

KnowBe4  
Human error. Conquered.



# Buyer's Guide

Security Awareness Training & Simulated Phishing Platform

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

KnowBe4 is the world's most popular integrated platform for security awareness training and simulated phishing. This guide explains everything that is included in the KnowBe4 Security Awareness Training and Simulated Phishing platform.

## Executive Summary

### Security Awareness Training & Simulated Phishing 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 most popular integrated Security Awareness Training and Simulated Phishing platform with over 15,000 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, giving you access to a constantly updated content library of 500+ items based on your subscription levels.

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



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

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

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

#### **Kevin Mitnick Security Awareness Training (25-Min)**

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. You'll learn how to spot red flags that alert you to possible danger in an email and then you'll help Jake Sanders, a typical computer user, steer clear of six real-world social engineering attacks.

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

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



## KnowBe4 Training Modules

*Also included in Training Access Level II*

### **KnowBe4 Basic Security Awareness Training Course (30-min)**

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

### **Basics of Credit Card Security**

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

### **Creating Strong Passwords**

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

### **Handling Sensitive Information Securely**

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

### **Mobile Device Security**

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

### **CEO Fraud**

In this 10-minute module, employees are quickly brought up to speed to inoculate them against what the FBI calls "Business Email Compromise" and what is commonly known as CEO Fraud. Concepts like social engineering, email spoofing, and the two ways that CEO Fraud is being perpetrated are covered. There is a short video with a live demo of an infected Excel file, and a short quiz to test understanding at the end. Downloadable PDF Resources: Social Engineering Red Flags, and Security Awareness: Best Practices.

### **Safe Web Browsing**

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

### **Ransomware**

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

### **Ransomware For Hospitals**

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

### **PCI Compliance Simplified**

This 15-minute module uses real examples of credit card fraud, and how to protect your organization against this by being PCI compliant. This course is for anyone that's responsible for handling credit cards in your organization and qualifies as Security Awareness Training. Especially owners, the CFO or Controller, managers and IT people in charge of credit card processing should take this course. After the training, you are able to download essential references regarding being or becoming PCI compliant.

### **GDPR**

The goal of this module is to familiarize you with the General Data Protection Regulation, also known as the "GDPR"; what it means to your organization; and what it means to your job function.

## Common Threats

In this 15-minute module you'll learn about strategies and techniques hackers use to trick people just like you. We provide you with three real-world-based scenarios that show you how these common threats can take place. At the end of each scenario, Kevin Mitnick will take you behind the scenes and reveal exactly how each type of hack is accomplished.

## The Danger Zone

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

## Financial Institution Physical Security (for Financial Institutions only)

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

## Your Role

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

## Red Flags: Warning Signs that Alert You

This fully interactive 8-minute module, shows you the seven areas of an email to pay attention to if you don't want to be hacked. Once you know where to look, it shows seven real-life examples, and you'll be asked to spot the red flags in each.

## GLBA Compliance Course (for Financial Institutions only)

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



## KnowBe4 Training Micro-modules

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

Credit Card Security (Part 1)  
Credit Card Security (Part 2)  
Danger Zone Exercise Micro-module  
Email Spoofing  
Handling Sensitive Information Securely (Part 1)  
Handling Sensitive Information Securely (Part 2)

Ransomware  
Safe Web Browsing  
Social Engineering  
Social Media Best Practices  
Strong Passwords  
USB Attack

### Executive Series Micro-modules

CEO Fraud  
Mobile Device Security  
Remote and Travel WiFi Dangers  
Ransomware and Bitcoin  
Social Media Precautions for Executives

Social Engineering the Executive  
Decision-Maker Email Threats  
Safe Web Browsing With Corporate Devices  
Securely Working From Home  
Secure Destruction of Sensitive Information



## Securable.io Videos

*Also included in Training Access Level III*

FISMA- Federal Information Security Management Act  
Intro to Phishing  
LinkedIn Security  
Monitoring Facebook Services  
Protect Your Kids Online

Public WiFi Safety  
Ransomware Attacks  
Traveling Abroad  
Twitter Security  
USB Safety



## AwareGO Videos

*Also included in Training Access Level III*

CEO Scam  
Chain Mail  
Clean Desk  
Dumpster Diving  
Free WiFi  
Handling Confidential Material  
Home WiFi  
HTTPS  
Keylogger  
Malicious Attachments  
Password Handling  
Passwords

Phishing  
Pop Ups  
Printouts  
Removable Media  
Shoulder Surfing  
Social Engineering  
Software Installs  
Spear Phishing  
Spyware  
Tailgating  
Think Twice  
USB Key Drop



## Security Awareness Company Content Library

*Also included in Training Access Level III*

### Cyber Security Awareness Interactive Learning Modules

- Call Center & Help Desk Awareness ILM
- Computer Security & Data Protection ILM
- Data Classification ILM
- Developing an Incident Response Plan
- Human Firewall ILM
- OWASP Top Ten ILM
- Phishing Andrew's Inbox ILM
- Ransomware ILM
- SAF Pre-Assessment
- Understanding and Protecting PII ILM

### Cyber Security Awareness Compliance Modules

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

### 30+ Cyber Security Awareness Games

#### Cyber Security Awareness Videos (2-5 mins)

- 10 Ways to Avoid Phishing Scams
- 10 Ways to Keep PII Private
- 10 Ways to Stay Safe on Social Media
- A Day of Bad Passwords
- APTs
- Back Up
- Being a Human Firewall
- Beyond Phishing
- Catching Malware
- Cyber Crime Starts with You
- Dangers of USBs
- Data Breach Overview
- Data Breaches and You
- Data Classification Overview
- Data Loss and Insider
- Definition of Social Engineering
- Dumpster Diving
- Email Spoofing
- Examples of Insider Jobs
- Examples of Phishing
- Firewalls
- Free Wifi
- Hide Your Passwords
- Human Firewall and Data Classification
- Incident Response 101
- Introduction to Ransomware
- Introduction to the Cloud
- Low-Tech Hacks to Steal Your ID
- Making Strong Passwords
- Mobile Cyber Crime
- Mobile Security Overview
- Mouse Overs
- Non-Technical Security Skills
- Non-Technical and Physical security tips and tricks
- Password Security

