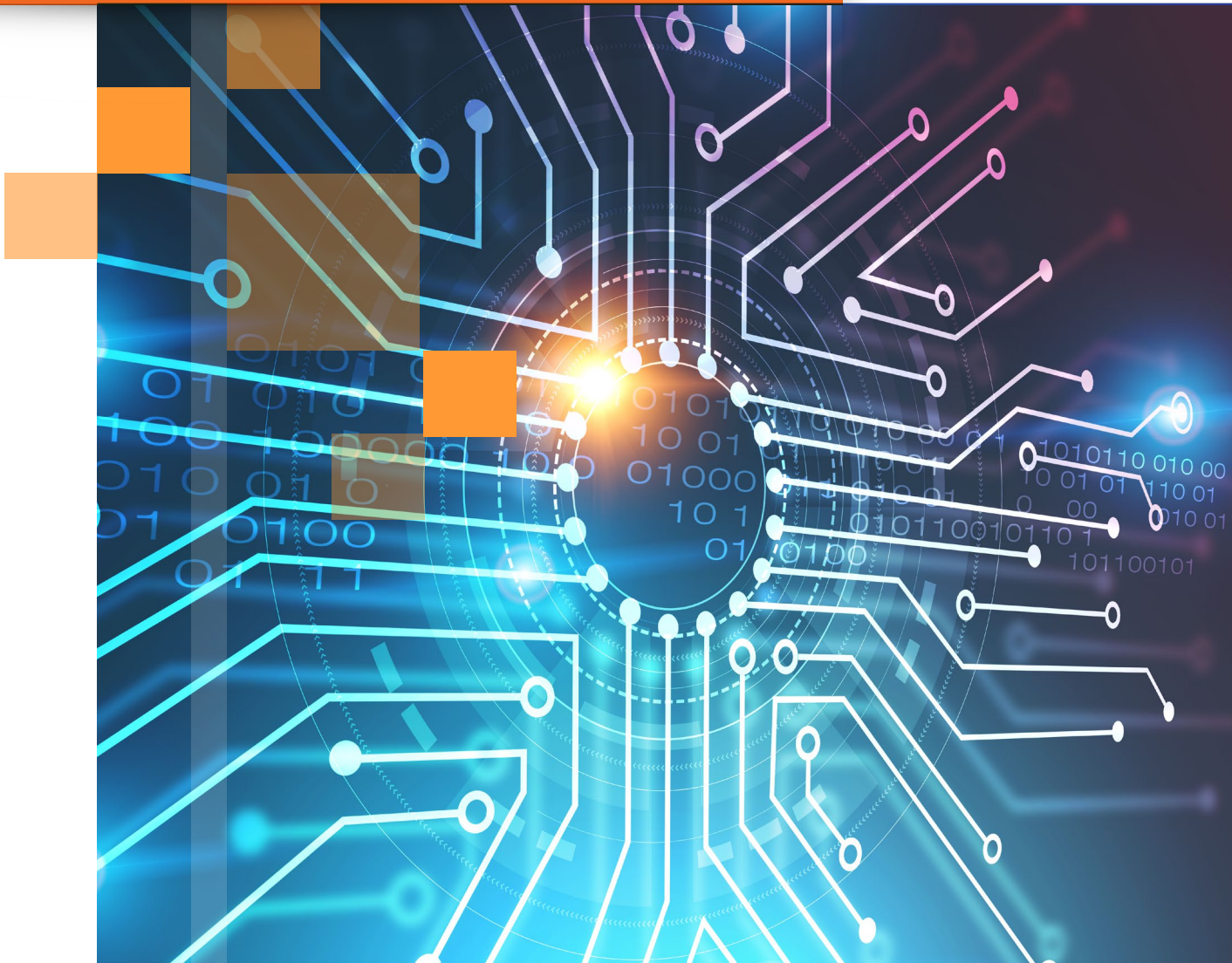


# Buyer's Guide

Security Awareness Training &  
Simulated Phishing Platform



## Table of Contents

<b>The Ongoing Problem of Social Engineering</b> .....	2
<b>The KnowBe4 Approach—Phish, Train, Analyze</b> .....	3
<b>The KnowBe4 Training Library and Simulated Phishing Content</b> .....	4
Training Library.....	4
Training Access Levels .....	7
Training Publishers.....	8
Simulated Phishing Content .....	9
Assessments.....	11
Multi-Language Support.....	12
<b>The KnowBe4 Console</b> .....	13
Automated Security Awareness Program (ASAP).....	13
Console Dashboard.....	14
Simulated Phishing Platform.....	15
Advanced Phishing Features.....	17
Training Platform.....	19
<b>SecurityCoach</b> .....	21
User Management.....	22
Reporting.....	23
Subscription Levels.....	26

KnowBe4 is the world's largest integrated platform for security awareness training and simulated phishing. In this guide you'll find:

- Why security awareness training is needed
- What the KnowBe4 platform offers
- Vital attributes to look for in any security awareness training vendor

## The Ongoing Problem of Social Engineering

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 cyber attacks 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 cyber attacks over the past five years.

Threat actors focusing on your employees means security awareness training is needed. Security awareness training is a form of education that seeks to equip members of an organization with the information they need to protect themselves and their organization's assets from loss or harm.

The goal of security awareness training is to arm your employees with the knowledge they need to combat these threats. Employees cannot be expected to know what threats exist or what to do about them on their own. They need to be taught what their employers consider risky or acceptable, what clues to look for that indicate threats, and how to respond when they see them.

“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



# The KnowBe4 Approach—Phish, Train, Analyze

KnowBe4 helps tens of thousands of customers to manage the ongoing problem of social engineering. With the world's largest library of security awareness training content, including interactive modules, videos, games, posters and newsletters, our mission is to enable your employees to make smarter security decisions, every day.

KnowBe4's competitive advantage is two-fold. First, using a variety of tools and information feeds, we give an organization a good snapshot of their current risk profile. This step, often skipped by competitors, is a necessary step to selecting the right defensive mitigations and efficiently decreasing risk. Second, KnowBe4's focus on local threat intelligence allows you to better focus on stopping the threats which are being specifically made, and succeeding, against your environment. Most security awareness training vendors focus primarily on using globally-collected phishing email statistics across all phishing email attempts and customers, and communicate the global trends as if they should be the ones, you too, should be most worried about. KnowBe4 reports on emerging global trends; but gives IT administrators the power to see how local phishing attempts and successes differ from those in the larger world and how to respond accordingly.

KnowBe4 uses a multi-pronged approach, which begins with understanding your organization's specific risk posture, and then allows you to leverage both the global pulse of the real-world phishing attempts, along with the ones that have made it past your specific defenses:

## Baseline Testing

We provide baseline testing to assess the Phish-prone™ Percentage of your users through a free simulated phishing attack.

## Train Your Users

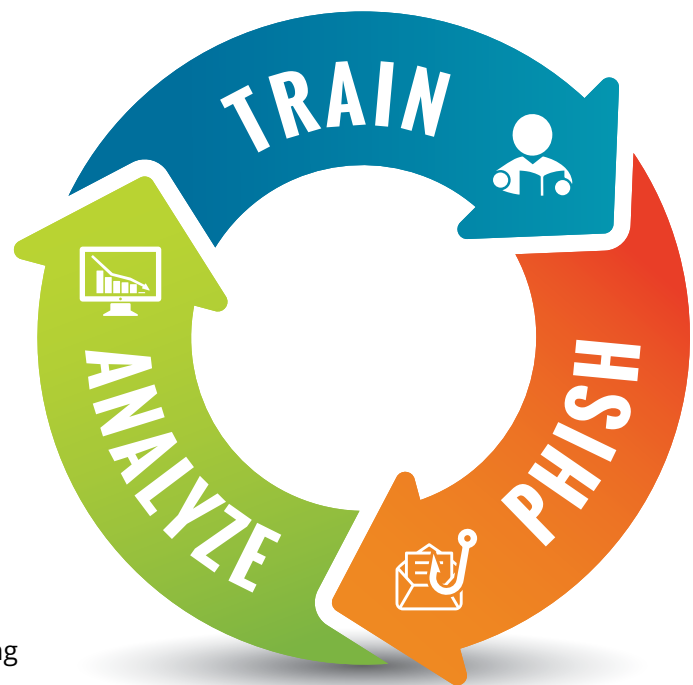
Take advantage of the world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

## Phish Your Users

Deploy best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

## See The Results

Explore enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management to show your successes and areas for improvement.



---

Continue reading this guide to explore our array of training content and the variety of features available in our training and simulated phishing platform.

# The KnowBe4 Training Library and Simulated Phishing Content

## Training Library

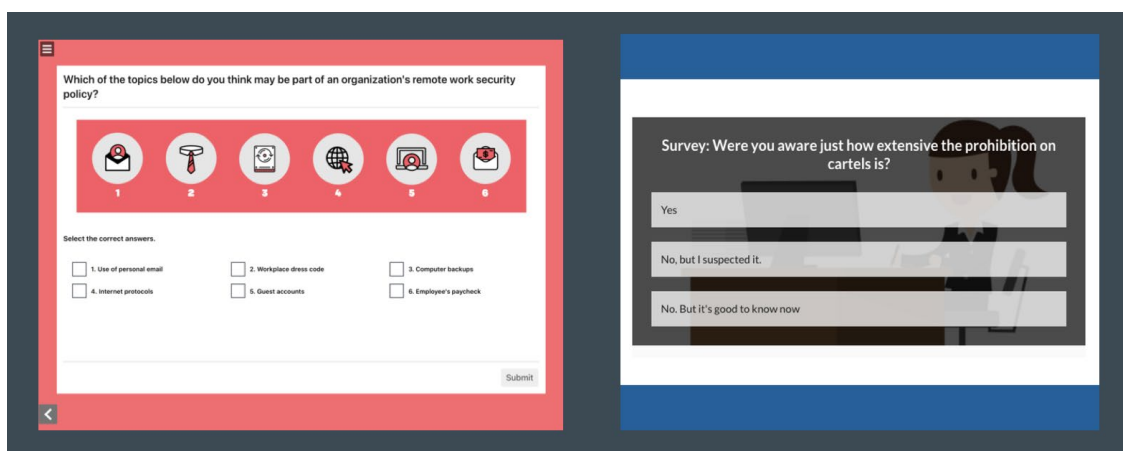
KnowBe4 offers the world's largest library of always-fresh security awareness training content that includes assessments, interactive training modules, videos, games, posters, and newsletters.

