KnowBe4
Human error. Conquered.

Buyer's Guide

Security Awareness Training & Simulated Phishing Platform

Table of Contents

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.
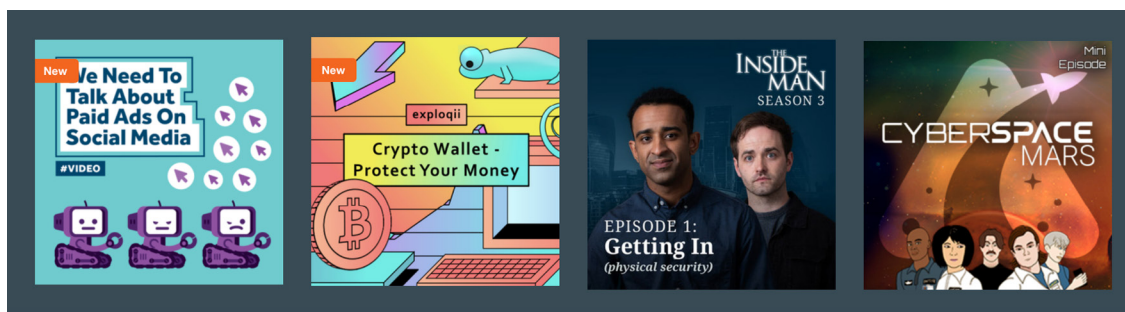
Training Modules

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.
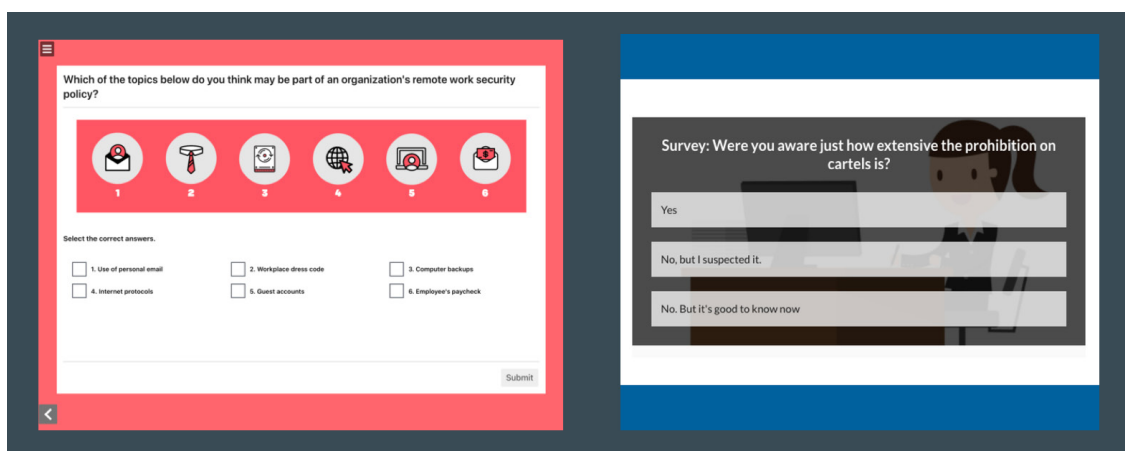

