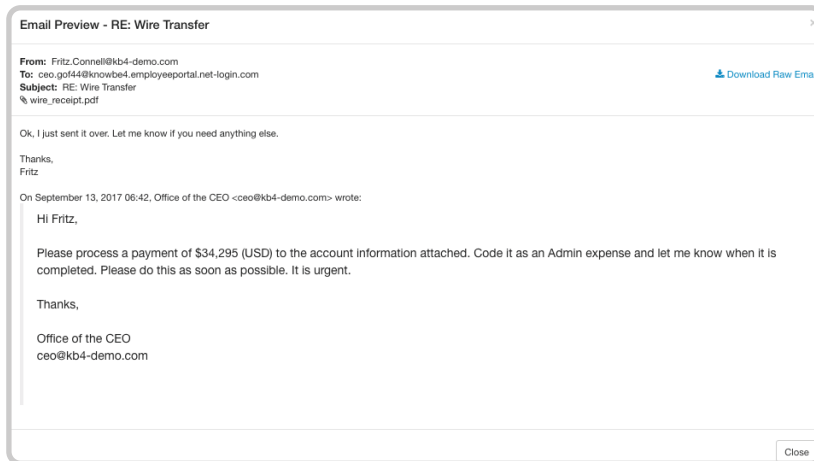
# Advanced Phishing Features

## Phishing Reply Tracking

KnowBe4's Phishing Reply Tracking allows you to track if a user replies to a simulated phishing email and can also capture the information in the reply for review within the KnowBe4 administrative console.



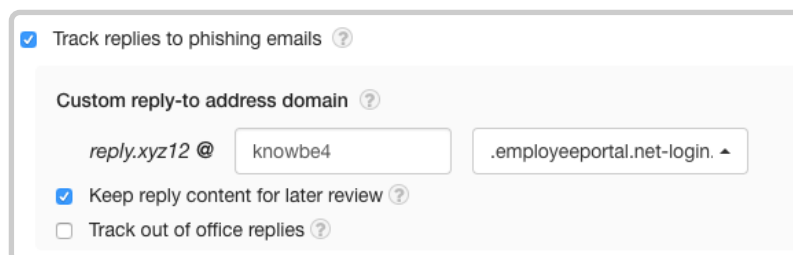
We have created a new category of system phishing templates called “Reply-To Online” which are specifically designed to test whether users will interact with “the bad guys” on the other end. However, the Phishing Reply Tracking also works with any of our 2000+ phishing templates.



Phishing Reply Tracking is simple to use, it's on by default for new phishing campaigns via the “Track replies to phishing emails” option.

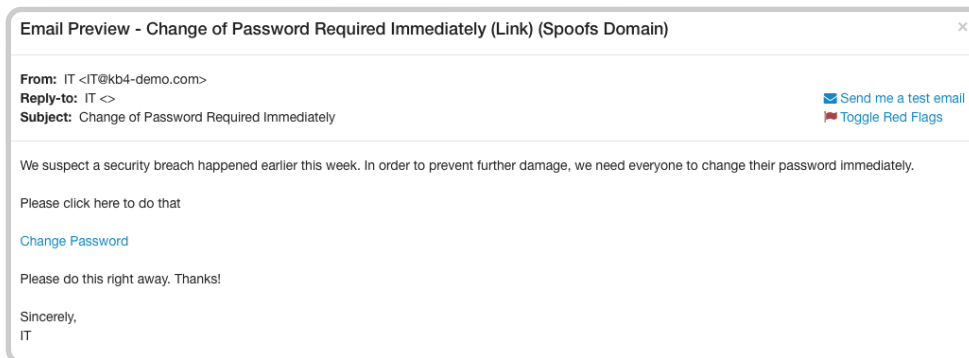
Additional options for this feature include:

- Store the reply-to content, this is on by default, but may be disabled.
- Customizable reply-to address sub-domain, making the reply-to address look similar to your actual domain.
- Track out of office replies to find out if your users are including company directories and other information with their OOO messages.