To easily deliver this content library to customers, KnowBe4 has a "ModStore." As a customer, you can use the ModStore to search, browse, and preview content and—depending on subscription level—add your chosen training content to your KnowBe4 account library.

Our partnerships with e-learning and security awareness content providers across the globe bring unique flavor and flair to the collection to ensure training campaigns stay current, relevant, and engaging for your users. The ModStore contains a wide variety of content on many different topics and content types.

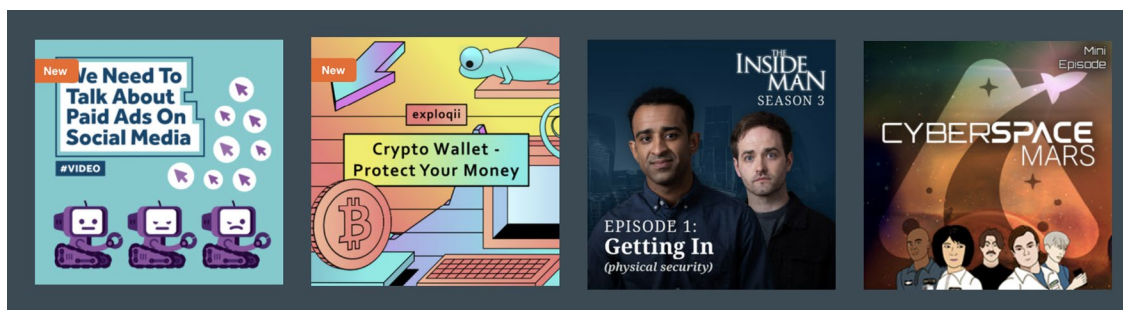
## Training Modules

Training Modules are interactive modules that cover a wide range of topics. Modules are SCORM-Compliant and can be downloaded for use with your own LMS. Hundreds of training modules are brandable.



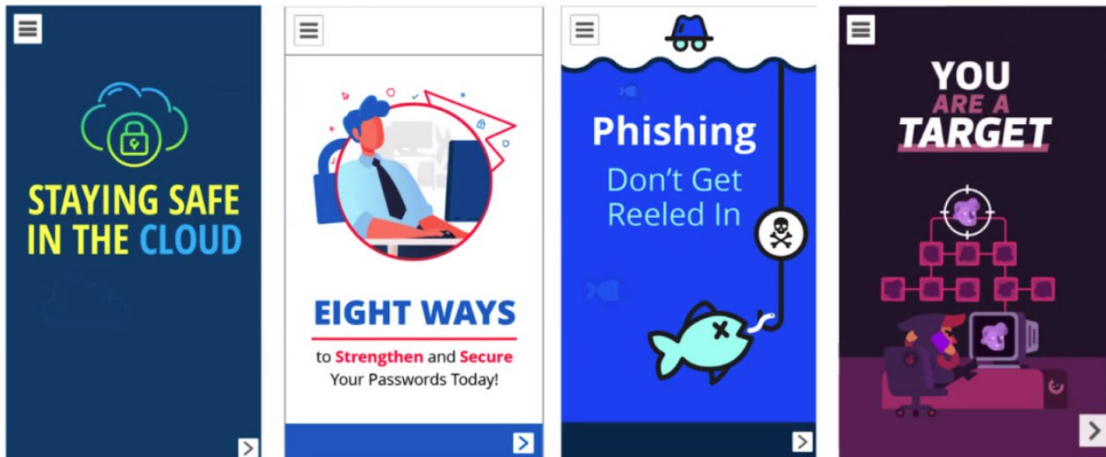
## Video Modules

Videos are MP4 files that can be watched in-browser or downloaded for use with your own LMS.



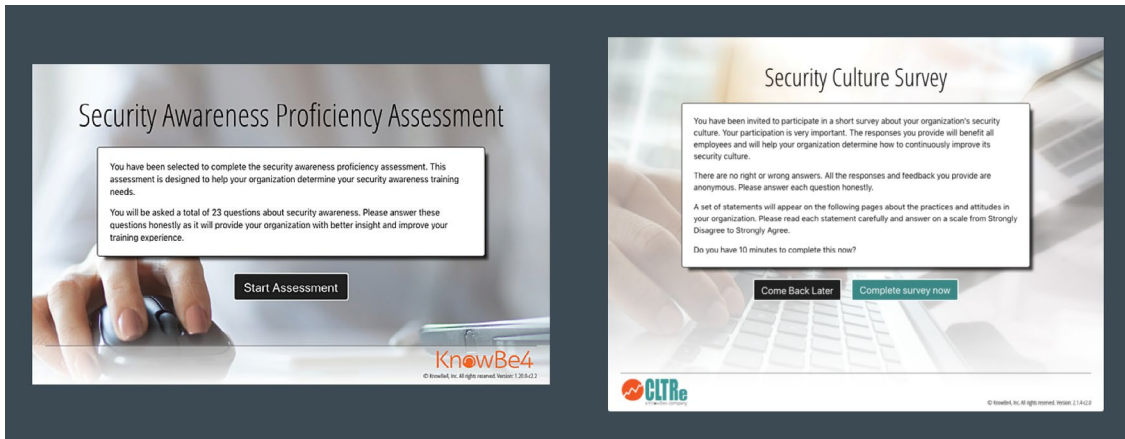
## Mobile-First Modules

Mobile-First Modules are optimized to be viewed and interacted with on a mobile device. These modules are no longer than five minutes and are designed to engage users; whether while they're on the go or located in low-bandwidth regions. Mobile-First Modules are brandable and SCORM-Compliant, so they can be downloaded for use with your own LMS.



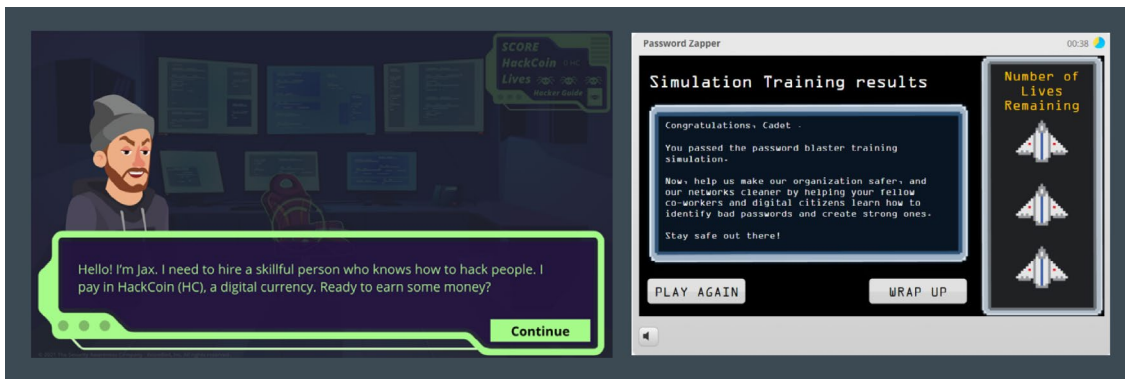
## Assessments

Assessments can provide a breakdown of your organization's strengths and weaknesses. You can use assessment results to create a more targeted security awareness training plan.



## Games

Games can reinforce the skills and information that your users are learning in a new and interesting way. Games are SCORM-Compliant and can be downloaded for use with your own LMS.



## Newsletters and Security Documents

Newsletters and security documents are PDF files that can be printed or shared digitally with your users. These documents cover a wide range of cybersecurity topics to help reinforce the skills your users learn from training.

The image displays three sample newsletters and security documents from KnowBe4:

- Left Document: Fraud Awareness & Prevention**
  - What Does Fraud Look Like?**
    - Identifying when someone is trying to defraud our organization is a vital part of our day-to-day responsibilities. Here are a few red flags that might indicate a fraud attempt:**
      - Large orders:** When a fraudster uses stolen payment methods, they will attempt to maximize spending in a single transaction before the victim realizes their information has been stolen.
      - Multiple transactions in a short period of time:** They could be a sign that someone gained unauthorized access to a customer's account or that someone is attempting to use a stolen credit card.
      - Fast shipping:** Most consumers choose affordable shipping options. Orders of overnight or priority shipments, especially those that involve high-priced orders.
      - Unusual shipping location:** Examples of unusual shipping locations include freight forwarders, virtual offices, self-storage facilities, and warehouses.
      - Multiple cards from a single address:** Transactions that use multiple payment methods, but ship to the same address, could indicate that a fraudster has a collection of stolen credit cards.
      - Large purchase of highly-targeted products:** If someone places a large order for highly-targeted products such as smart devices, tablets, and other electronics, it could be a sign that they are using stolen account credentials or credit cards.
  - How to Prevent Fraud**
    - Easy Alert:** Recognizing fraud attempts can be as simple as remaining vigilant and identifying red flags.
    - Use Common Sense:** If something seems off or out of the ordinary, think critically and follow your instincts.
    - Scrutinize All Requests For Sensitive Information:** Unauthorized access to confidential data makes fraud possible.
    - Report It Immediately:** When you suspect fraudulent activity, report it immediately so our organization can take appropriate measures to minimize damage.
    - Think Before You Click:** Fraudsters utilize phishing attacks to compromise passwords and steal data.
    - Ask Questions:** If you're unsure of something, please ask! Never make assumptions.
- Middle Document: No longer do we have to worry about fire breathing dragons and terrible curses cast by evil witches. Today we face a much scarier enemy, cyber threats.**
  - Dark Web:** Don't be your information and opt on the dark web. Yes, the dark web is real, and the content you find there is pretty scary.
  - Your Digital Footprint:** In a world where you share, where you share, and with whom you share, all your data can be used to build a profile of you and can be used against you in targeted attacks.
  - Remember and Don't Forget Authentication:** Make sure you are using secure passwords. Never make use of a password, think of the first few favorite song, all your numbers and characters. Include two-factor authentication and you're looking good!
  - Social Media:** Think with things going on. It's tempting to share everything about your life, but what you share can be used to someone else. Be careful not to overshare your personal info with anyone with the information they found on your profiles.
  - Social Engineering:** Criminals use your emotions against you to get what they want because hacking a human is so much easier than hacking a machine.
  - Mobile devices:** Be careful not to get careless without our mobile phones, making or walking targets for criminals. Do you know how to protect all the information contained on your device?
- Right Document: May 2021 Security Awareness Newsletter Hacking the Human**
  - Scavenger Hunt Fun for Your Employees:** Each month scavenger hunt questions are created to help you identify the topics covered in each newsletter. You can use the questions as they are or edit as you see fit.
  - Questions and Answers:**
    - What should you do if you click on a phishing link at work or on a work device? (Report it immediately)
    - Name three of the six principles of influence. (Reciprocity, Commitment, Social Proof, Liking, Authority, Scarcity)
    - If you click on a phishing link on a personal device, you should update these (passwords)
    - When scammers pose as executives and send emails to employees asking for money, it's known as this. (Business email compromise or BEC)
    - Social engineers use \_\_\_\_\_ tactics to convince people to click on links. (bait)
  - Additional Information:** Don't forget, the newsletter is available in 18 different languages. You can view the languages and download the version of your choice directly from the KnowBe4 Moodle.