### Cyber Security Concepts Modules

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

### 140+ Cyber Security Awareness Posters

- Phishing Contest Winner
- Phishing From Facebook
- Phishing From Netflix
- Phishing From Your Bank
- Phishing in Action
- Physical Security Threats
- PII and Compliance
- Pretexting 1 (Fake Fraud Protection)
- Pretexting 2 (Fake Help Desk)
- Pretexting From Fake I.T.
- Pretexting: Fake Employee to Help Desk
- Pretexting: Fake Executive to I.T.
- Pretexting: From Fake Credit Card Company
- Privacy Vs. Security
- Proper Hard Drive Disposal
- Road Warriors
- Safe Surfing 1: HTTP vs HTTPS & Online Authentication
- Security Myths Busted
- Social Media
- Social Media Data Mining
- Social Networking Do's and Don't's
- Spam
- The CIA Triad
- The Domains Triad
- The Human Firewall's Top Concerns in All Three Domains
- The Many Lives of PII
- The Many Lives Triad
- Types of Social Engineering
- Understanding Encryption
- What Does a Social Engineer Look Like?
- What is I.D. Theft
- What is PII?
- Why Executives Need Awareness
- Why Security Awareness?
- Your Security Awareness Journey



## Security Awareness Training Content By Subscription Level

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



# 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.

ASAP | Automated Security Awareness Program

## Start your Automated Security Awareness Program (ASAP)

Create a customized Security Awareness Program for your organization that helps you to implement all the steps needed to create a fully mature training program.

ASAP has the necessary information

Information

ASAP is a simple tool engineered to yield powerful results. By stepping through the brief questionnaire, we will collect the necessary information to create the foundations of a mature security awareness, training, behavior, and culture management program.

If you have questions at any time during the process, or would like to work with an experienced security awareness expert, don't hesitate to contact a friendly member of our staff.

Let's Get Started >>

ASAP | Automated Security Awareness Program

## Your Security Awareness Program Tasks

Based on your questionnaire feedback, we have generated the following tasks that need to be completed for you to get the most out of your Automated Security Awareness Program.

0% of 18

Task List Calendar

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

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.

ASAP | Automated Security Awareness Program

## Your Security Awareness Program Tasks

Based on your questionnaire feedback, we have generated the following tasks that need to be completed for you to get the most out of your Automated Security Awareness Program.

0% of 18

Task List Calendar

July 2017

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

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.

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

#### Dashboard

##### Phishing

###### Phishing Security Tests – Last 6 Months

412 Clicks 52 Attachment Open 7 Macro Enabled 159 Data Entered 13 Reported

Day	Clicks	Attachment Open	Macro Enabled	Data Entered	Reported	Phish-Prone %
Feb 24	30	2	1	1	1	35
Feb 26	18	6	1	12	1	28
Feb 28	18	1	1	1	1	22
Mar 1	18	1	1	1	1	18
Mar 3	18	1	1	1	1	15
Mar 5	13	1	1	1	1	12
Mar 7	12	1	1	1	1	10
Mar 9	12	1	1	1	1	8
Mar 11	5	1	1	1	1	6
Mar 13	5	1	1	1	1	5
Mar 15	2	1	1	1	1	4
Mar 17	2	1	1	1	1	3
Mar 19	1	1	1	1	1	2
Mar 21	1	1	1	1	1	1
Mar 23	1	1	1	1	1	1

#### 100.0% Delivered (3787)

Based on 3787 Sent  
0 Bounced

[See more phishing reports](#)

##### Phish Alert

Installed 170 times, uninstalled 31 times

**Total Emails Reported: 348**  
Simulated Reported: 116  
Non-simulated Reported: 232

###### Reporting of simulated vs non-simulated phishing emails

Last 30 days

Date	Simulated	Non-Simulated
Feb 24	3	3
Feb 25	4	8
Feb 26	3	9
Feb 27	5	2
Feb 28	5	15
Mar 1	5	10
Mar 2	4	12
Mar 3	4	8
Mar 4	4	2
Mar 5	1	1
Mar 6	1	1
Mar 7	5	15
Mar 8	5	15
Mar 9	2	5
Mar 10	1	3
Mar 11	5	10
Mar 12	4	12
Mar 13	3	9
Mar 14	3	9
Mar 15	3	3
Mar 16	5	10
Mar 17	5	4
Mar 18	3	9
Mar 19	5	5
Mar 20	2	2
Mar 21	4	9
Mar 22	4	12
Mar 23	4	4

##### Training

###### Campaigns in Progress

[See all](#)

- Sales Ongoing Campaign** In progress 89%
- Powerplant Production Ongoing** In progress 80%

###### Other Campaigns

- Initial campaign** Completed 100%

To invite your users to start a course, copy this link:

```
https://training.knowbe4.com/login?domain=kb4-demo.com  
https://training.knowbe4.com/login?domain=kb4-sales-demo.com  
https://training.knowbe4.com/login?domain=kb4salesdemo.com  
https://training.knowbe4.com/login?domain=kb4salesdemo.co.uk  
https://training.knowbe4.com/login?domain=kb4salesdemo.net
```

Send it to them by email or other means.

# 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:**  
**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  
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

**From:** AccountRecovery@noreply.accountreset.com  
**Reply-to:**  
**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?est=02f3e9wx0>

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

**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:**  
**Shipping Details : (order will arrive in 1 shipment)**

<b>Order #:</b>	842J5O-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**

**Delivery Status:** Could not deliver package due to invalid information.  
**Fix Errors:** [HERE](#)  
 Please click the above link to correct the errors and we will attempt to re-deliver your package.  
**Driver Release Location:** COULD NOT DELIVER

**Shipment Detail**

**Number of Packages1**  
**PAK Service:** 1 DAY OVERNIGHT - URGENT  
**Weight:** 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

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   after sending is complete

Track replies to phishing emails

Categories   [Preview](#)