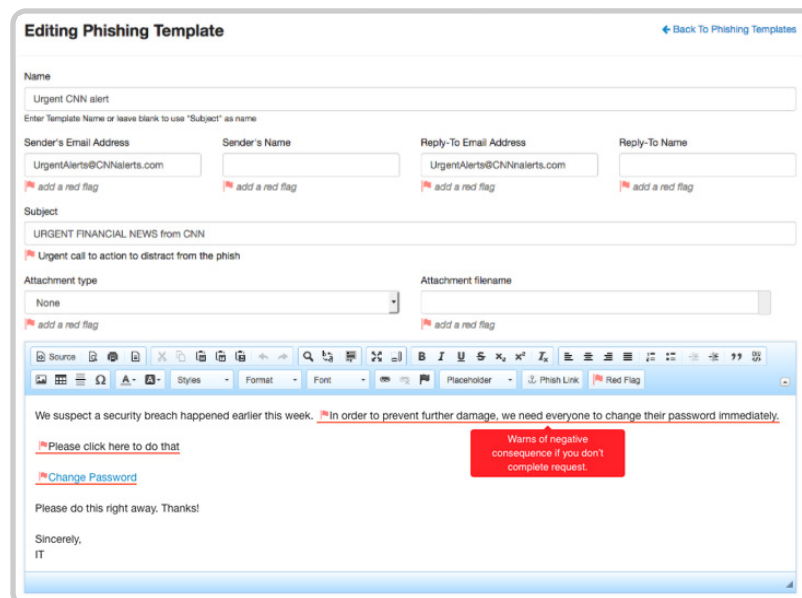


## Social Engineering Indicators (SEI)

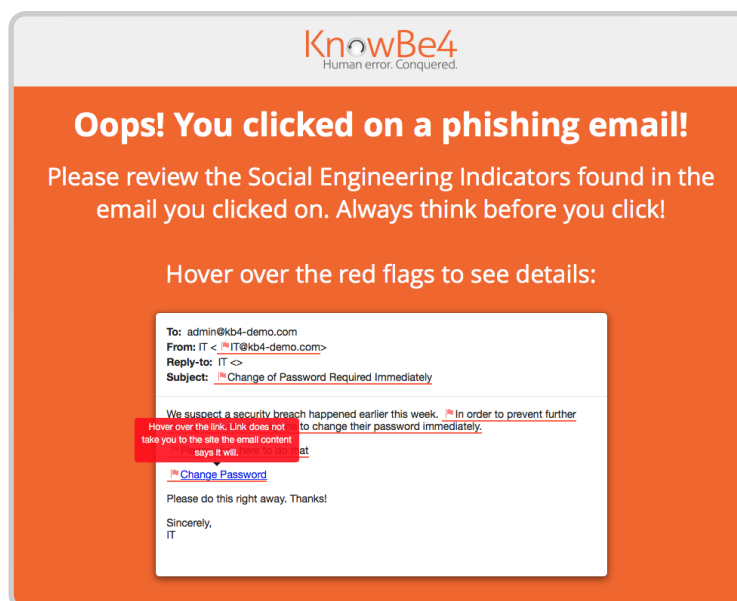
Patented technology that turns every simulated phishing email into a tool IT can use to instantly train employees. When a user clicks on any of the 2000+ KnowBe4 simulated phishing emails, they are routed to a landing page that includes a dynamic copy of that phishing email showing all the red flags.



You can also customize any simulated phishing email and create your own red flags.



Users can then immediately see the potential pitfalls and learn to spot the indicators they missed in the future.



## USB Drive Test™

Allows you to test your user's reactions to unknown USBs, on average 45% of users will plug in USBs they find!

You can easily create your USB Drive Test from the KnowBe4 admin console and download special "beaconized" Microsoft Office files. You can also rename these files to entice employees to open them. Then place the files onto any USB drive, which you can then drop at an on-site high traffic area.

If an employee picks up the USB drive, plugs it in their workstation, and opens the file, it will "call home" and report the fail as well as information such as access time and IP address. Should a user also enable the macros in the file, then additional data such as username and computer name is also tracked and made available in the admin console.

## GEO-location

See where your simulated phishing attack failures are on a map, with drilldown capability and CSV-export options.



## AIDA: Artificial Intelligence Driven Agent (Beta)

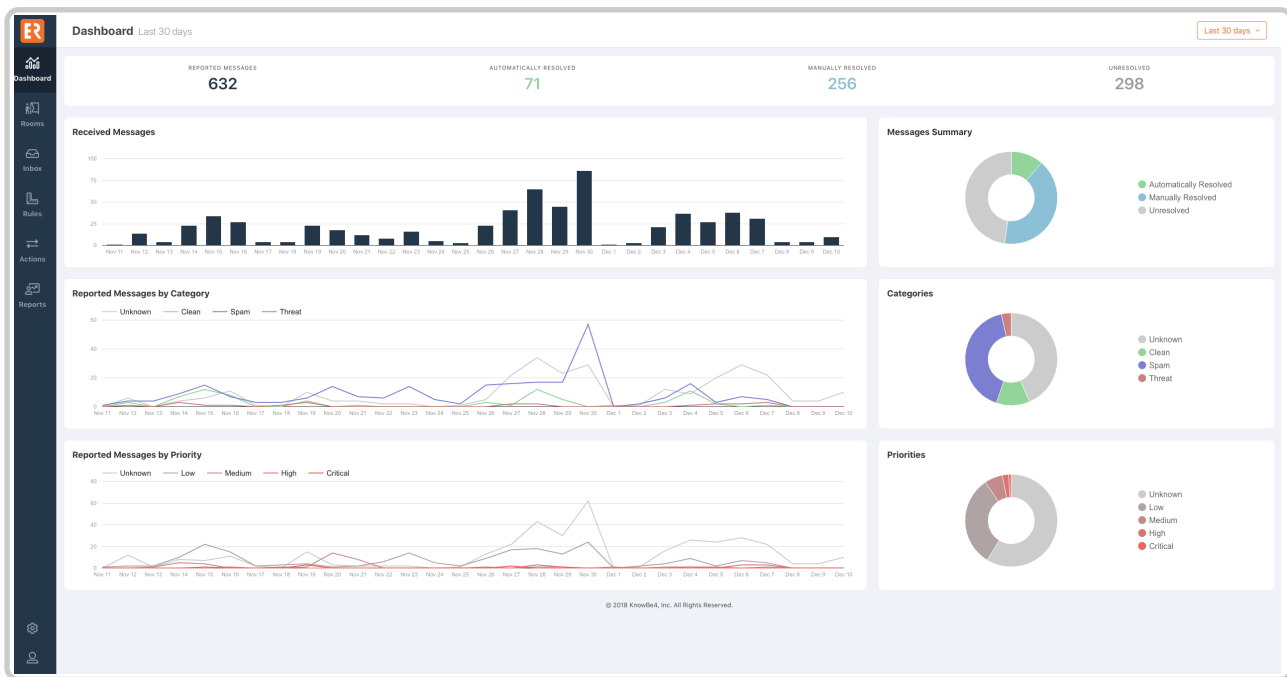
AIDA uses artificial intelligence to dynamically create integrated campaigns that send emails, text and voicemail to an employee, simulating a multi-vector social engineering attack. It attempts to have the employee either click on a phishing link, tap on a link in a text message, or respond to a voice mail – any of which could compromise your network. In short, AIDA uses Artificial Intelligence to inoculate your employees against social engineering and allows you to simulate a multi-faceted social engineering attack using email, phone, and SMS messaging. (Available for U.S. and Canada)