## Posters and Artwork

Posters and artwork are high-quality images and PDFs that can be printed or shared digitally with your users. We encourage you to hang posters within your office or distribute them to your employees' home offices to act as a visual reminder to keep security in mind during everyday tasks.

The image displays three sample posters and artworks from KnowBe4:

- Left Poster: WHEN IN DOUBT CHECK IT OUT!**
  - Ask yourself these questions before you share any information.
  - Is the headline trying to elicit a strong emotional reaction?
  - Is the date current?
  - Is the author credible?
  - Are all the facts accurate?
  - Has the image been altered?
  - Is the source of the information legitimate?
  - Check sources and articles by using fact-checking websites before posting or forwarding any information.
- Middle Poster: YOU Just saved the day!**
  - You used the PAB! (The Phish Alert Button)
- Right Poster: PUMP UP YOUR PASSWORD STRENGTH**
  - The bad guys love weak passwords! Protect yourself and your organization with these best practices:
  - Don't share your password.
  - Change your password regularly.
  - Make passwords hard to guess.
  - Use a different password for each app and website.

# Training Access Levels

We offer three Training Access Levels: I, II, and III, depending on your subscription level. The security awareness training content in each level is carefully curated to build on the level before it, and each subscription provides varying levels of multi-language support and mobile-friendly content options. To see our entire continually-updated library in real time, sign up for the [KnowBe4 ModStore Training Preview!](#)

## Training Access Level I (Silver)

Training Access Level I provides you with the fundamental elements required to begin a security awareness training program. It's ideal for organizations that do not have security awareness training in place and want to start at least an annual training program. You get training and video modules, assessments, and educational reinforcements such as security documents and posters. We see many customers get started with Level I so their users get the basics of security awareness, including understanding what social engineering is, and then find they are ready to move to the next level of training content that takes a deeper dive into other cybersecurity topics. When annual training is no longer sufficient and you are ready to launch more frequent training campaigns, the Training Access Levels II and III set you on a path to develop a more robust and fully mature security awareness training program.

## Training Access Level II (Gold & Platinum)

The Training Access Level II library builds on Level I and expands to provide a greater variety in training content styles, formats, and topics. From animation, to live action, to self-paced learning, Level II unlocks the potential for you to offer more targeted training based on your users' roles, their location around the world, and your organization's industry. And, with an assortment of bite-sized training modules that are 5 minutes or less, it's easy to set up a more frequent cadence of training campaigns that keep your users engaged. More training more often can help drive behavior change with security awareness top of mind.

## Training Access Level III (Diamond)

Training Access Level III includes all the training content in Levels I and II, plus access to the most comprehensive library of security awareness training content, enhancing your organization's ability to deliver a fully mature awareness program on an ongoing basis. Level III includes multiple award-winning streaming-quality video series that tie scenes from each episode to key cybersecurity best practices, making learning how to make smarter security decisions via real-world applications fun and engaging. With a wide array of topics, formats, lengths, and styles from multiple content publishers, you have more content options to meet the unique needs of your users and align with your organization's corporate culture. With Level III, you can experiment with different styles and formats to different audience segments to maximize user engagement. This level also gives you the flexibility to mix things up to hone in on what content resonates best across different departments and regional locations. You can create shorter and more frequent training campaigns that make it easier to deploy your awareness program all year long. Keep your learners engaged with a consistent cadence of campaigns using a variety of content on security best practices. This mix of fresh content will build muscle memory over time without using the same training over and over again.



## Training Publishers

Learn a little bit about each of the publishers below and find the best mix to build your own mature multi-faceted security awareness training program.



### KnowBe4

Interactive security awareness training content developed by KnowBe4 and Kevin Mitnick shows real-world scenarios where Kevin, the world's most famous hacker, takes learners behind the scenes to see how cybercriminals do what they do. KnowBe4 training content includes the right mix of graphics and text to keep learners engaged and absorbing information. Training modules and videos include actionable tips and hints, memorable characters, and impactful storylines.



### The Security Awareness Company (SAC)

SAC offers diverse, foundational training jam packed with information. The content is thoughtfully designed to maximize comprehension, retention and behavior change with a well-rounded course lineup that also features knowledge checks, course interactions, quizzes, games, documents, and monthly newsletters.



### Popcorn Training

Everyone loves a good story! This training engages emotions, triggers imagination, and motivates learners to take action. Colorful animations, live action video clips and quizzes help reinforce learning and come with complementing security documents and posters to reinforce key messages.



### Exploqii

Security awareness training simplified. Quick, bite-sized training videos presented in lively colorful animations. This content is focused on delivering a message that's easy to digest and retain.



### Twist & Shout

Edutainment sprinkled with humor that's sure to be an instant hit. These TV-series-inspired videos bring it all together in a way that makes training personable, relatable, real, and enjoyable.



### El Pescador

Colorful animations bring training to life! Adventures with the memorable Captain El Pescador will have learners tuned in to sound advice for security awareness with a variety of training modules, videos, posters, and documents.



### CLTRe

CLTRe's Security Culture Survey provides an effective and easy-to-use method to assess the current state of your security culture and track its changes over time. The Security Culture Survey uses proven social scientific methods and principles to provide reliable, evidence-based results that enable organizations to assess, build and improve their security culture.



### Saya University

Saya University's microlearning modules are originally scripted and produced to represent the actual voices and social economic and threat landscape in Japan to ensure every person is empowered with information to guard against the global threats of cybersecurity.



### MediaPRO

Interactive modules and short videos ensure lessons are engaging and information is retained and cover such topics as data privacy regulations, corporate compliance and preventing sexual harassment.

## Compliance Plus

### Compliance Plus Training

*(Available as an add-on to any subscription level)*

KnowBe4's Compliance Plus training is interactive, relevant, and engaging with real-life simulated scenarios to help teach your users how to respond in a challenging situation. The content addresses difficult topics such as sexual harassment, diversity and inclusion, discrimination, and business ethics. The Compliance Plus library includes various types of media formats and reinforcement materials to support your compliance training program.

## Simulated Phishing Content

Our extensive library of templates allows you to use the KnowBe4 platform for "turnkey phishing." You can be up and running in less than 30 minutes.

### Email Templates

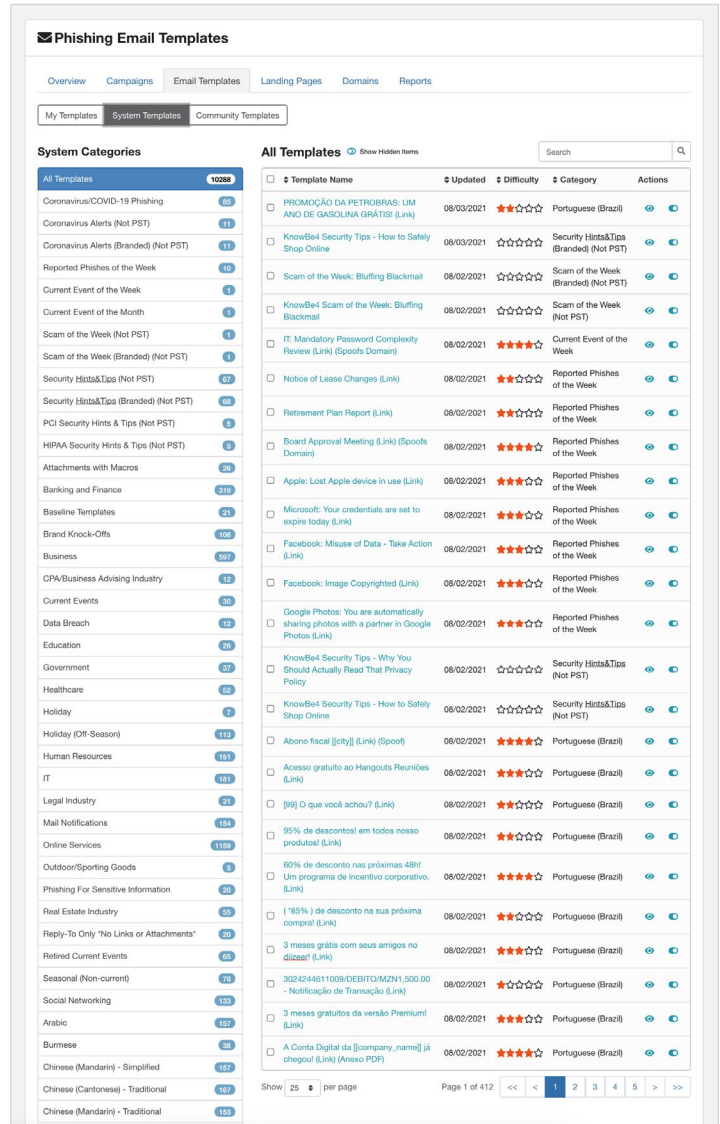
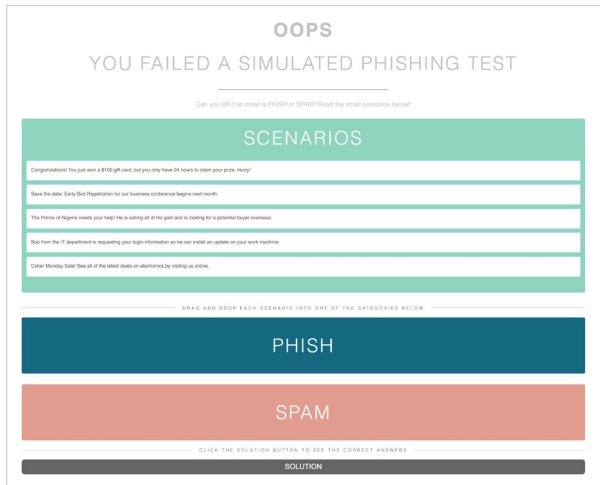
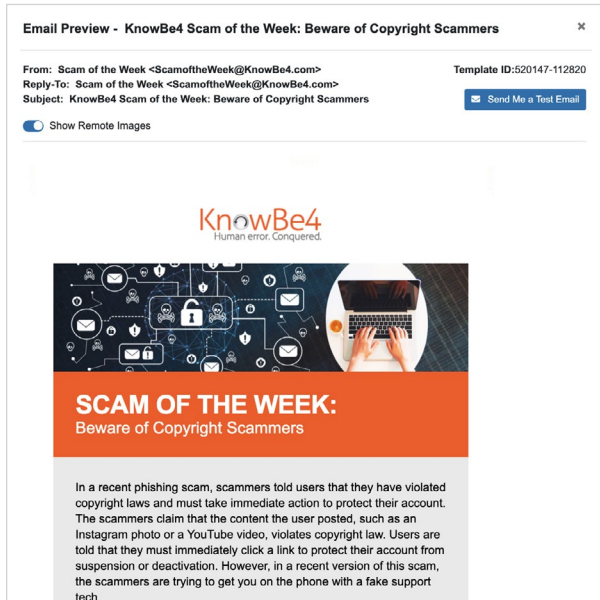
Our library of multi-language templates includes emails in 30+ categories and include: Banking and Finance, Social Media, IT, Government, Online Services, Current Events, Healthcare, and many more. You also have access to a community section where you can swap templates with thousands of other KnowBe4 customers.