Difficulty Rating

Phish Link Domain

Landing Page

Add Exploit

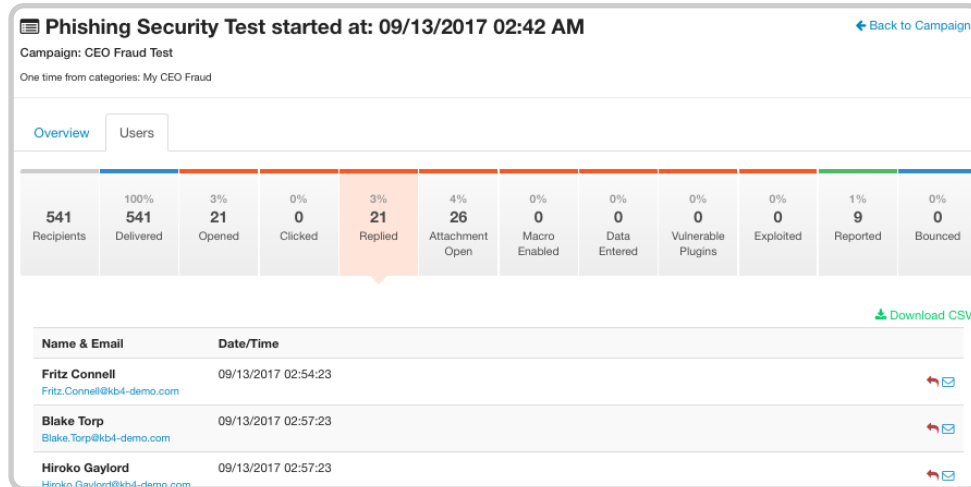
Add Clickers To

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

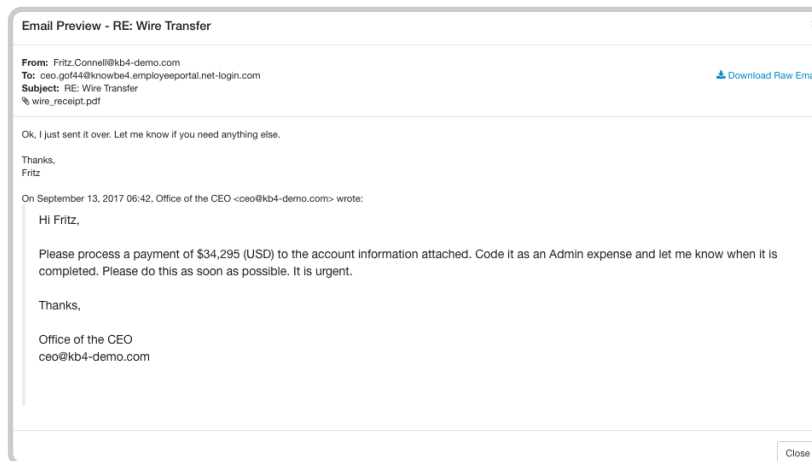
[Create Campaign](#)

## 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.



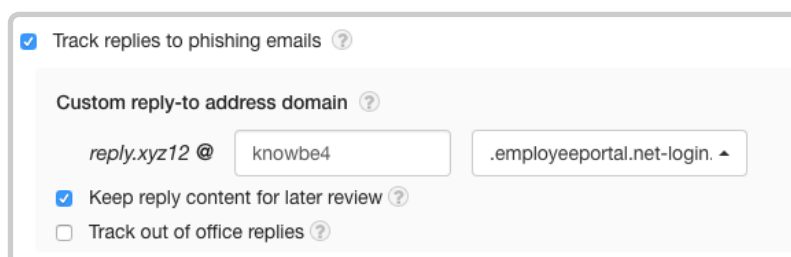
We have created a new category of system phishing templates called “Reply-To Online” which are specifically designed to test whether users will interact with “the bad guys” on the other end. However, the Phishing Reply Tracking also works with any of our 2000+ phishing templates.



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

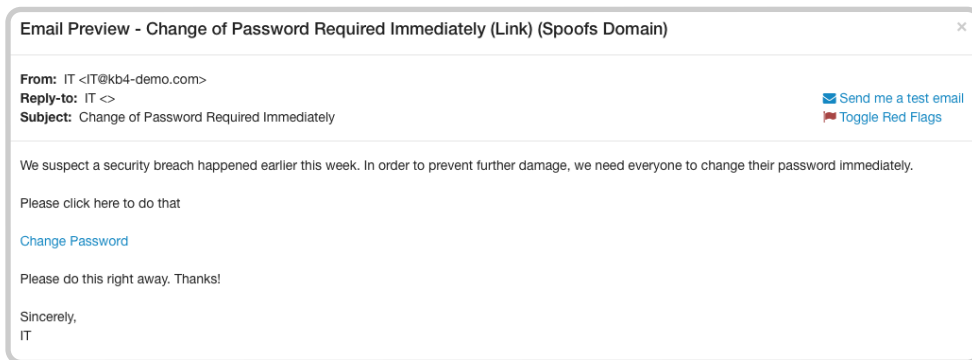
Additional options for this feature include:

- 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.