## PhishER: Identify and respond to email threats faster

Whether or not you step employees through security awareness training doesn't change the fact that your users are likely already reporting potentially dangerous emails in some fashion within your organization. The increase of this email traffic ... can present a new problem! How do you best manage your user-reported messages?

With the firehose of spam and malicious email that attack your network, some 10-15% of these make it past your filters. With only approximately 1 in 10 user-reported emails being verified as actually malicious, how do you not only handle the real phishing attacks and email threats —and just as importantly— effectively manage the other 90% of user-reported messages accurately and efficiently? PhishER.

PhishER is a critical element to help your IR teams work together to mitigate the phishing threat and is suited is for any organization that wants to automatically prioritize and manage potentially malicious messages—accurately and fast! PhishER is available as a stand-alone product or as an add-on option for KnowBe4 customers currently using the KnowBe4 Phish Alert button.



# Training Campaigns

## Training Campaigns

Allows you to fully automate the roll out of your training, including scheduled automated reminder emails for all of your end users.

### Initial campaign

Groups: All Users [← Back to Training Campaigns](#)

Overview **Users**

**2016 Basics of Credit Card Security**  
100% Completed

**2018 Kevin Mitnick Security Awareness Training - 45 Min**  
100% Completed

100%  
Completed  
All Courses

* This Training Campaign	
STATUS	Completed
START DATE	7/1/2017 02:42 AM
END DATE	7/31/2017 02:42 AM
USERS	537
AUTO-ENROLL	False
SCHEDULED NOTIFICATIONS	
<ul style="list-style-type: none"> <li>Send welcome notification to User on enrollment</li> <li>Remind User 5 days after enrollment</li> <li>Remind User 5 days before due date</li> <li>Remind User 2 days before due date</li> <li>Send completion notification to User</li> </ul>	

**User training activity**  
Number of users that started at least one course (per day)

### Sales Ongoing Campaign

for course 2016 Basics of Credit Card Security [← Back to Training Campaign Summary](#)

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.

Overview **Users**

28  
All Users

10%  
3  
Incomplete

3%  
1  
Not Started

7%  
2  
In Progress

89%  
25  
Complete

Notify Selected
Pass Selected
Reset Progress
Download CSV

<input type="checkbox"/>	Email address	Enrolled	Started	Completed	Time Spent	Time Left	Status
<input type="checkbox"/>	<a href="mailto:Aaron.Lesch@kb4salesdemo.net">Aaron.Lesch@kb4salesdemo.net</a>	12/21/2017 01:44	✓	✓	00:43:00	-	Passed
<input type="checkbox"/>	<a href="mailto:admin@kb4-demo.com">admin@kb4-demo.com</a>	12/21/2017 01:44	✓		00:04:41	-	In progress
<input type="checkbox"/>	<a href="mailto:Alita.Walker@kb4salesdemo.net">Alita.Walker@kb4salesdemo.net</a>	12/21/2017 01:44	✓	✓	00:34:00	-	Passed
<input type="checkbox"/>	<a href="mailto:Chara.Swaniawski@kb4salesdemo.net">Chara.Swaniawski@kb4salesdemo.net</a>	12/21/2017 01:44	✓	✓	00:46:00	-	Passed
<input type="checkbox"/>	<a href="mailto:Denna.Jaskolski@kb4salesdemo.net">Denna.Jaskolski@kb4salesdemo.net</a>	12/21/2017 01:44	✓	✓	00:56:00	-	Passed



## Engaging, interactive Browser-based Training

KnowBe4's new learner experience offers optional gamification, in the form of leaderboards and badges, so your users will be incentivized and motivated to take their assigned training.

### KB4-Tutorials Leaderboard

See how your group ranks below! Improve your group's rank on the leaderboard by completing all of your training assignments.