### Landing Page Templates

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. Choosing from 200+ landing pages, you have the ability to influence your users' reaction to a phishing test. There are three options for setting which landing page your users will see when they fail your phishing tests. With support for mobile-friendly pages, you can 1) customize your default landing page, 2) choose a campaign-specific landing page, or 3) set a template-specific landing page.

# Newsletters

As part of KnowBe4's phishing template categories, you have access to "Scam of the Week" and "Security Hints & Tips" newsletters to keep your users informed on the latest phishing scams and help reinforce basic security tips. You can use these newsletters as part of a weekly, bi-weekly, or monthly campaign when you set up a phishing campaign in the KnowBe4 console.



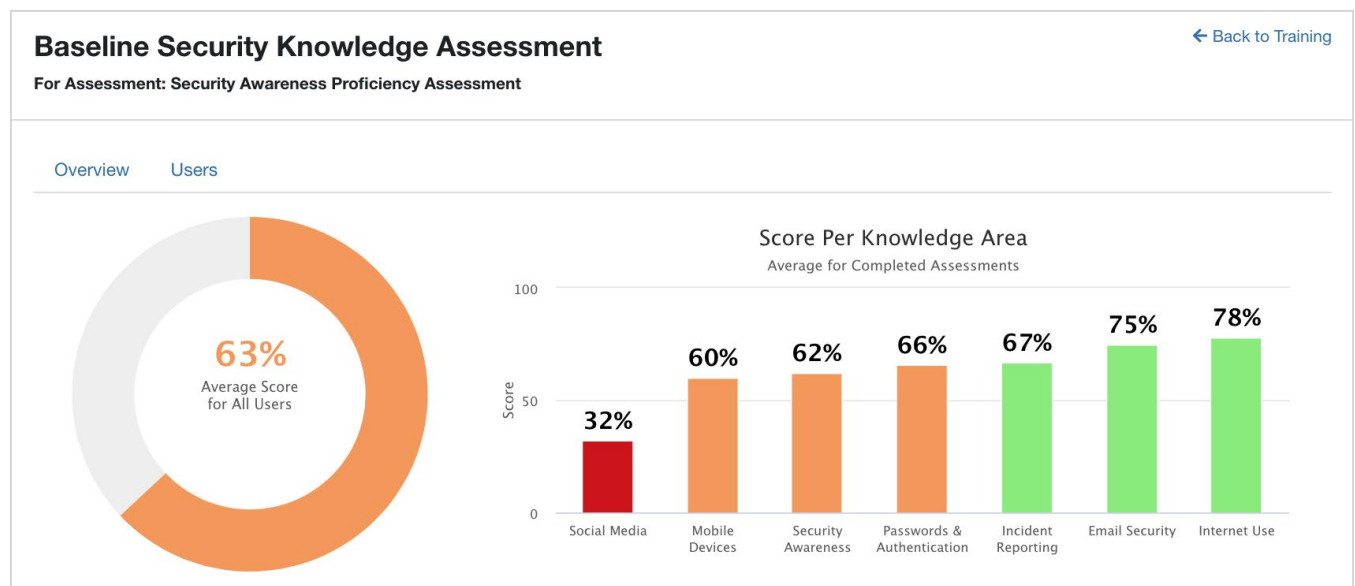
# Assessments

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 assessments, built into the KnowBe4 platform and included at no additional cost, help you identify users who are both aware of the most secure action to take in risky situations and know how to follow through. This knowledge helps you set a baseline for the security culture you're trying to achieve in your organization and track the success of your training efforts.

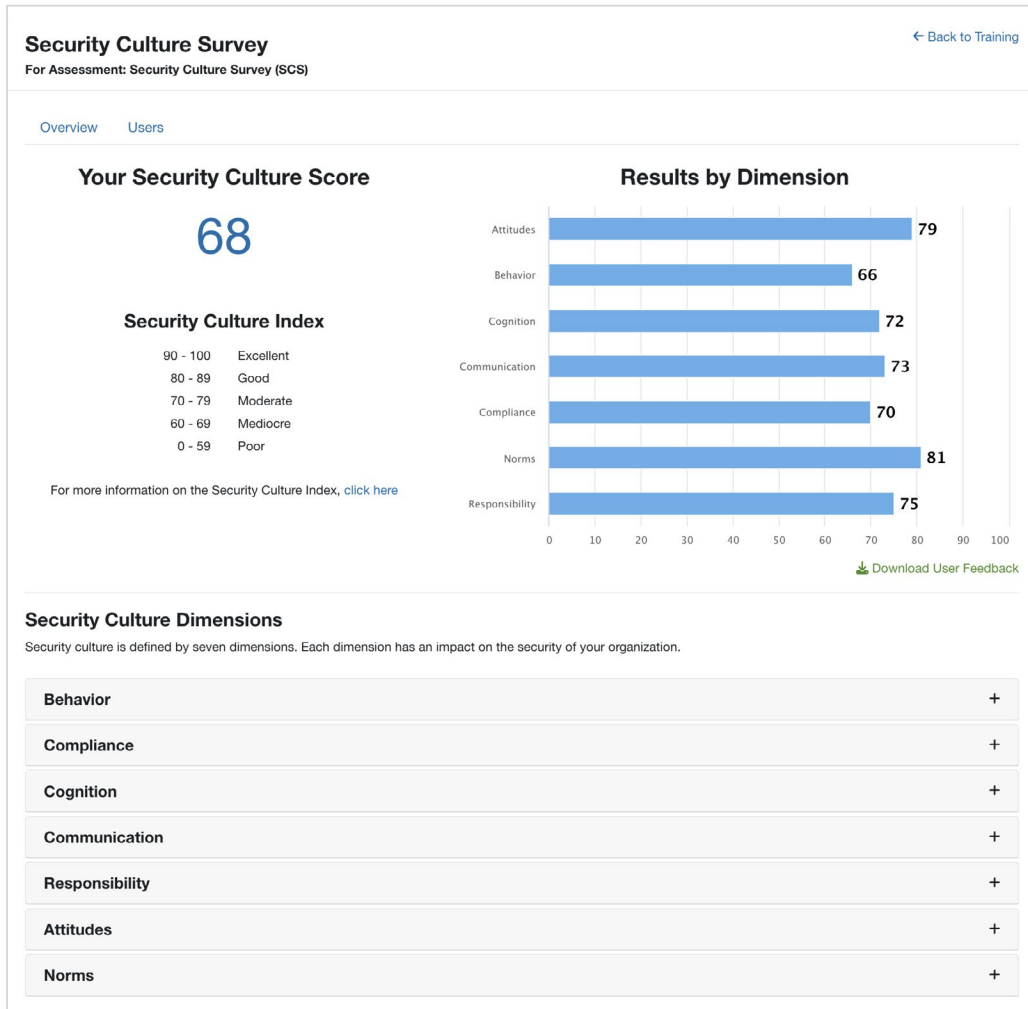
## Security Awareness Proficiency Assessment (SAPA)

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 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 shows you the overall effectiveness of your security culture program and how your security culture improves over time.



Both SAPA and SCS are rooted 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.

## Multi-Language Support

Localized learner interface and end-to-end translated content for phishing and training campaigns is available in 35 core languages for global coverage of your learners. The localized Admin Console is available in 10 languages.