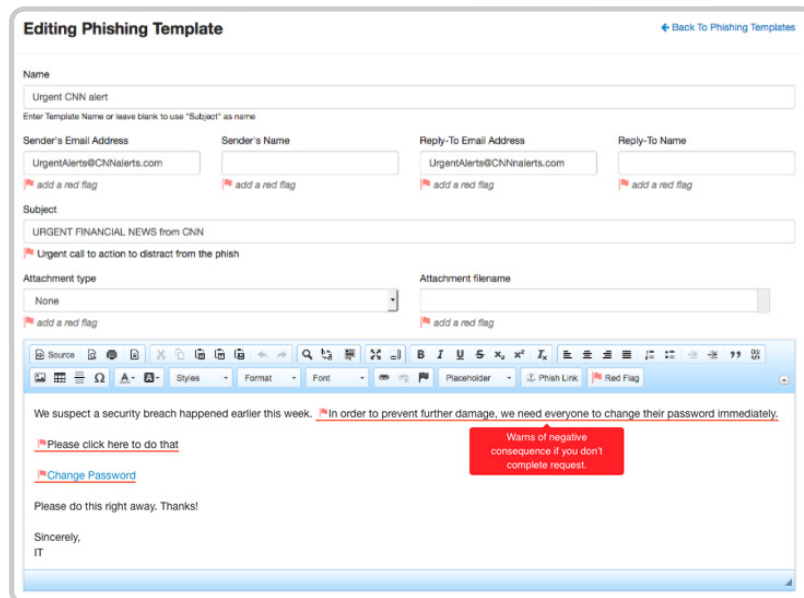


## Social Engineering Indicators (SEI)

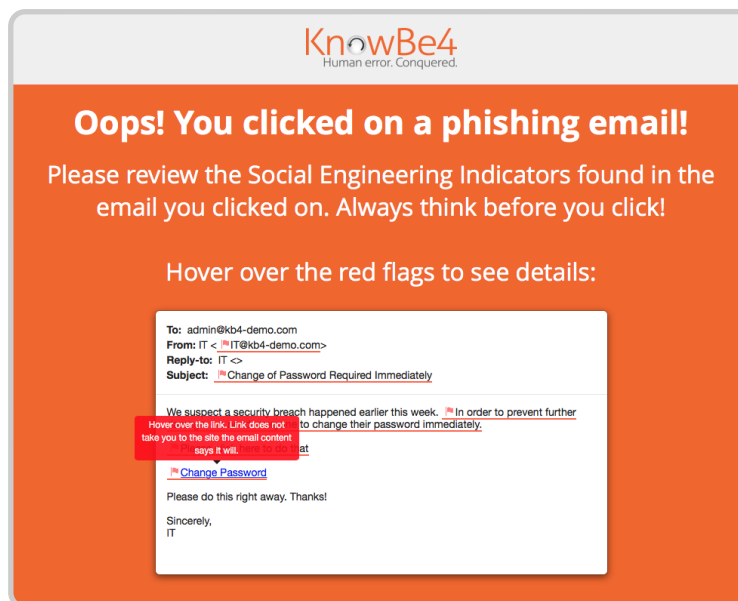
Patented technology that turns every simulated phishing email into a tool IT can use to instantly train employees. When a user clicks on any of the 2000+ KnowBe4 simulated phishing emails, they are routed to a landing page that includes a dynamic copy of that phishing email showing all the red flags.



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.



## Phish Alert Button

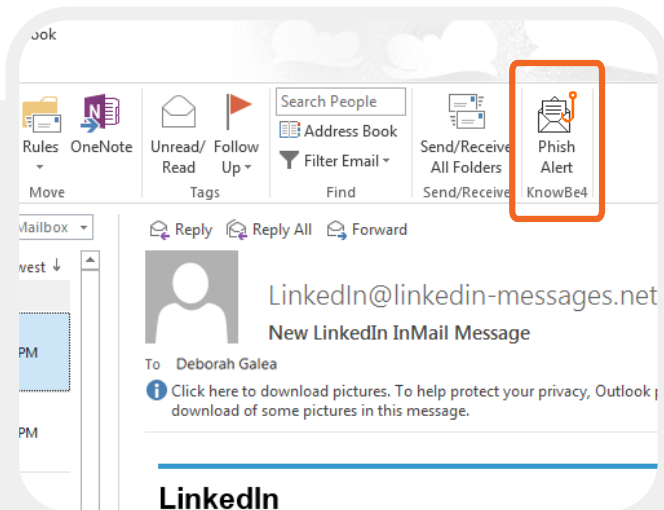
### Employees Report Phishing Attacks With One Click

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 and Outlook for Office 365, Exchange 2013 and 2016, IBM Notes 8.5.3 and 9.0, Chrome 54 and later (Linux, OS X and Windows)