**Congrats!**  
Your group is 2nd

Rank	Name	Percentage Complete
1	HR	19%
2	IT	14%
3	Admins	13%

Rank	Name	Percentage Complete
1	HR	19%
2	IT	14%
3	Admins	13%

### Your Achievements

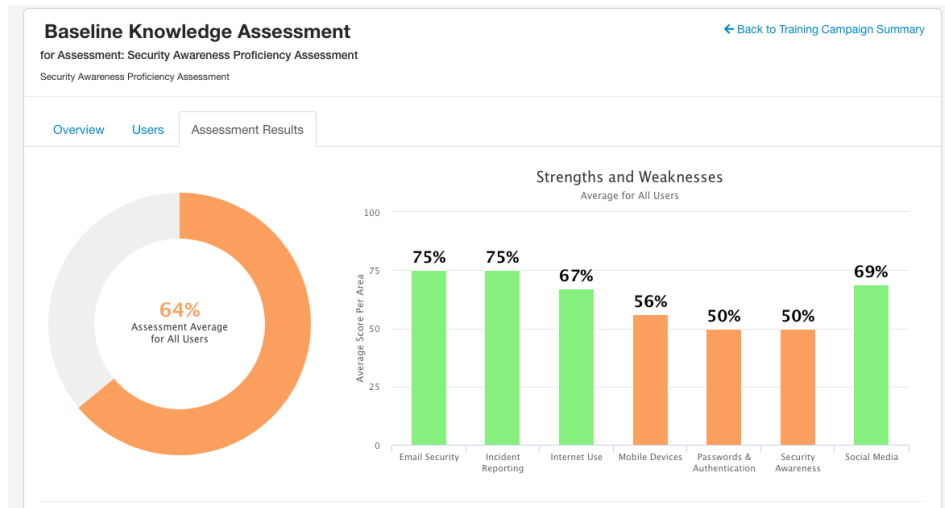
Good work, Cyber Hero! You've earned 4 badges! Check out your heroic achievements below and find out how you can collect more badges.

## Assessments

Find out where your users are regarding both security knowledge and security culture to help establish baseline security metrics you can improve over time. KnowBe4's new Assessments help you identify users that have a higher proficiency in security in not only knowing the right thing to do but also actually doing the right thing as part of the security culture you're trying to achieve in your organization.

### Security Awareness Proficiency Assessment (SAPA)

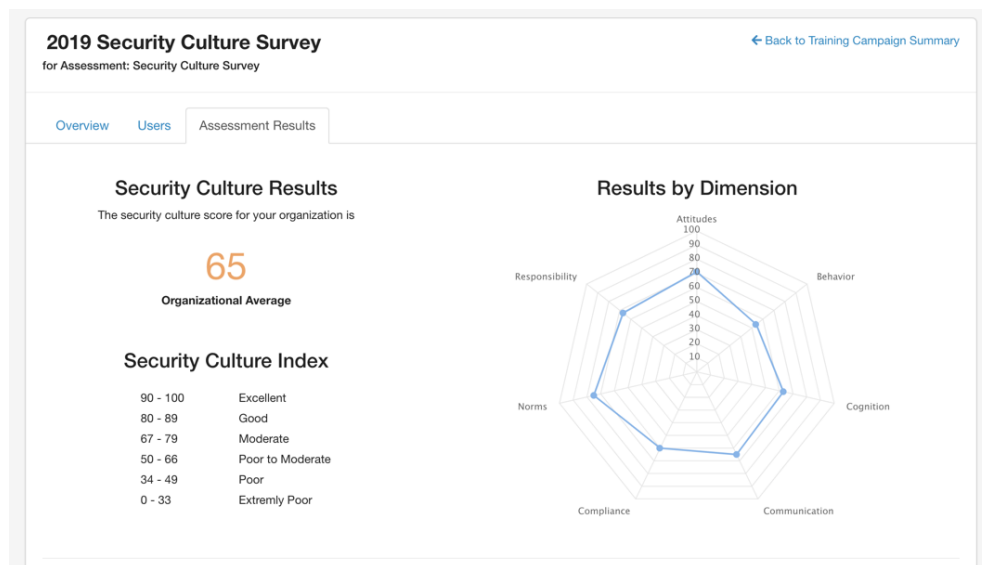
SAPA is a skills-based assessment designed to help your organization determine your security awareness training needs by identifying gaps in individual users' knowledge as well as recommended learning improvements.



### Security Awareness Proficiency Assessment Results

### Security Culture Survey (SCS)

The Security Culture Survey measures the sentiments of your users towards security in your organization – the psychological and social aspects that drive social behavior. The SCS leverages the CLTRe Security Culture Framework and research-driven measurement platform acquired by KnowBe4 earlier this year. The SCS shows you the overall effectiveness of your security culture program and how your security culture improves over time.



### Security Culture Survey Results

Both SAPA and SCS are strongly based in assessment science and allow you to measure the security knowledge and proficiency of your users and measure your organization's overall security culture posture.

# User Management

## Active Directory Integration

KnowBe4's Active Directory Integration allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes. Once the ADI is configured, users will be added, changed and archived in sync with changes made within AD automatically. You can also upload users with CSV files. If you use Microsoft Azure AD you can enable automatic user provisioning for the addition and removal of users via KnowBe4's Active Directory Integration.

### ✓ Active Directory Sync Report

[← Back to Active Directory Sync Reports](#)

[Users](#) [Groups](#) [Import Users](#) [Active Directory](#) [Merge Users](#) [Security Roles](#)

[Groups](#) 7 [Users](#) 539 [Memberships](#) 0


#### 539 users Newly Managed

List of users that existed but were not managed by Active Directory and were switched to being managed by Active Directory.

Name	Email	Manager	GUID
Aaron Lesch	Aaron.Lesch@kb4salesdemo.net	Boyer	ce498bc8-d44c-4ee2-9188-7d3ee54dd77b
Abbey Zieme	Abbey.Zieme@kb4-demo.com	Gibson	b2f63dda-5fd2-4c89-a9dd-3d2b66641896
Abe Trantow	Abe.Trantow@kb4-demo.com	Smith	453a6600-36e6-4f01-b4da-696451985ca8
Abram Hermiston	Abram.Hermiston@kb4salesdemo.net	Smith	2babd686-2d92-41bf-b9d6-832619a993c7

### Manage Users & Groups

[Users](#) [Groups](#) [Import Users](#) [Active Directory](#) [Merge Users](#) [Security Roles](#)