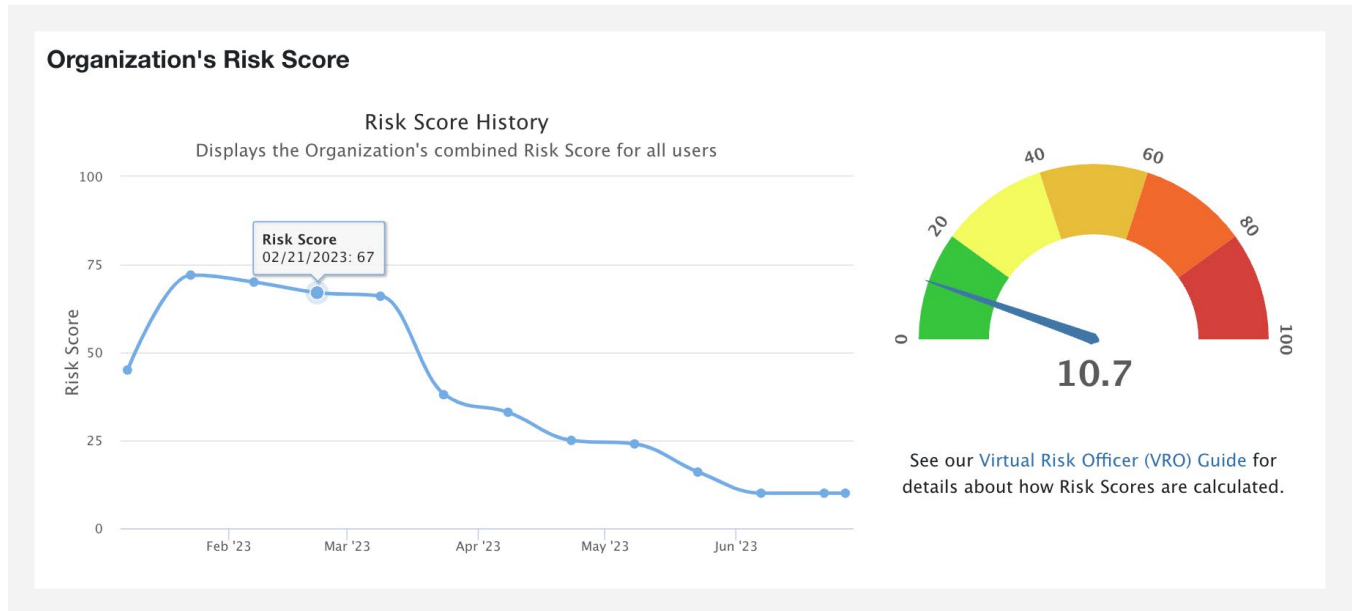


# Console Dashboard

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

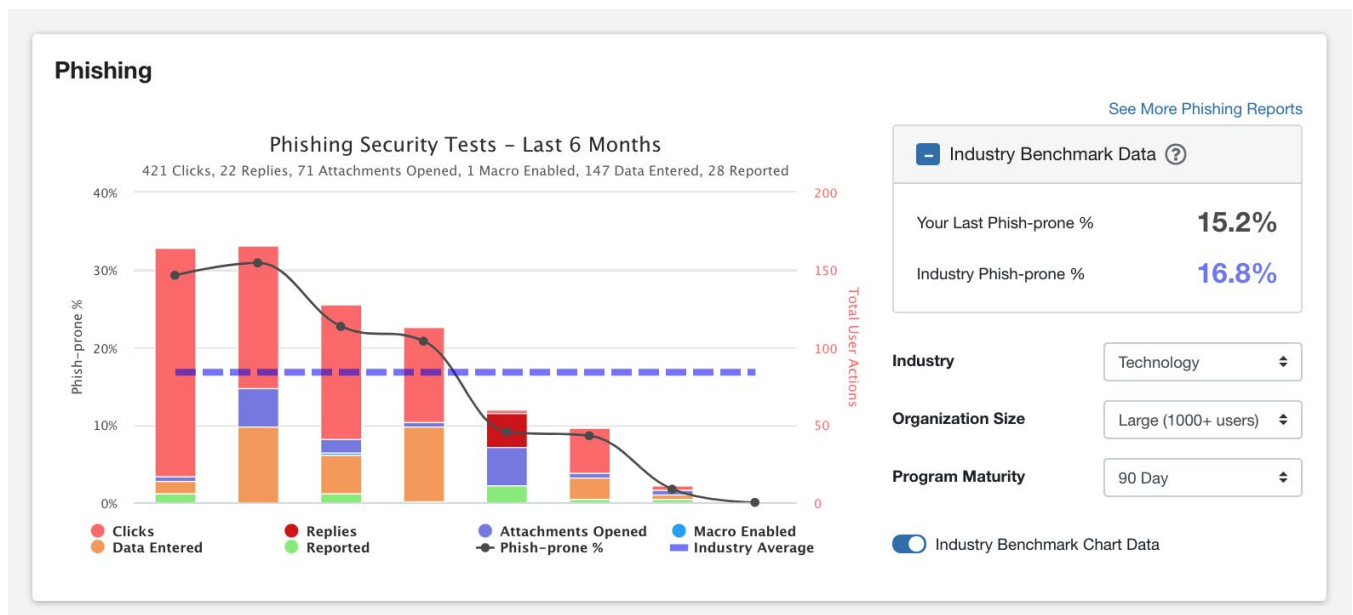
## View Organization Risk Score

View your organization's overall risk score based on the combined risk scores across all your users.



## Phish-Prone Percentage Results

Our platform offers different ways to gauge your end-users progress across similar industries based on phishing and assessment results. This dashboard feature lets you see your organization's Phish-prone Percentage (or how many users are likely to click on a phishing email) benchmarked against peers in your industry.



# Simulated Phishing Platform

KnowBe4 offers a new-school approach to training users on the threat of phishing by allowing you to create phishing campaigns that send your users simulated phishing emails. These simulated attacks mimic actual phishing attacks and teach users how to stay alert.

KnowBe4 customers can schedule and send an unlimited number of simulated Phishing Security Tests (PSTs) to your users during the subscription period. Read on to learn more about our phishing platform's most popular features.

## Phishing Campaigns

The KnowBe4 platform is designed to help you determine what types of attacks your users are vulnerable to, educate users on how to look for red flags, and calculate your organization's Phish-prone Percentage. To get started with your training program, creating your phishing campaigns is the first step to testing your users so you can determine what training your users need to be enrolled in.

## Phishing Test Scheduling

You can schedule phishing tests from our large library of more than 25,000 templates available in 40+ languages or choose from the community templates section, which were created by admins for admins to share with their peers. Choose

from one-shot, weekly, bi-weekly or monthly simulated phishing attacks and immediately see which employees fall for these social engineering attacks. And, with KnowBe4's unique "anti-prairie dog" feature, you can send random phishing templates at random times throughout a phishing campaign, mimicking real life phishing attacks preventing users from giving each other notice of a phishing test.

**New Phishing Campaign** ← Back to Campaigns

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

Campaign Name: Q1 SAT Training Campaign

Send to: All Users | Specific Groups

Frequency: One-time | Weekly | Biweekly | Monthly | Quarterly

Start Time: 08/03/2021 6:35 PM (GMT-05:00 Eastern Time (US & Canada))

Sending Period:  Send all emails when the campaign starts  Send emails over 3 business days

Define Business Days and Hours: Using Time Zone: (GMT-05:00) 9:00 AM to 5:00 PM.  Sun  Mon  Tues  Wed  Thur  Fri  Sat

Track Activity: 3 days after the last email is sent

Template Categories: All Ratings | Full Random (Random email to each user)

Difficulty Rating: All Ratings

Phish Link Domain: Random Domain

Landing Page: Default Landing Pages

Add Clickers to: Select Group

Send an email report to account admins after each phishing test

Hide from Reports

**Create Campaign**

**WebFaxOnline: Your Customer Sent A Fax (Link)** ← Back to Phishing Email Templates

This is a system template. By saving it, it will be added to your templates list.

Template Name: WebFaxOnline: Your Customer Sent A Fax (Link)

Sender's Email Address: FaxMessage@web.ofaxOnlines.com | Sender's Name: WebFaxOnline | Reply-To Email Address: FaxMessage@web.ofaxOnlines.com | Reply-To Name: WebFaxOnline

Subject: Your Customer has sent an ofax message - 4 Pages

Attachment File Name: | Attachment Type: Select Option

WebFaxBusiness logo and text: "World Leader in Digital Phishing"

Fax Message [Caller-ID: [random\_number\_3]]-[random\_number\_3]-[random\_number\_4]]  
You have received a 4 pages fax.

\* The reference number for this fax is [AT-41-9992466036c](#).

View this fax using your PDF reader.

[Click here to view the message](#)

Please visit [www.webfaxbusiness.com/ofax/faq/faq.html](#) if you have any questions regarding this message or our service. Thank you for using our ofax service!

Landing Page: Default Landing Page | Landing Domain: Default (secured-login.net)

Difficulty Rating: ★★★★★ Moderate

**Save**

## Phishing Template Customization

You can customize any system template as well as include simulated attachments and macros. You have the ability to create custom phishing email templates from scratch or by changing our existing templates to send to your users. You can go even further and customize scenarios based on public and/or personal information, creating targeted spear phishing campaigns, which replace fields with personalized data.

With the ability to use logos in phishing emails, you can create legitimate looking email templates with our platform, through the use of embedded links in the email pointing back to the original URL address of the logo. This way the owner of the logo is still hosting the image and owns the rights to it.



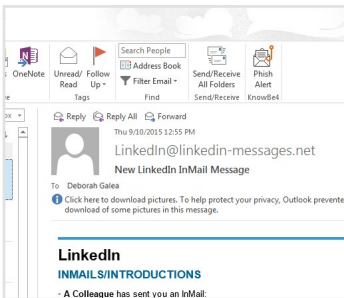
## Phish Alert Button

With just 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. The Phish Alert Button (PAB) for Microsoft 365 allows you to add languages to your PAB instance to automatically display the preferred language based on your users' system language setting.

- 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 2016, 2019, 2021 & Outlook for Microsoft 365, Exchange 2016, 2019 & 2021, Outlook on the web (Outlook.com), the Outlook Mobile App (iOS and Android), Chrome 80 and later (Linux, OS X, and Windows), Gmail accounts connected through Google Workspace, Gmail Add-on is compatible with Gmail in browser and mobile clients.

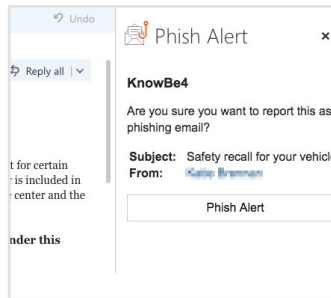
### Outlook Toolbar

Adds a Phish Alert Button for your users



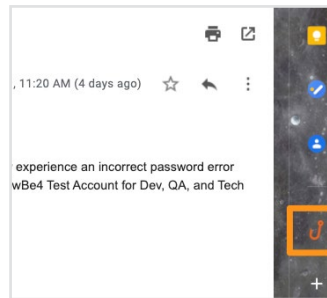
### Microsoft 365 Add-in Pane

Adds a Phish Alert Button for your users



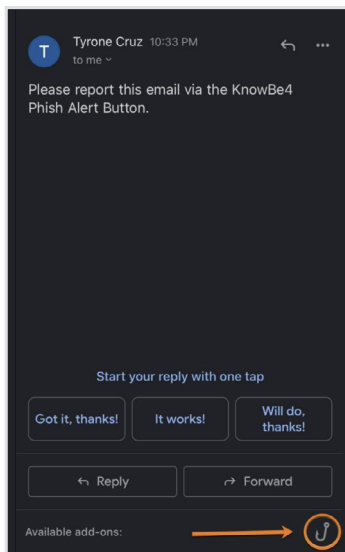
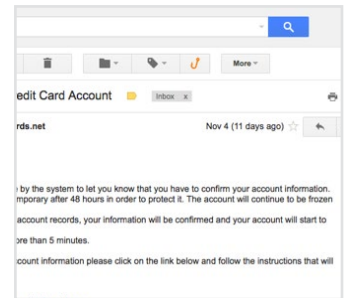
### Gmail Add-On

Adds a Phish Alert Button for your users

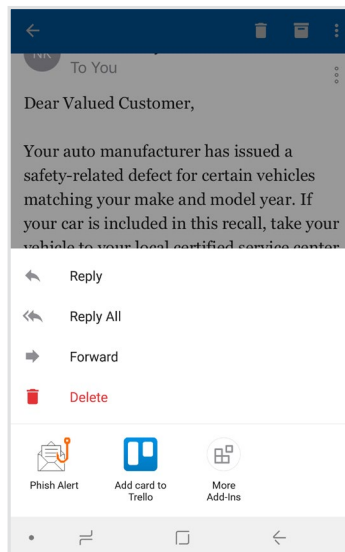


### Gmail Extension

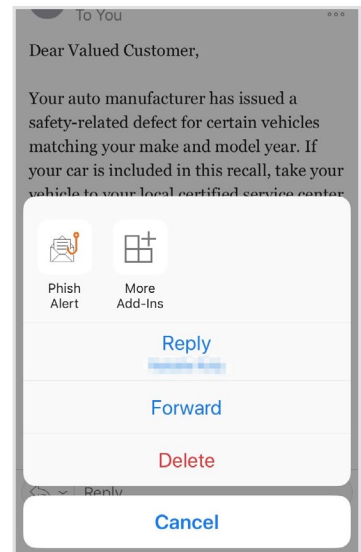
Adds a Phish Alert Button for your users



Gmail Mobile (Android)



Outlook Mobile (Android)



Outlook Mobile (iOS)

## 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 console. We make available a category of system simulated phishing templates called "Reply-To Online" that are specifically designed to test whether users will interact with the bad actors on the other end. However, the Phishing Reply Tracking also works with any of our phishing templates.