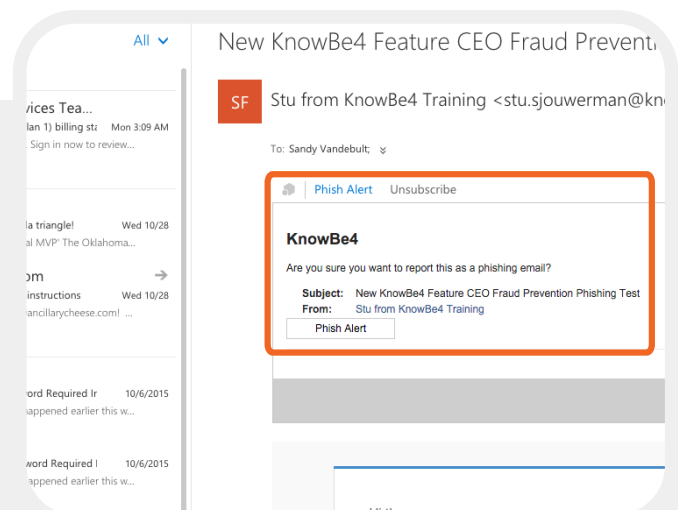
## Outlook Toolbar

Adds a Phish Alert button for your users



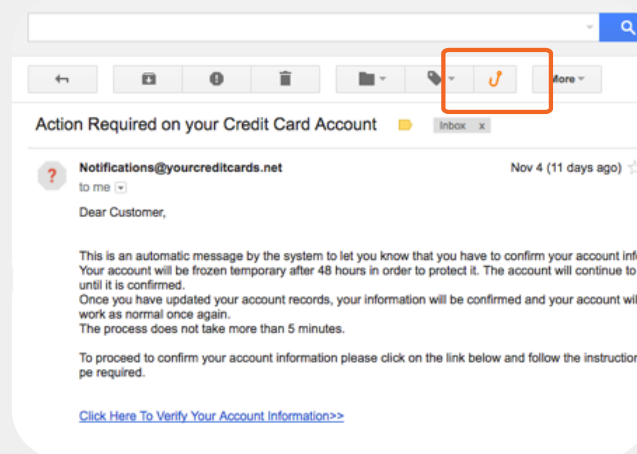
## Office 365 Add-in Pane

Adds a Phish Alert link for your users



## Gmail Extension

Adds a Phish Alert button for your users





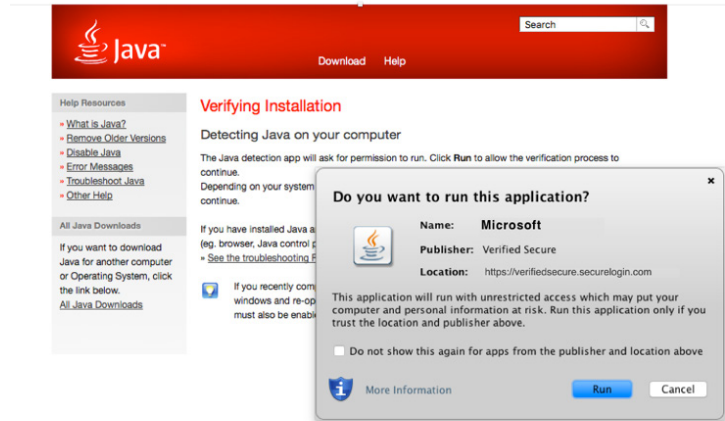
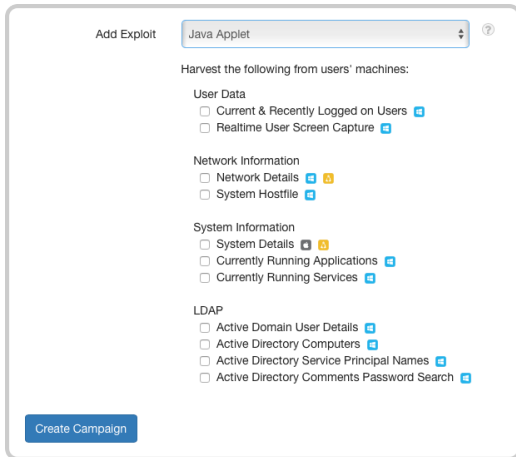
# Advanced Phishing Features

## EZXploit™

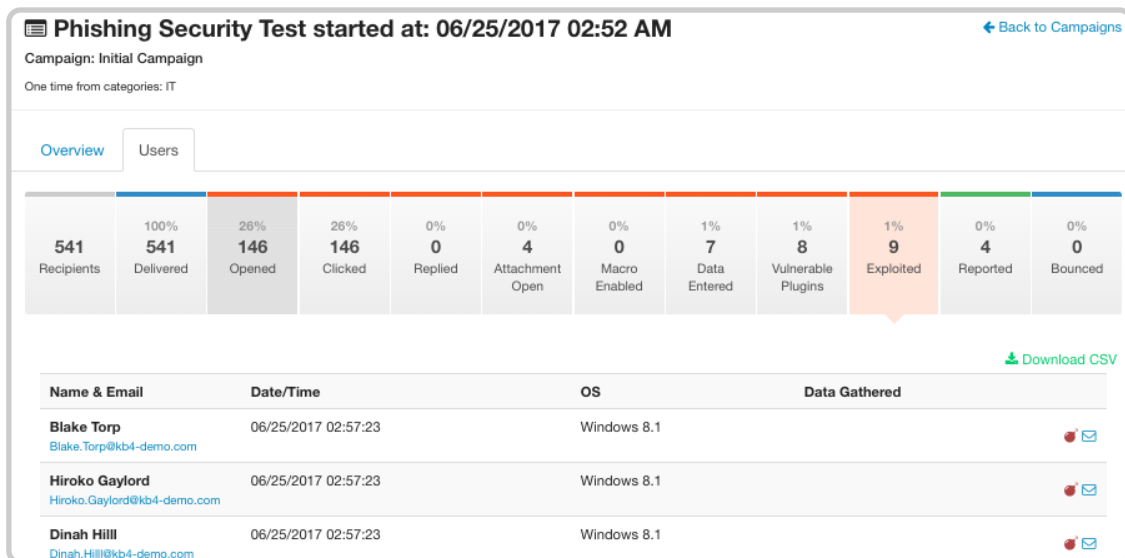
EZXploit has patent-pending functionality that allows you to do an internal, fully automated "human pentest" at a fraction of the cost to do this manually.

EZXploit takes your simulated phishing attacks to the next level. You can now find out which of your users can actually be exploited by hackers.

Using EZXploit, you can launch a simulated phishing attack on (groups of) users that contains a link to a web page – which if clicked on – is recorded as a 'failure' in your admin console, but then takes an extra step and comes up with a secondary ploy like a Java popup that the user is social engineered to click on.



If the user clicks on the secondary action, another 'failure' is recorded in your admin console and their workstation can be scanned for several things like user name, IP address and other data related to that user's workstation and Active Directory information as specified by you in the admin console.



No malicious action is performed on the user's system and all private data is deleted upon campaign deletion. Within your KnowBe4 admin console you can view the result data collected by EZXploit in a timeline preview as well as a full download of the data gathered.

EZXploit gives you a new, automated way to pentest your users and prevent hackers from owning your network.

### Exploit Details for: Fritz.Connell@kb4-demo.com

Exploited At: 06/25/2017 03:03 AM

Attack Vector: Java Applet

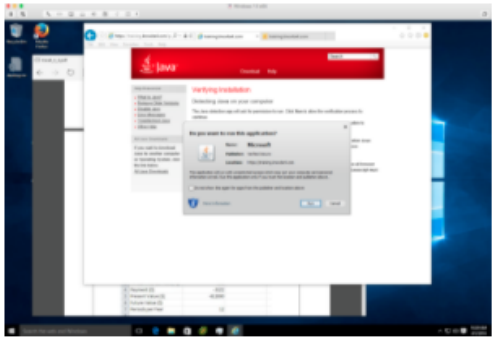
[← Back to PST Users](#)

Details

#### User Data

##### Realtime User Screen Capture

[Download Output \(437KB\)](#)



#### Network Information

##### Network Details

[Download Output \(3KB\)](#)

```
Windows IP Configuration

Host Name . . . . . : GK-W10-LVM
Primary Dns Suffix . . . . . : DevKB4-a.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS
...download to continue
```

## 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.

### Initial USB drive test

Started at: 07/20/2017 02:52 AM  
Location: Parking lot  
We set up this test to see what happens when we leave 4 usb devices in the parking lot. This was done before any training.