Received	Status	Affected Groups ?	Affected Users ?	Affected Memberships ?	Test Mode ?
8 hours and 32 minutes ago	✓ Completed	7	539	-	<a href="#">Details</a>
1 day, 8 hours, and 32 minutes ago	✓ Completed	-	5	1	<a href="#">Details</a>
2 days, 8 hours, and 32 minutes ago	✓ Completed	7	539	-	<a href="#">Details</a>
3 days, 6 hours, and 33 minutes ago	✓ Completed	7	539	-	<a href="#">Details</a>
3 days, 8 hours, and 33 minutes ago	✓ Completed	7	539	-	 <a href="#">Details</a>

## Smart Groups

### Put phishing, training and reporting on autopilot with Smart Groups

Automate the path your employees take to smarter security decisions. With the powerful Smart Groups feature, you can use each employees' behavior and user attributes to tailor phishing campaigns, training assignments, remedial learning and reporting.

You can create “set-it-and-forget-it” phishing and training campaigns so you can instantly respond to any phishing clicks with remedial training or have new employees automatically notified of onboarding training, and much more. Choose from five key criteria types per Smart Group then add your triggers, conditions, and actions to send the right phishing emails or training to the right employee at the right time.

Best of all, you have the ability to filter and pull reports based on the different criteria used in your Smart Group rules. For example, you may want to filter specific “Phish Event” criteria and create a report showing which users may or may not be improving as a result of the phishing tests you have conducted, enabling you to assign remedial training campaigns or advanced phishing tests for this Smart Group.

### Easily see and customize your workflows

Create sophisticated, targeted workflows without the headache, and make sure every employee is a strong building block of your human firewall. You can see the intersection of the criteria you specify—whether you're building simple phishing clickers remedial training workflow or complex, multi-criteria location, behavior and timing-based workflow. Use advanced segmentation logic to determine exactly who gets enrolled and un-enrolled in your workflows and when.


### Put time back into your day with powerful task automation

You can use workflows to set up remedial training and auto-enroll new employees into training. You can easily create time-based training re-enrollment, send phishing emails, manage your data, create custom reports, and more. The possibilities are endless!

 **Group: Sample SG** [← Back to Groups](#)

Smart Group Criteria + Add a new criteria 



User Field	The location	must	be equal to	Northeast	7248 Users		
User Field	The manager's name	must	be equal to	Miller	997 Users		
Phish Event	User must	have clicked	exactly	1 time	in the last 6 months	187 Users	

Save Cancel **Total Users: 187**

## Security Roles

KnowBe4's Security Roles feature can be used to assign granular access throughout the KnowBe4 console. Each Security Role is completely customizable to allow for the creation of the exact roles needed by your organization.

Because the roles are not simply a set of predefined permissions it is possible to create the exact permission model that fits your needs. Below are some common scenarios where Security Roles will allow the console administrator to give users access to only the portions of the KnowBe4 console that are needed to obtain their results:

- Auditors that need to review training history
- HR departments that want to see individual user results
- Training groups that want to review training content prior to deployment

Here are a few examples of access controls that can be set:

- Review (but don't touch!) results of phishing tests
- Management of Users and Groups
- Create new Phishing Security Campaigns
- Review of training content available in the ModStore

### Edit Security Role [← Back to Security Roles](#)

[Role Definition](#)   [General](#)   [Phishing](#)   [Training](#)

Phishing Campaigns ?	No Access	<b>Read Only</b>	Read/Write
Phishing Email Templates ?	No Access	Read Only	Read/Write
Phishing Landing Pages ?	No Access	Read Only	Read/Write
Phishing Reports ?	No Access	<b>Read Only</b>	
Phishing Dashboard ?	Don't Show	<b>Show</b>	

[Update Security Role](#)

# Reporting

## Ability to Download all Clickers Over all Campaigns as an Easy to Sort CSV File

**Phishing Security Test started at: 06/25/2017 02:52 AM** [← Back to Campaigns](#)

Campaign: Initial Campaign  
One time from categories: IT

[Overview](#) [Users](#)

541 Recipients	100% 541 Delivered	26% 146 Opened	26% 146 Clicked	0% 0 Replied	0% 4 Attachment Open	0% 0 Macro Enabled	1% 7 Data Entered	1% 8 Vulnerable Plugins	1% 9 Exploited	0% 4 Reported	0% 0 Bounced
-------------------	--------------------------	----------------------	-----------------------	--------------------	-------------------------------	-----------------------------	----------------------------	----------------------------------	----------------------	---------------------	--------------------

[Download CSV](#)

Name & Email	Date/Time	IP Address	IP Location	Browser	Browser version	OS
Rocio Morissette <a href="mailto:Rocio.Morissette@kb4-demo.com">Rocio.Morissette@kb4-demo.com</a>	06/25/2017 02:56:23	65.49.22.66	Fremont, CA	IE	11	Windows 8.1
Mitzie Larkin <a href="mailto:Mitzie.Larkin@kb4-demo.com">Mitzie.Larkin@kb4-demo.com</a>	06/25/2017 02:57:23	65.49.22.66	Fremont, CA	IE	11	Windows 8.1
Kurt Green <a href="mailto:Kurt.Green@kb4-demo.com">Kurt.Green@kb4-demo.com</a>	06/25/2017 02:57:23	65.49.22.66	Fremont, CA	IE	11	Windows 8.1

## Reporting Per User is Also Available for Annual Employee Evaluations

**Fritz.Connell@kb4-demo.com details** [← Back](#)

Personal Phish-Prone Percentage: **87.5%** (based on 8 emails delivered)