538	100%	6.1%	0.4%	4.1%	4.6%	0%	0%	0%	2%	0%
Recipients	Delivered	Opened	Clicked	Replied	Attachment Opened	Macro Enabled	Data Entered	Vulnerable Plugins	Reported	Bounced

[Download CSV](#)

Name and Email	Date and Time	
Aaron Anderson admin@kb4-demo.com	07/29/2020 2:59 AM	<a href="#">↩</a> <a href="#">🗑</a> <a href="#">✉</a>

Phishing Reply Tracking is simple to use and on by default for new phishing campaigns via the "Track replies to phishing emails" option.

## 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. With unlimited domain spoofing, we allow you to spoof any email address when doing simulated phishing campaigns.

## Advanced Phishing Features


Select subscription levels include additional ways to get the most out of our phishing platform. Read on for more on these features.

## Social Engineering Indicators

Our Social Engineering Indicators (SEI) feature is 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 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.



Oops!  
You clicked on a simulated phishing test!

Remember these three rules to stay safe online:

- 01**  
Always stop, look, and think before you click!
- 02**  
Check for red flags that indicate a phishing attack is happening.
- 03**  
Verify suspicious emails with the sender through a different medium.

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:

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

## USB Drive Test

You can easily create your USB Drive Test from the KnowBe4 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 failure 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 console.

## QR Code Phishing

You can test your users with QR codes instead of phishing links or attachments in emails. QR codes, or quick response codes, are scannable barcodes that contain data in a compact format. If your users scan a malicious barcode, they could be prompted to visit a dangerous website. Additionally, malicious links hidden in QR codes may be able to bypass your organization’s security filters.

Physical QR code phishing campaigns allow you to test how your users will react to finding an unexpected QR code. For example, if your users see a QR code on a poster in a familiar location, they may scan it and open the link without verifying that the link is secure. QR code Phishing Security Tests can help prepare your users for real QR code phishing attacks.

## AI-Driven Phishing

AI-Driven Phishing enables you to leverage the power of AI to automatically choose the best phishing template for each of your users based on their individual training and phishing history. Using data from KnowBe4’s AIDA (Artificial Intelligence Driven Agent), a recommendation engine enables you to automate the dynamic selection of unique phishing security test templates for your users.

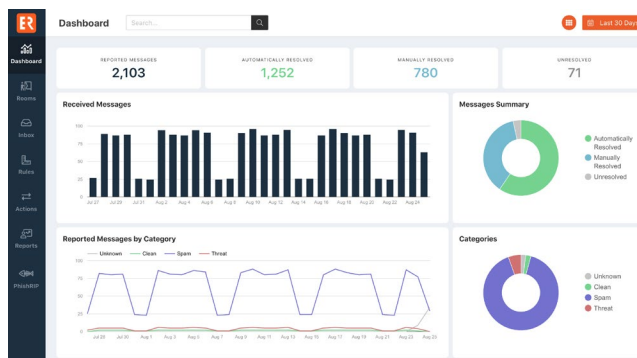
Think of it as your own AI phishing assistant that automatically chooses the best phishing test for each user, at that moment. When you use AI-Driven Phishing, you essentially create a unique phishing campaign for each of your users to make sure every user receives simulated phishing tests personalized to their individual level. Give your users a more personalized experience that adapts to their current level of knowledge.

## Callback Phishing

As an admin, you can use the new Callback Phishing feature in your KnowBe4 console and run a simulated callback phishing campaign to see if your employees would fall for this trick. An email lands in their inbox, with a phone number and a code. If they dial that number, they’ll be asked for the code. But here’s the catch—enter the code, that’s the first failure point, give up personal or sensitive info, that’s a double whammy.

## PhishER Plus

PhishER Plus is available as a product add-on option to any subscription level, and is a simple and easy-to-use web-based platform that helps your InfoSec and Security Operations team cut through the inbox noise and respond to the most dangerous threats more quickly. PhishER Plus was developed to help you supercharge your organization’s email security defenses and is an additional final layer after your existing SEG and other cybersecurity layers fail. PhishER Plus enables a critical workstream to help your IR teams work together to mitigate the phishing threat and is suited for any organization that wants to automatically prioritize and manage potentially malicious messages—accurately and fast! When you combine KnowBe4 and PhishER Plus as part of your email security workstream, you not only can reduce the burden on your Infosec and IR teams while identifying true threats more quickly, you can also take your security awareness training program to a whole new level.



## Key benefits of PhishER Plus include:

- Free up incident response resources to identify and manage the 90% of messages that are either spam or legitimate email
- See clusters or groups of messages based on patterns that can help you identify a widespread phishing attack against your organization
- Global Blocklist entries of validated threats crowdsourced from 10+ million trained users are leveraged to automatically block matching new incoming messages from reaching your users' inboxes. This continually updated threat feed is managed by KnowBe4 and syncs with your Microsoft 365 mail server.
- PhishML™ is a PhishER Plus machine-learning module that analyzes every message coming into the PhishER Plus platform and gives you info to make your prioritization process easier, faster, and more accurate
- Global PhishRIP is an email quarantine feature that integrates with Microsoft 365 and Google Workspace so your incident response team can quickly and easily remediate. Messages that match an identified phishing threat other PhishER Plus customers have “ripped” from their organization’s mailboxes are then validated by the KnowBe4 Threat Research Lab.
- PhishFlip™ is a PhishER Plus feature that automatically turns user-reported phishing attacks targeted at your organization into safe simulated phishing campaigns

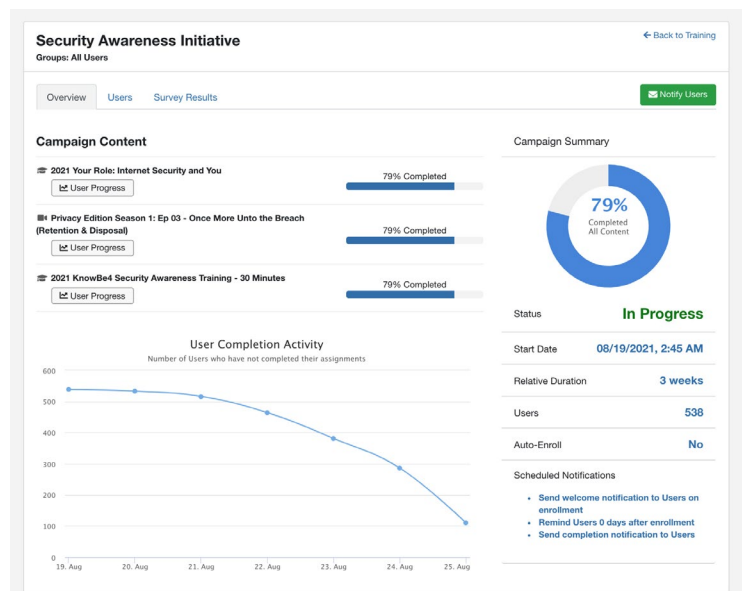
## Training Platform

### Training Campaigns

In the KnowBe4 console you can quickly create ongoing or time-limited campaigns, select training modules by user groups, auto-enroll new users, and automate “nudge” emails to your users who have not completed training. You can also edit training notification templates, prepare policies for user acknowledgment, and view training reports. Training campaigns are used to customize and manage your users’ training content within our learner experience.

### Learning Management System Options

With KnowBe4’s robust learning management system (LMS), you can upload your own SCORM-compliant training and video content in any language you choose and manage it alongside your KnowBe4 ModStore Training content all in one place—at no extra cost!



ModStore Browse Library Brandable Content Uploaded Content

Add New Content

Content Title

Description

Expected Duration (Minutes)

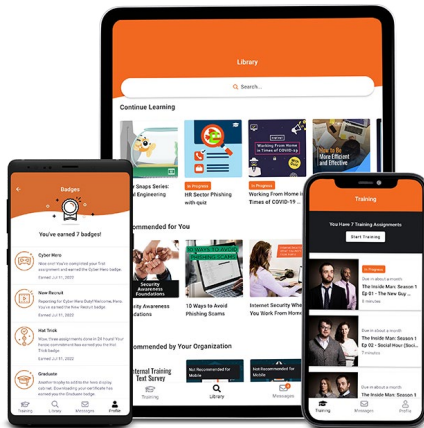
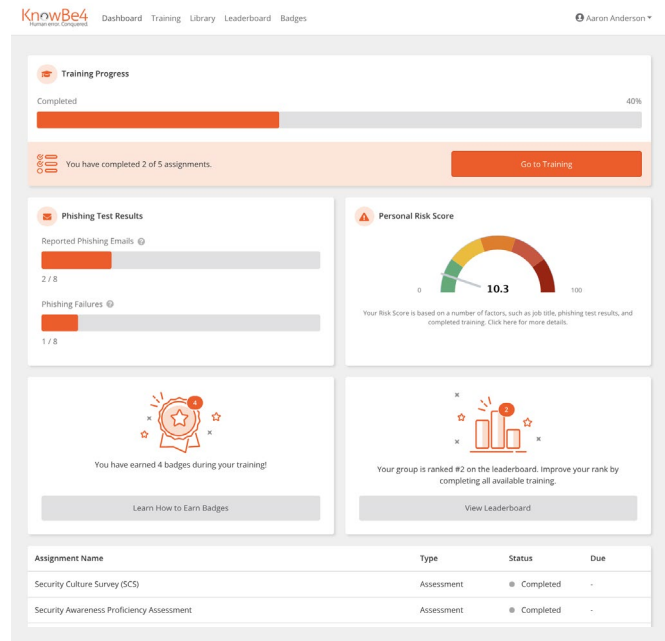
Artwork  No file chosen

## Learner Experience

KnowBe4's learner experience (LX) adds customization ability and engaging and fun gamification to your security awareness training plan.