[Back to USB Drive Tests](#)

[Download CSV](#)

Overview Details

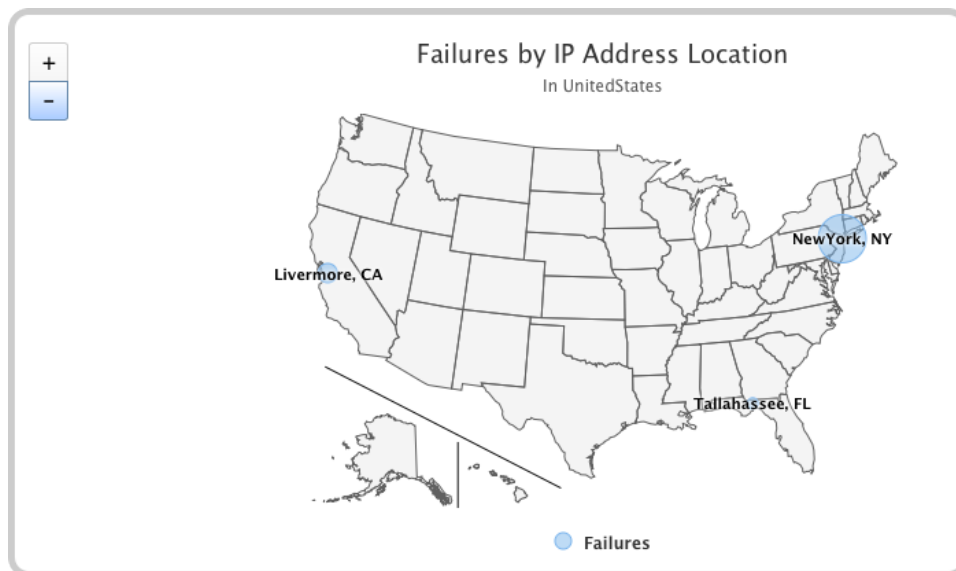
Search:

File Type	Opened	Macro Enabled	IP Address	IP Location	Username	Display Name	Computer Name
Word With Macro	07/23/2017 02:42:22	07/23/2017 02:42:22	216.81.87.6	Gaithersburg, MD	jkrauss	Joey Krauss	eng-sw-jk
Excel With Macro	07/22/2017 02:42:22	07/22/2017 02:42:22	198.47.77.10	CocoaBeach, FL	frankc	Frank Connel	acct-ap-fc
Word	07/21/2017 02:42:22		198.47.77.10	CocoaBeach, FL			

Username, Display Name, and Computer Name information are only available if the macro was enabled.

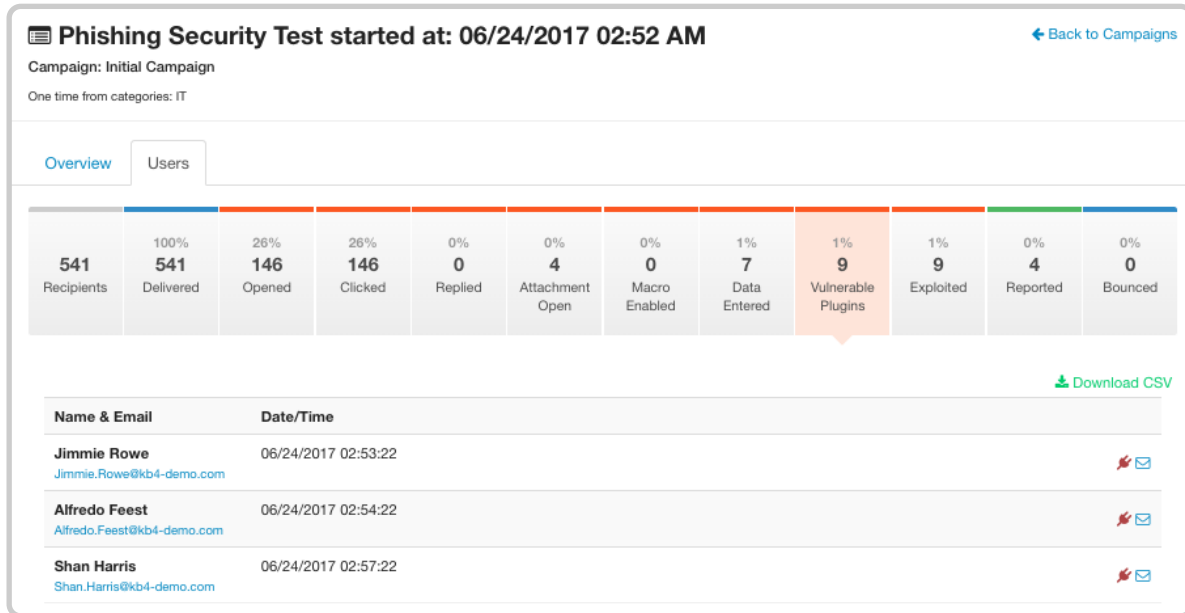
## GEO-location

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

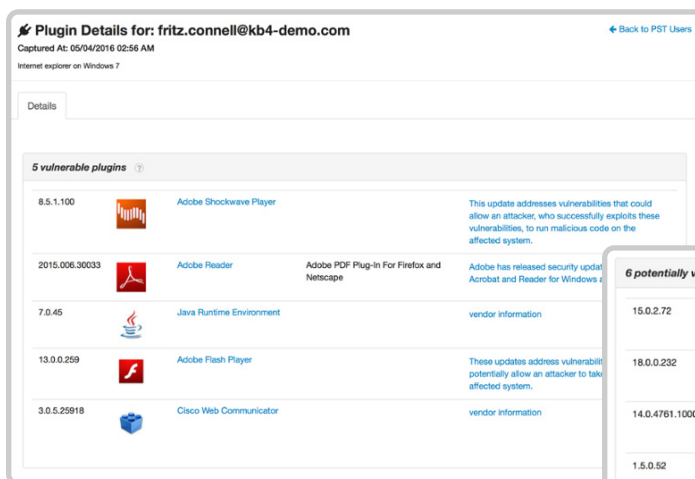


## Vulnerable Browser Plugin Detection

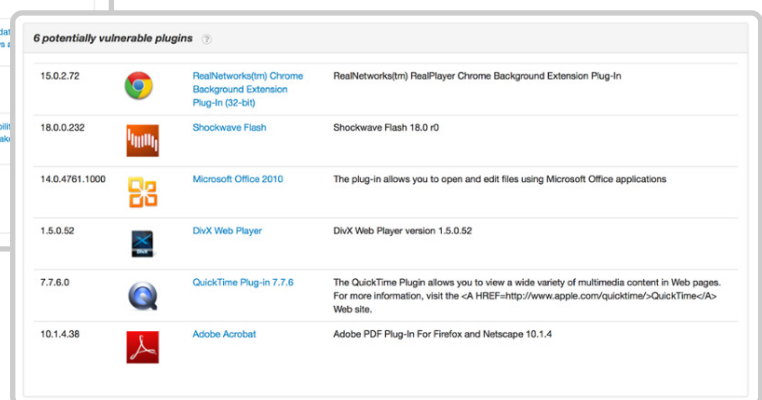
Information about vulnerable plugins your users have installed on their browsers is automatically gathered during a phishing campaign. When a user fails and clicks on your phishing test, they arrive on our landing page which will gather information on what plugins are installed on that user's browser. We look at the results and compare them to a database of known vulnerable plugins and report it back to you.