Clicked	Replied	Attachment Opened	Macro Enabled	Data Entered	Vulnerable Plugins	Exploited	Reported
✓					✓	✓	✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗
✓				✓			✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗
		✓	✓				✓ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗
	✓						✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗

### Training

Initial campaign

Passed 2016 Basics of Credit Card Security  
**Started at:** 07/17/17  
**Completed at:** 07/17/2017  
**Time spent:** 00:22:00  
[📄 Course Completion Certificate](#)

Passed 2018 Kevin Mitnick Security Awareness Training - 45 Min  
**Policy not acknowledged**  
**Started at:** 07/18/17  
**Completed at:** 07/18/2017  
**Time spent:** 00:20:00

General [Edit](#)

Email: Fritz.Connell@kb4-demo.com

First Name: Fritz

Last Name: Connell

Job Title:

Phone Number:

Mobile Phone Number:

Extension:

Location: Northwest

Division:

Manager Name: Jones

Manager Email: Jones@kb4-demo.com

Employee Number:

Group(s): kb4-demo.com, Accounting, Marketing

Aliases: Fritz.Connell@kb4-demo.com

Registration

Sign in count: 3

Created at: 06/21/2017 02:42:23

Confirmed at: 12/21/2017 01:42:24

Confirmation sent at:

Last sign in at: 07/29/2017 02:42:23

Last sign in IP:



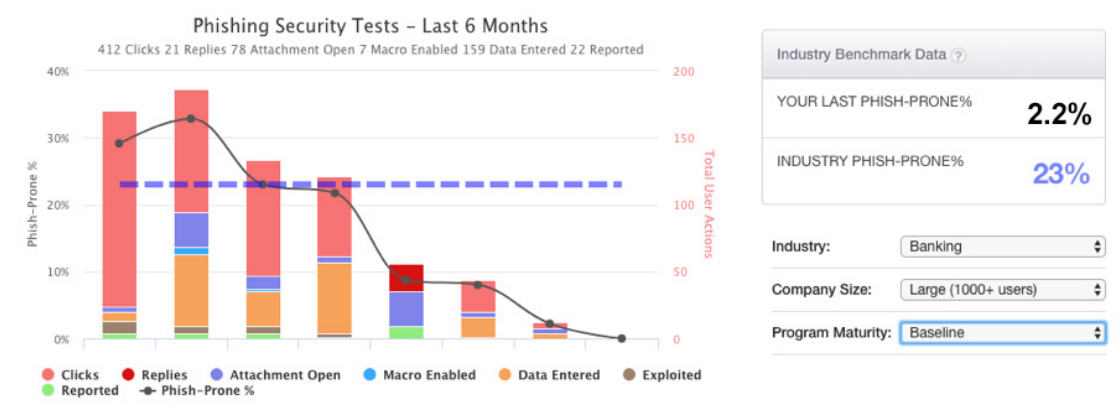
# Phishing Security Test Reports

[+ Create Campaign](#)

- Overview
- Campaigns
- Email Templates
- Landing Pages
- Reports

Date Range:  | Include Selected Campaigns:  | Include Campaigns Sent To:

Compare:  | Group Comparison By:  |  Include Non-failures



## Reports

- Campaigns
- Notification Templates
- Store Purchases
- My Training
- Reports

### Sign-ups

#### Users who signed up

Users who have signed-up for the service and logged in at least once

[CSV](#)

#### Users who did not sign up

Users who have accounts but have never signed in

[CSV](#)

### Courses

2018 Kevin Mitnick Security Awareness Training - 45 Min

All Users

Start:

End:

Include Archived Users

#### Users who started their courses

Users who have started their courses within the given date range

[CSV](#)

#### Users who did not start courses

Users who were enrolled within the given date range but have not started their courses

[CSV](#)

#### Users with incomplete courses

Users who started their courses within the given date range but have not finished them

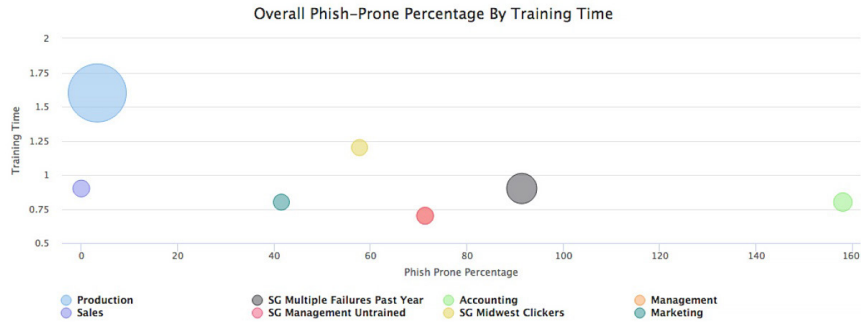
[CSV](#)

## Access a Collection of 60+ Built-in Advanced Reports that Provide Holistic View of Over Time

Executive and enterprise-level reporting gives visibility into your entire organization's security awareness performance with insights into correlated training and phishing simulation data over any specified period of time. Leverage Reporting APIs to create your own customized reports to integrate with other BI systems. If you manage multiple KnowBe4 accounts, Roll-up Reporting makes it easy to select reports and compare results in aggregate across accounts or multi-location offices.