Your users can compete against their peers on leaderboards and earn badges while learning how to keep themselves and your organization safe from cyber attacks. An informative, optional tour is also provided to show your users around and make them feel comfortable with their new learning environment.

The LX interface also includes a Learner Dashboard. Here your users will see a summary of their training completion including the training status and due dates. Optionally, you can choose to show your users' Phishing Test Results, Personal Risk Score, and gamification statistics.



## KnowBe4 Learner App

The KnowBe4 Learner App enables your users to complete their assigned training conveniently from their tablets, smartphones and other mobile devices. Broaden the protection of your largest attack surface and cover employees that don't typically have access to a desktop or laptop device with an app designed with both the user and admin in mind.

The KnowBe4 Learner App is included with your training subscription at no extra cost and provides your users with the flexibility and convenience of 24/7 learning. The app, available for iOS and Android, supports push notifications for custom announcements, updates on assigned training as well as KnowBe4 newsletters.

## Brandable Content

The brandable content feature allows you to create a branded theme and apply it to active training campaigns with eligible content. Use the Brandable Content tab to set your brand color, upload a company logo, and add an introduction and final page. These optional pages include your company logo, custom text, and an image of your choice.

Use this feature to provide a familiar look and feel for your employees. You also have the ability to upload your organization's Branded Certificates into the KnowBe4 platform. The customized certificates of completion can be made available at the end of each training module for your users.

The 'Create Theme' interface in ModStore includes the following sections:

- Theme Settings:** Includes a 'Theme Name' field with the value 'New Content Theme (kb4-demo.com) - 25 Aug 2021, 17:02:44' and a 'Brand Color' field with the value '#f26721'. A warning message states: 'The color you have selected may be difficult for some users to read. We recommend that you select another color to help distinguish the text from the background.'
- Company Logo:** A field for 'Company Logo (200px x 100px) \*' with a 'Browse' button.
- Optional Pages:** Checkboxes for 'Introduction Page (Optional)' and 'Final Page (Optional)', both of which are checked.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom.

## Content Manager

With Content Manager you can customize your training content preferences effortlessly. Adjust passing scores, infuse branded themes, allow test-outs and say goodbye to content skipping. And here's the kicker—it's available across all subscription levels.

## AI-Recommended Training

The KnowBe4 ModStore leverages machine learning to offer informed training suggestions based on your users' performance metrics from your phishing security test campaigns. Personalized to your overall organization's Phish-prone Percentage, the ModStore will present recommended training modules you can select to help reduce your users' click rates over time.

## Optional Learning for Users

Optional Learning enables you to offer your users additional training content from your KnowBe4 ModStore. Simply create specific training campaigns with the optional training content you would like to make available for your users to self-select. You can also leverage the advanced AI-Recommended Optional Learning feature, available to Diamond customers, to recommend and deploy additional training content to your users based on their previous course completions without the need to create a separate training campaign.

# SecurityCoach

**SecurityCoach** is the first real-time security coaching product created to help IT and Security Operations teams further protect your organization's largest attack surface — your employees. Introducing a new category of technology called Human Detection and Response (HDR), SecurityCoach helps strengthen your security culture by enabling real-time coaching of your users in response to their risky security behavior.

SecurityCoach integrates with KnowBe4's new-school security awareness training platform and your existing security stack to deliver immediate feedback to your users at the moment risky behavior occurs. SecurityCoach is an optional add-on for KnowBe4 customers with a Platinum or Diamond level security awareness training subscription. SecurityCoach uses standard APIs to quickly and easily integrate your organization's existing security products with your KnowBe4 console. Your security stack generates alerts that are then analyzed by SecurityCoach to identify events related to any risky security behavior from your users.

### Key Benefits of SecurityCoach include:

- Reinforce user comprehension and retention of security training and established security policies with real-time coaching on real-world behavior
- Leverage your existing security stack to deliver real-time coaching to your risky users and gain additional value from your existing investments
- Build custom campaigns for high-risk users or roles that are considered a valuable target for cybercriminals or that keep repeating risky behaviors
- Track and report on improved real-world security behavior across your organization, providing justification for continued investment
- Measurably reduce risk while building a mature security culture in less time
- Reduce the burden on your SOC and improve efficacy by decreasing alert noise caused by repetitive risky security behaviors

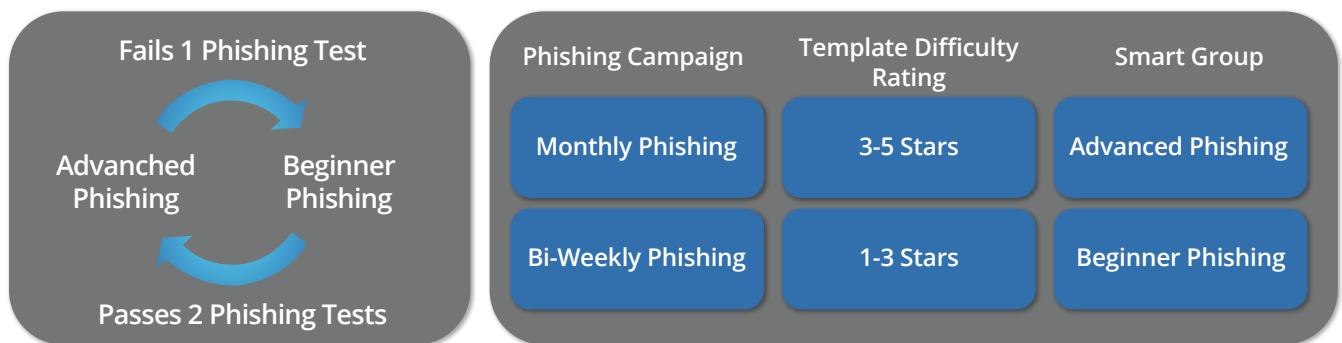
# User Management

## User Provisioning via Active Directory or SCIM Integration

KnowBe4 makes user management easy using Active Directory Integration (ADI) or SCIM Integration for identity providers such as Microsoft Entra ID, Okta or OneLogin. Both ADI and SCIM integration allow you to upload or sync user data to your KnowBe4 console and save you time by eliminating the need to manually manage user changes.

## Smart Groups

Put phishing, training and reporting on autopilot with Smart Groups. Automate the path your employees take to smarter security decisions. Our Smart Groups feature, available to Platinum and Diamond customers, allows you to deliver dynamic phishing campaigns by creating groups based on criteria you choose. Users are dynamically added and removed from Smart Groups based on these criteria. Campaigns are considered dynamic because your users are tested more or less often, as necessary, depending on their performance in phishing campaigns. We recommend using this feature for phishing tests, training campaigns, and generating unique reports. With the powerful Smart Groups feature, you can use each employee's 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.

## 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

# Reporting

KnowBe4's security awareness training platform offers a wide range of reports that give insight into the effectiveness of your security awareness training program. Each available report in your console can be downloaded as either a CSV or PDF file, depending on the type of report. Learn more about the various report categories and types [here](#).

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. You can even save reports to be viewed at a later time or send saved reports to other users. You can also choose to schedule reports to be generated and sent at a set frequency, such as every quarter. 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.

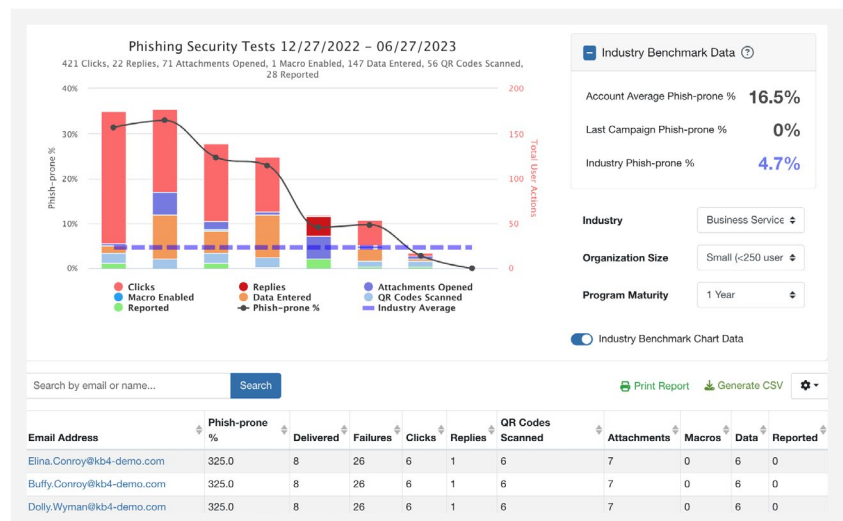
The **Dashboard** of your console contains your Organization's Risk Score and Phishing reports. These reports provide general information about your organization's Phish-prone Percentage at the time of the phishing campaign and your users' actions during the campaigns. You can hover over the points in the table to get more details on specific phishing campaigns, how many users each test was sent to, and your users' actions.

Read on for more details about the variety of reporting features available.

## Phishing Reports

The Phishing Reports section of the KnowBe4 console gives you access to reports that are useful for totaling user actions on multiple campaigns (for example, how many times did each user click on a phishing link?).

Your report can be filtered by specific date range, certain campaigns, and campaigns sent to certain users. You can also compare failures, reported phishing emails (emails reported using the Phish Alert Button), or compare results by groups.



## Training Reports

The Training Reports section of the KnowBe4 console gives you access to reports that show which users have logged in at least once and a report of which users have never logged in. You can also create reports based on specific courses offered in the console. This report can be filtered to include All Users or certain groups and can have a certain start or end date; you also have the option of including archived users.

These reports can provide the following information about your users:

- Users who have started their courses within the given date range
- Users who were enrolled within the given date range but have not started their courses
- Users who started their courses within the given date range but have not finished them
- Users who were enrolled within the given date range but have not started or finished their courses
- Users who completed their courses within the given date range



- Users who were enrolled within the given date range but have not acknowledged their course-attached policies
- Users who acknowledged their course-attached policies within the given date range

## Email Exposure Check Pro

Available in the Gold and above subscription levels, the Email Exposure Check (EEC) Pro tool identifies the at-risk users in your organization by crawling business social media information and now thousands of breach databases.