You can see a detailed list of what vulnerable plugins a user has installed. This view will also provide a link to any additional information we can provide about that vulnerable plugin.



**Example of Detailed Report Showing Vulnerable Plugins**



**Example of Detailed Report Showing Potentially Vulnerable Plugins**

# 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.

### Sample Training Campaigns

Training Campaigns				<a href="#">+ Create Campaign</a>			
Campaigns				<a href="#">Notification Templates</a>	<a href="#">Store Purchases</a>	<a href="#">My Training</a>	<a href="#">Reports</a>
Campaign Name	Groups	Courses	Complete %				
<a href="#">Powerplant Production Ongoing</a> 7/16/17 - (No End Date)	<a href="#">Production</a> <a href="#">Production West</a>	2018 Kevin Mitnick Security Awareness Training - 45 Min	<span>In progress</span> <span>80%</span>				
<a href="#">Sales Ongoing Campaign</a> 7/11/17 - (No End Date)	<a href="#">Sales</a>	2016 Basics of Credit Card Security	<span>In progress</span> <span>89%</span>				
<a href="#">Initial campaign</a> 7/1/17 - 7/31/17	<a href="#">All Users</a>	2016 Basics of Credit Card Security 2018 Kevin Mitnick Security Awareness Training - 45 Min	<span>Completed</span> <span>100% Completed</span>				

### Our Console Allows You To Schedule Multiple Training Campaigns Which Can Overlap

#### Edit Training Campaign

[← Back to Training](#)

Name:

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

End Campaign At:  Specify Date  Relative Duration  No End Date

**Specify Date & Time**

Courses:   
2016 Basics of Credit Card Security  
2018 Kevin Mitnick Security Awareness Training - 45 Min

Enroll Groups:

Automatically enroll users that are added to the above groups in the future

Enable courses to be done multiple times

Add Completed Users To:

Remove Completed Users From:

Notifications:

- Send welcome notification to [User Q](#) on enrollment [Edit](#) [Delete](#)
- Remind [User Q](#) 5 days after enrollment [Edit](#) [Delete](#)
- Remind [User Q](#) 5 days before due date [Edit](#) [Delete](#)
- Remind [User Q](#) 2 days before due date [Edit](#) [Delete](#)
- Send completion notification to [User Q](#) [Edit](#) [Delete](#)

[+ Add Notification](#)

## Initial campaign

[← Back to Training Campaigns](#)

Groups: All Users

Overview **Users**

### 2016 Basics of Credit Card Security

100% Completed

### 2018 Kevin Mitnick Security Awareness Training - 45 Min

100% Completed



#### 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

- Send welcome notification to User on enrollment
- Remind User 5 days after enrollment
- Remind User 5 days before due date
- Remind User 2 days before due date
- Send completion notification to User

### User training activity

Number of users that started at least one course (per day)



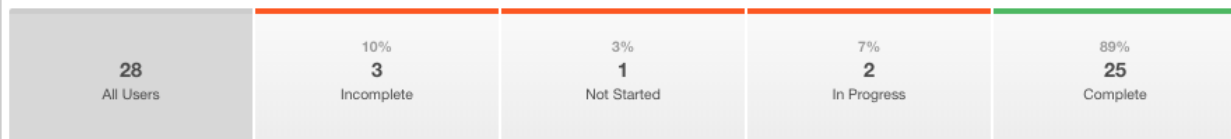
## Sales Ongoing Campaign

[← Back to Training Campaign Summary](#)

for course 2016 Basics of Credit Card Security

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

Overview **Users**



[Notify Selected](#)
[Pass Selected](#)
[Reset Progress](#)
[Download CSV](#)

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

# 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.

### ✓ 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



Criteria Type	Criteria	Count
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	100%	26%	26%	0%	0%	0%	1%	1%	1%	0%	0%
Recipients	Delivered	Opened	Clicked	Replied	Attachment Open	Macro Enabled	Data Entered	Vulnerable Plugins	Exploited	Reported	Bounced

[Download CSV](#)

Name & Email	Date/Time	IP Address	IP Location	Browser	Browser version	OS
Rocio Morissette <a href="#">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="#">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="#">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:	

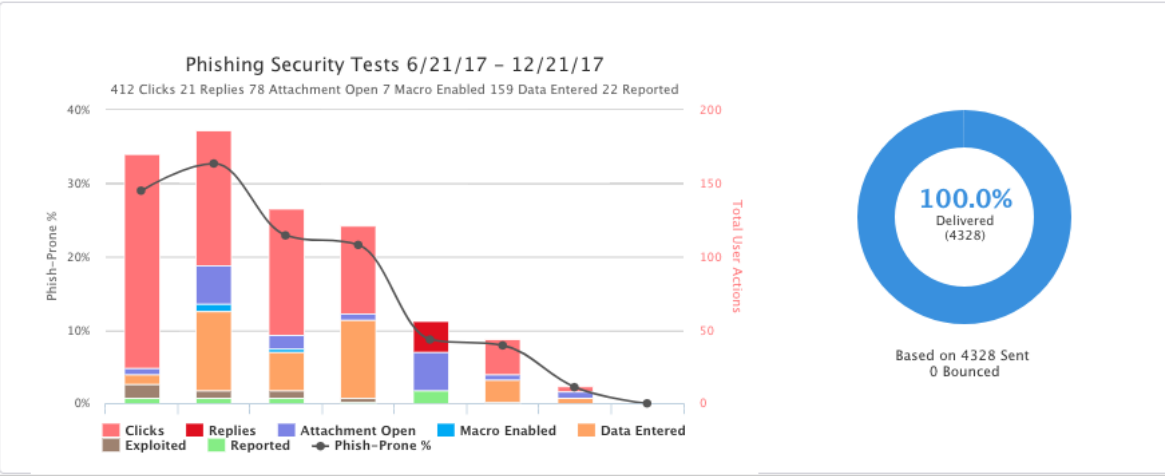
# Phishing Security Test Reports

[+ 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](#)