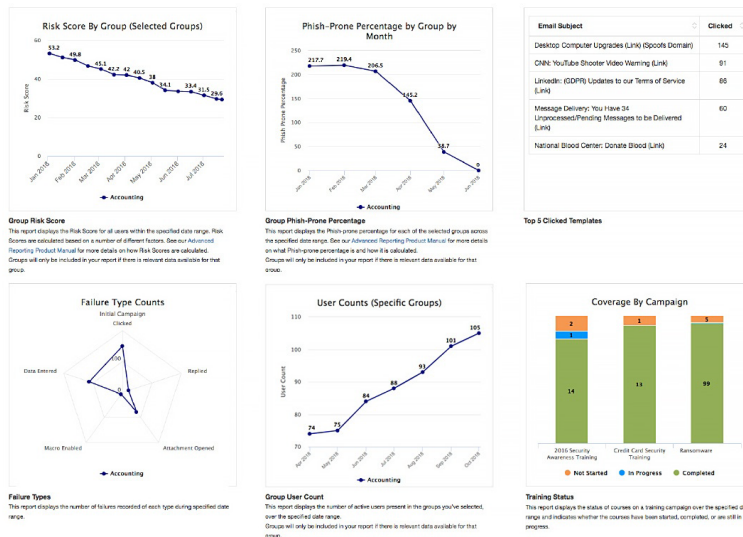
### Phish-Prone™ Percentage (PPP) By Training Time

This report shows your organization's PPP for groups relative to the amount of time spent training.



### Group Report Card

This report includes Risk Score, Phish-prone Percentage (PPP), Failure Types, Group Size, Top 5 failed templates and Training Status for the specified group over the past 6 months (or other time period).



### Identify Risk at User, Group, and Organizational Level with Virtual Risk Officer™

The innovative Virtual Risk Officer functionality helps you identify risk and enables you to make data-driven decisions when it comes to your security awareness plan.

#### Personal Risk Score



Risk Scores are calculated based on a number of different factors. See our [Advanced Reporting Product Manual](#) for more details on how Risk Scores are calculated.

#### Risk Score Factors

05/18/2018



#### Risk Score - Last 6 Months

Displays the user's Risk Score over time.



# Key Features

**Automated Security Awareness Program (ASAP):** Allows you to create a customized Security Awareness Program for your organization that will help you to implement all the steps needed to create a fully mature training program in just a few minutes!

**Custom Phishing Templates:** The ability to create custom phishing email templates from scratch or by changing our existing templates to send to your users. You can now go even further and customize scenarios based on public and/or personal information, creating targeted spear phishing campaigns, which replace fields with personalized data.

**Custom Phish Domains:** Phish Domain is the name we've given to the URL that populates in the lower left hand corner of your screen when you hover your mouse over a link in a suspicious email. We have a variety of different phish domains you can select from so the URL that populates is always changing, keeping your end users on their toes.

**Simulated Attachments:** These customized phishing templates can also include simulated attachments in the following formats: Word, Excel, PowerPoint and zip, and they can have macros in them (also zipped versions of these files).

**Custom Landing Pages:** Each phishing email template can also have its own custom landing page, which allows for point of failure education and landing pages that specifically phish for sensitive information.

**Anti-Prairie Dog:** KnowBe4's unique "anti-prairie dog" feature allows you to send random phishing templates at random times throughout a Phishing Campaign, mimicking real life phishing attacks preventing employees from giving each other notice of a phishing test.

**Phish Alert Button:** Employees now have a safe way to forward email threats to the security team for analysis and have the email deleted from the user's inbox to prevent future exposure. All with just one click.

**Phishing Reply Tracking:** Allows you to track if a user replies to a simulated phishing email and can capture the information sent in the reply.

**Social Engineering Indicators:** Patented technology, turns every simulated phishing email into a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email.

**Security Awareness Training:** The world's largest library of security awareness training content; including interactive modules, videos, games, posters, and newsletters with the Diamond level subscription.

**Training Campaigns:** Within the admin console you can quickly create ongoing or time-limited campaigns, select training module by user groups, auto-enroll new users, and automate "nudge" emails to your users who have not completed training.

**Assessments:** Assessments help you gauge the security awareness proficiency of your users and measure your organization's overall security culture posture. These two science-based assessments help you tailor training to address proficiency gaps and weaknesses, as well as monitor the impact your security awareness training program has on improving your users' knowledge and sentiment to security awareness over time.

**Smart Groups:** Allows you to use each employees' behavior and user attributes to tailor and automate your phishing campaigns, training assignments, remedial learning and reporting.

**Advanced Reporting:** Gives you a collection of 60+ built-in reports with insights that provide a holistic view of your entire organization over time, and dramatically expands instant detailed reporting on a host of key awareness training indicators. Additionally, you can leverage Reporting APIs to obtain data from your KnowBe4 console to create your own customized reports to integrate with other BI systems.

**Virtual Risk Officer:** The new innovative Virtual Risk Officer (VRO) functionality helps you identify risk at the user, group and organizational level and enables you to make data-driven decisions when it comes to your security awareness plan.

**USB Drive Test:** Allows you to test your user's reactions to unknown USBs they find.

**Active Directory Integration:** Allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes.

**Security Roles:** Allows you to define the level of access and administrative ability that you'd like specific user groups to have. This feature helps you follow the principle of least privilege in your KnowBe4 console, ensuring that the various areas of your KnowBe4 account are only accessible to those who need them.

**User Event API:** Enables you to send custom security-related user events from third party security platforms or any data source and push to your KnowBe4 Console. Add these events to your users' timelines, choose to use these events to augment your users' risk scores to help you tailor specific content for additional phishing or training campaigns.