Video Modules

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.
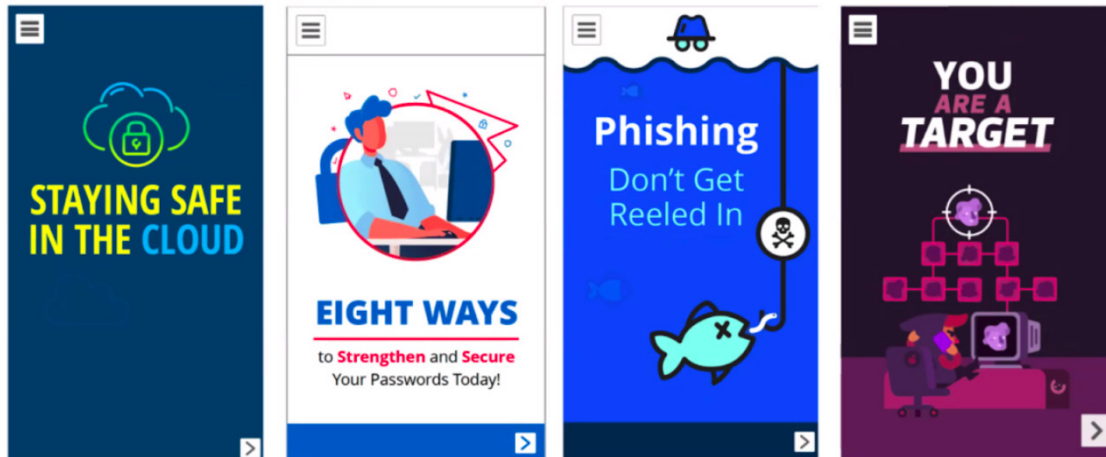

Assessments

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.
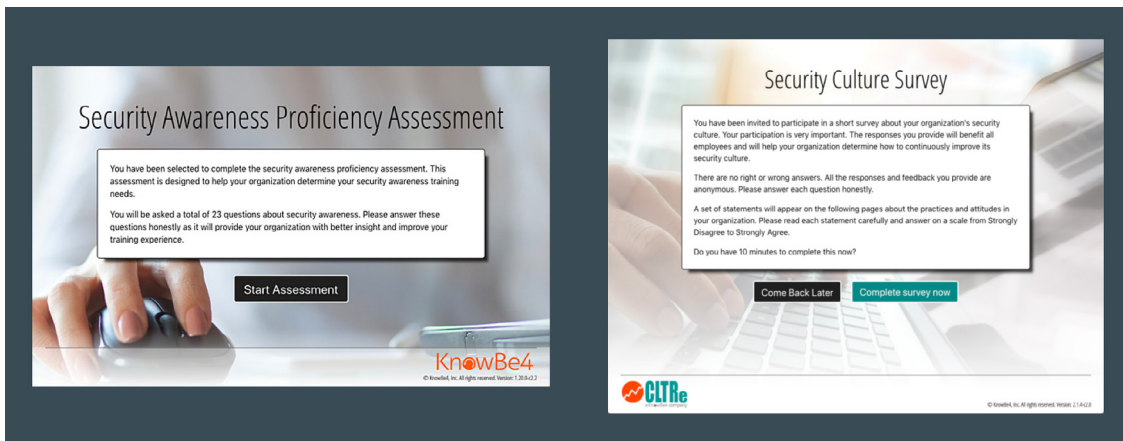
Games

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.
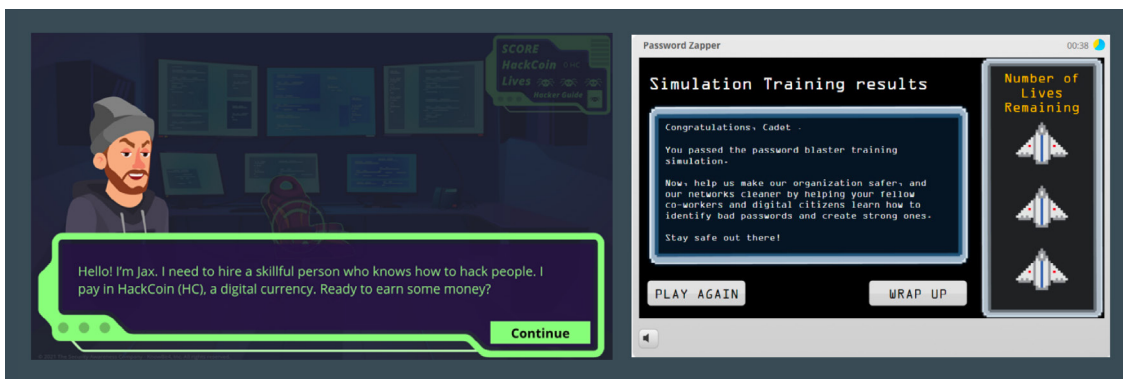
Newsletters and Security Documents

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.