# 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. Custom phish domains may be added upon request.

**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.

**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.

**Detailed Reporting:** Enterprise-strength reporting capabilities provide stats and graphs for both training and phishing, including instant reports on Phishing failures by groups, by location, and the Top 50 'clickers' report that shows your most Phish-prone users. You can drilldown into one-time and recurring campaigns for more detail. You can also leverage Reporting APIs to customize and obtain reports by integrating with other business systems that present data from your KnowBe4 Console.

**EZXploit:** Patent pending functionality that allows an internal, fully automated "human pentest".

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

**Vulnerable Browser Plugin Detection:** Within your console, you can automatically detect what vulnerable plugins any clickers on your phishing tests have installed in their browsers.

**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.

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

**Silver Level:** Training Access Level I includes the Kevin Mitnick Security Awareness Training in the full 45-minute module, the shortened 25-minute module, and the executive 15-minute version. Also includes unlimited Simulated Phishing Tests 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.

- Email Exposure Check monthly reports show you which email addresses from your domain are exposed on the Internet and are a target for phishing attacks
- Vishing Security Tests using IVR attacks over phone (available for U.S. and Canada)

**Platinum Level:** Includes all features of Silver and Gold. Platinum also includes our Advanced Phishing Features; EZxploit, USB Drive Test, Vulnerable Browser Plugin Detection, Smart Groups, Reporting APIs, Security Roles, and landing page Social Engineering Indicators.

- EZxploit™ is a patent-pending functionality that allows an internal, fully automated "human pentest" (available for U.S. and Canada)
- USB Drive Test™ allows you to test your user's reactions to unknown USBs they find
- Vulnerable Browser Plugin Detection reports on browser / device used to open a phishing email and vulnerable browser plugins the user has installed
- 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
- Security Roles allows you to provide role-based access to specific areas of your KnowBe4 admin console
- 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.
- Reporting APIs enable you to customize and obtain reports by integrating with other business systems that present data from your KnowBe4 Console.

**Diamond Level:** Includes all features of Silver, Gold and Platinum. Diamond also includes Training Access Level III, giving you full access to our content library of nearly 500 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.

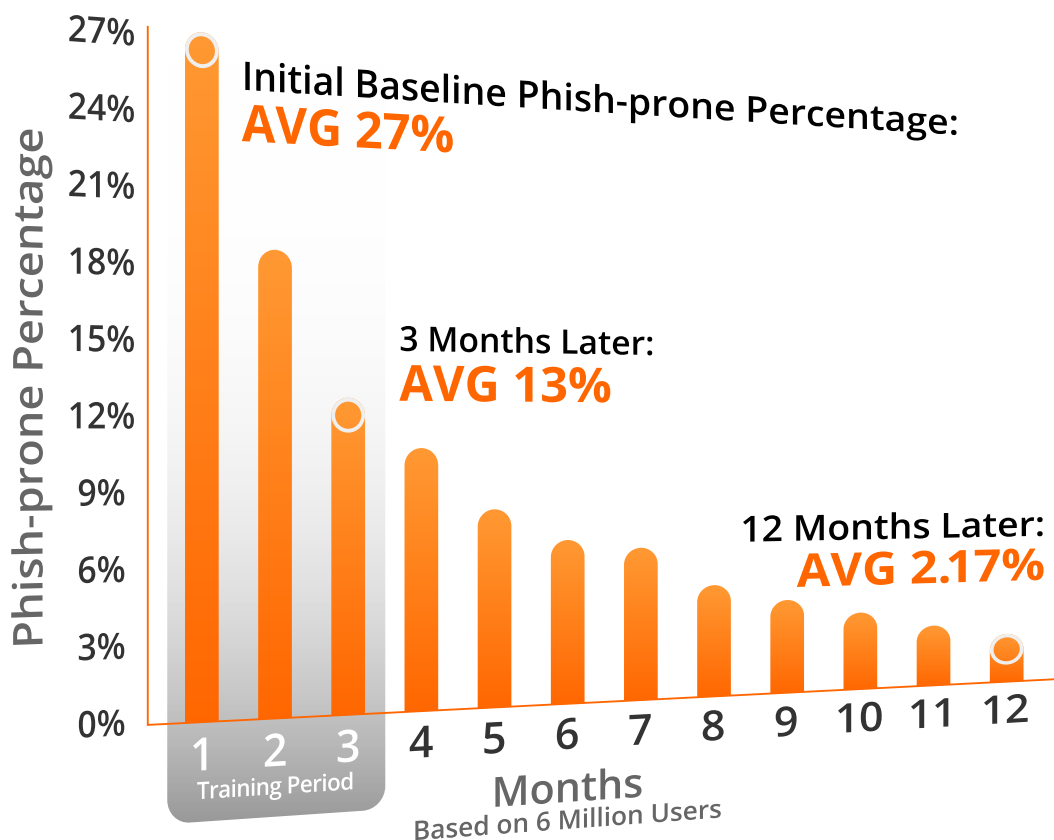
- AIDA™ uses artificial intelligence to inoculate your users against various attack vectors of social engineering. AIDA allows you to simulate a multi-faceted social engineering attack using email, phone, and SMS messaging (available for U.S. and Canada)

**“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

In the first quarter of 2018, after 7 years of helping our customers to enable their employees to make smarter security decisions and having reached the milestone of 15,000 customers, we decided to redo our initial 2014 analysis of average Phish-prone percentages and this time also break them out by industry and size.

Now having a massive database to analyze, the new research uncovered some surprising results. The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 27%. Fortunately, the data showed that this 27% can be brought down more than half to just 13% 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 2.17% on average.



**KnowBe4**  
Human error. Conquered.