**AIDA™ Artificial Intelligence-driven Agent:** Uses artificial intelligence to inoculate your users against various attack vectors of social engineering. AIDA quickly and easily allows you to simulate a multi-faceted social engineering attack, which will prompt your users to click on a phishing link, tap on a link in a text message, or respond to a voicemail--any of which could compromise your network. You will be able to see exactly who falls for your test and who is leaving your organization vulnerable.

# Subscription Levels

Our SaaS subscription is priced per seat, per year. We offer Silver, Gold, Platinum or Diamond levels to meet your organization's needs.

Features	MOST POPULAR			
	Silver	Gold	Platinum	Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program (ASAP)	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Brandable Content	✓	✓	✓	✓
Assessments	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration (ADI)	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
User Event API			✓	✓
Security Roles			✓	✓
Social Engineering Indicators (SEI)			✓	✓
USB Drive Test			✓	✓
Priority Level Support			✓	✓
Training Access Level III				✓
AIDA™ Artificial Intelligence-driven Agent BETA				✓
<b>PhishER™ - Optional Add-on</b>	✓	✓	✓	✓

**Silver Level:** Training Access Level I includes the Kevin Mitnick Security Awareness Training in the full 45-minute module and the executive 15-minute version. Also includes unlimited Simulated Phishing Tests, Assessments, and Enterprise-strength Reporting for the length of your subscription.

**Gold Level:** Includes all Silver level features plus Training Access Level II content which also includes KnowBe4 training modules. Gold also includes monthly Email Exposure Check (EEC) Reports and Vishing Security Tests using IVR attacks over the phone. (available for U.S. and Canada)

**Platinum Level:** Includes all features of Silver and Gold. Platinum also includes our Advanced Phishing Features; Smart Groups, Reporting APIs, User Event API, Security Roles, and landing page Social Engineering Indicators.

**Diamond Level:** Includes all features of Silver, Gold and Platinum plus Training Access Level III, giving you full access to our content library of 1,000+ items including interactive modules, videos, games, posters and newsletters. In addition, you will have access to our cutting-edge Artificial Intelligence-driven Agent (AIDA™), currently in beta that allows for simulated multi-faceted social engineering attack using email, phone, and SMS messaging. (available for U.S. and Canada)

**PhishER:** Available as a stand-alone product or as an optional add-on across all subscription levels. PhishER is your lightweight SOAR platform to orchestrate your threat response and manage the high volume of potentially malicious messages reported by your users. Emails can be reported through the KnowBe4 Phish Alert Button or simply by forwarding to a mailbox. With automatic prioritization for emails, PhishER helps your InfoSec and security operations team cut through the inbox noise and respond to the most dangerous threats more quickly. (minimum 101 seats)

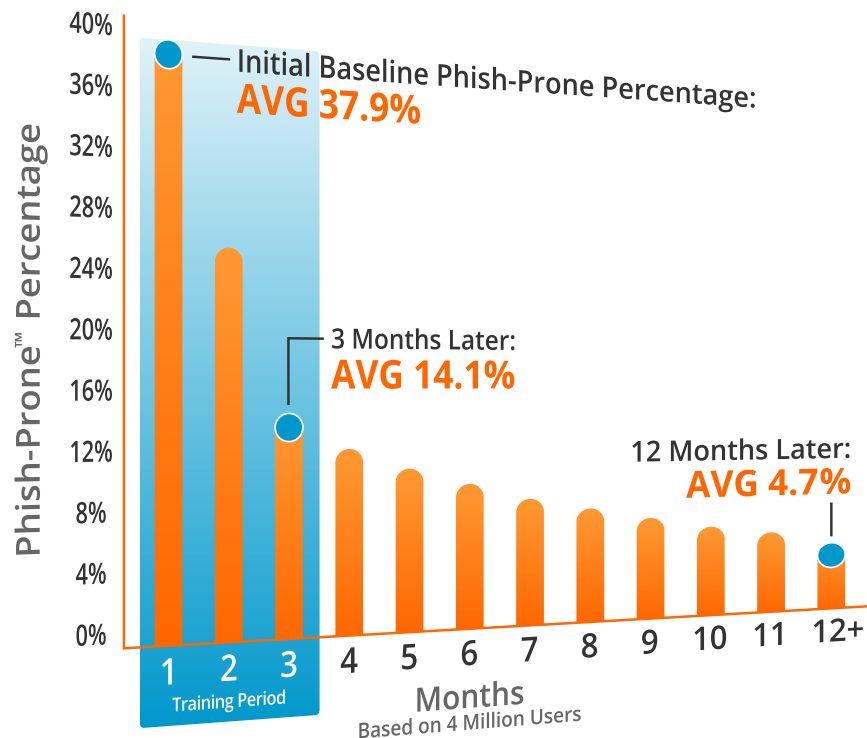
“Social Engineering is information security’s weakest link.”  
– Kevin Mitnick, ‘The World’s Most Famous Hacker’, IT Security Consultant

## Visible Proof The KnowBe4 System Works

When you invest in Security Awareness Training and Phishing Security Testing you see value and ROI—fast.

The results of the 2020 KnowBe4 Phishing Industry Benchmarking Report clearly show where organizations’ Phish-Prone percentages started and where they ended up after 12 months of regular testing and security awareness training.

The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 37.9%. However, there is light at the end of the tunnel. Fortunately, the data showed that this 37.9% can be brought down more than half to just 14.1% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 4.7% on average.



KnowBe4  
Human error. Conquered.