Users are placed in a Risk Distribution group after the EEC Pro tool has gathered data from the searches that it performs. The group placements, **Very High Risk**, **High Risk**, and **Medium Risk**, are based on how much data was gathered on that specific user.

## Advanced Reporting

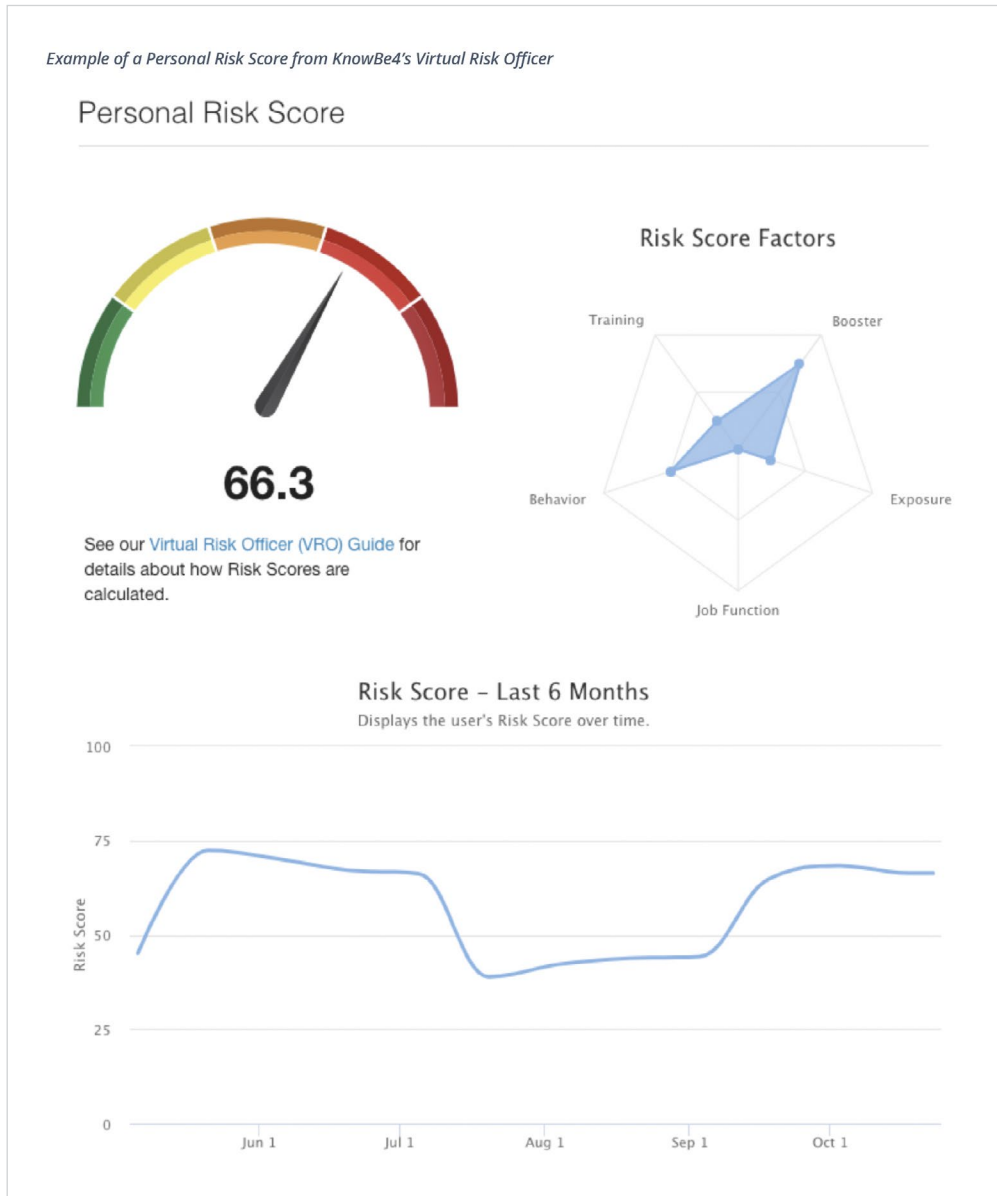
Advanced Reporting provides actionable metrics and insight into the effectiveness of your security awareness training. You can use Advanced Reporting to create many types of reports to meet the needs of your organization. This feature comes with a collection of 60+ built-in reports with insights that 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, with **Executive Reports**, you can create and deliver tailored executive-level reports that provide insights to help make data-driven decisions about your program.



## Virtual Risk Officer

The 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. With VRO, you can monitor where your employees and organization stand over time when it comes to user risk.



## Flexible APIs

Available in the Platinum and above subscription levels, KnowBe4 offers two robust APIs for additional options for user activity analysis and reporting.

- Reporting APIs allow you to pull data from your KnowBe4 console for reporting purposes. The APIs allow requests for phishing, training, user, and group data.
- The User Event API allows you to easily integrate data from your users' security-related events or training activities that happen in other third-party platforms and push them into 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.

## Password IQ

Available in the Diamond subscription level, PasswordIQ continuously monitors your organization for any detected password vulnerabilities in your Active Directory. It checks to see if your users are currently using passwords that are shared, weak, or show up in publicly available data breaches so you can establish a baseline of password issues and better manage the ongoing problem of password risk across your users.

## Subscription Levels

**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, KnowBe4 Learner App, AI-Recommended Training, 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.

**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 1,300+ items including interactive modules, videos, games, posters and newsletters related to security awareness training. In addition, you will be able to leverage our AI-Driven Phishing feature to personalize phishing tests per user, enable AI-Recommended Optional Learning for your users, and use PasswordIQ to continuously monitor your organization for any detected password vulnerabilities in your Active Directory.

**Compliance Plus:** Available as an optional add-on across all subscription levels. Compliance Plus training is interactive, relevant, and engaging with real-life simulated scenarios to help teach your users how to respond in a challenging situation. The content addresses difficult topics such as sexual harassment, diversity and inclusion, discrimination, and business ethics. The Compliance Plus library includes various types of media formats and reinforcement materials to support your compliance training program.

**PhishER Plus:** Available as a stand-alone product or as an optional add-on across all subscription levels. PhishER Plus is a light-weight SOAR platform that automatically analyzes and prioritizes reported email messages to identify and quarantine malicious email across an organization. Additionally, transforms in-the-wild phishing emails into training opportunities by flipping them into simulated phishing campaigns. With added AI-validated, crowdsourced blocklist and global PhishRIP capabilities to proactively block and remove active phishing attacks that have bypassed email filters BEFORE your user gets exposed to them, PhishER Plus saves significant budget and InfoSec time by reducing the volume of remediation efforts handled by your SOC team.

**SecurityCoach:** Available as an optional add-on for KnowBe4 customers with a Platinum or Diamond level security awareness training subscription. SecurityCoach is the first real-time security coaching product created to help IT and Security Operations teams further protect your organization's largest attack surface — your employees. Introducing a new category of technology called Human Detection and Response (HDR), SecurityCoach helps strengthen your security culture by enabling real-time coaching of your users in response to their risky security behavior.

“Social Engineering is information security’s weakest link.”

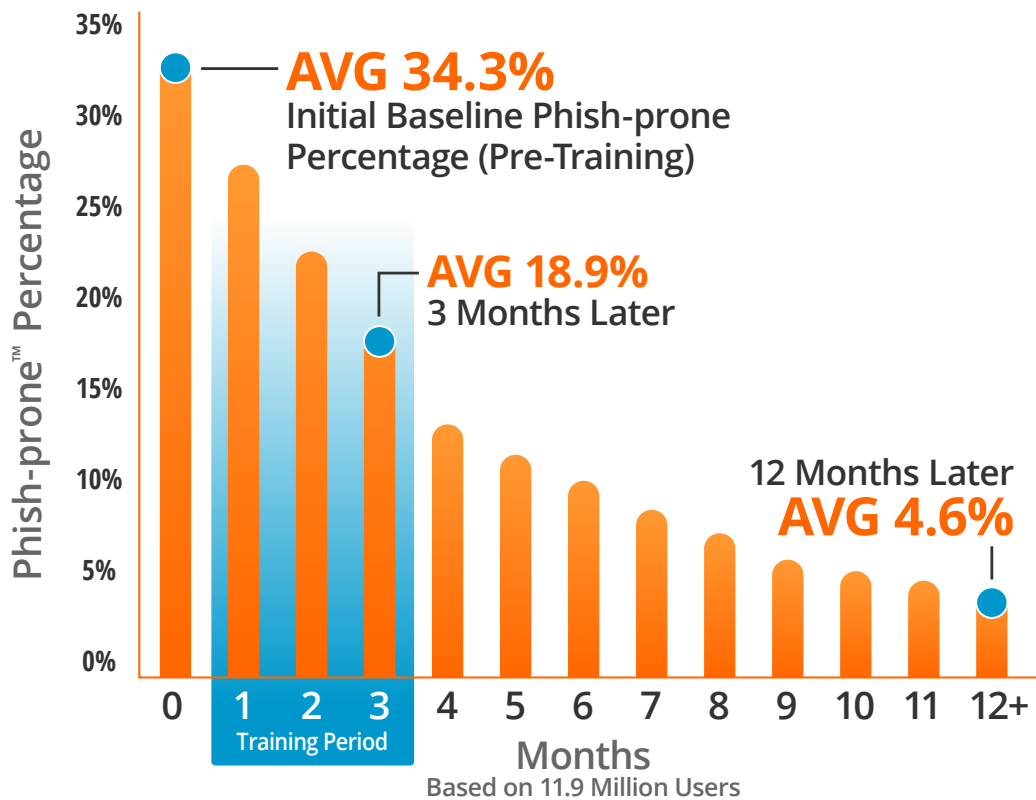
– Kevin Mitnick, ‘The World’s Most Famous Hacker’, IT Security Consultant

## 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 2024 KnowBe4 Phishing Industry Benchmarking Report clearly show where organizations’ Phish-prone Percentages started and where they ended up after at least 12 months of regular testing and security awareness training.

The overall industry initial Phish-prone Percentage benchmark turned out to be a troubling 34.3%. Fortunately, the data showed that this 34.3% can be brought down almost in half to 18.9% within 90 days of deploying new-school security awareness training. The one-year results show that by following these best practices, the final Phish-prone Percentage can be minimized to 4.6% on average.



Source: 2024 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

# KnowBe4

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

© 2024 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.