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.
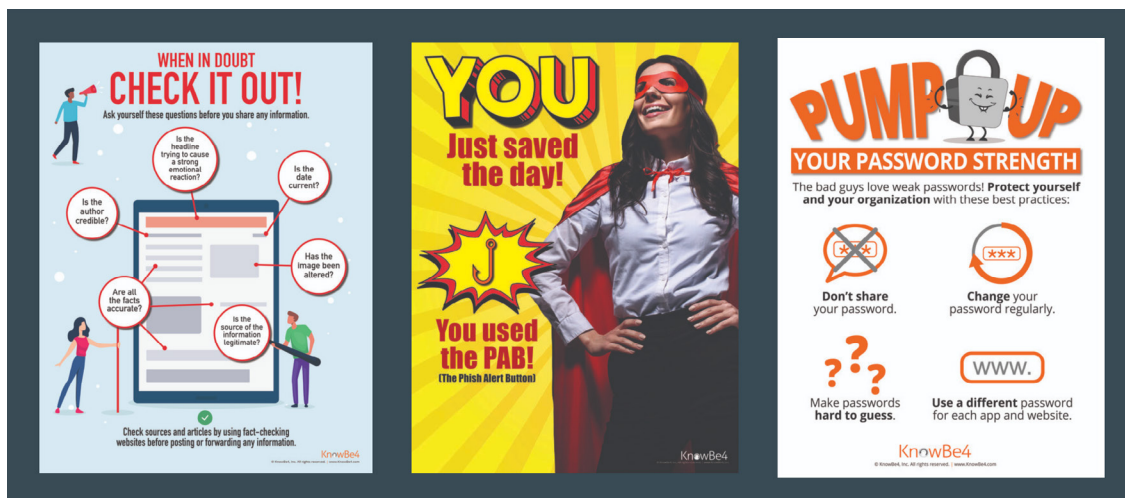
Training Access Levels

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.

Canada Privacy Training

Training content tailored to Canadian privacy laws including the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

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.

lawpilots

Prepare your users for the legal challenges of digitization with training content from Berlin-based lawpilots, which helps your users develop sustainable awareness of data protection, compliance, information security, and occupational safety.

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 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 150+ 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.
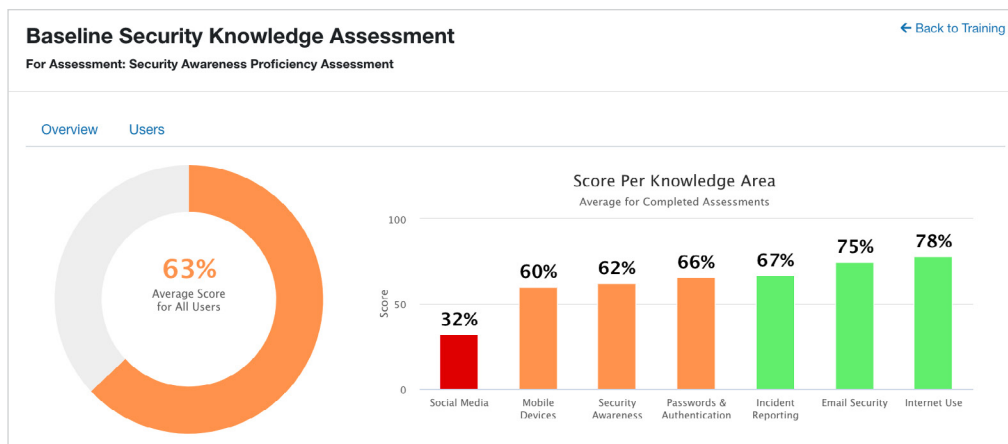
Security Culture Survey (SCS)

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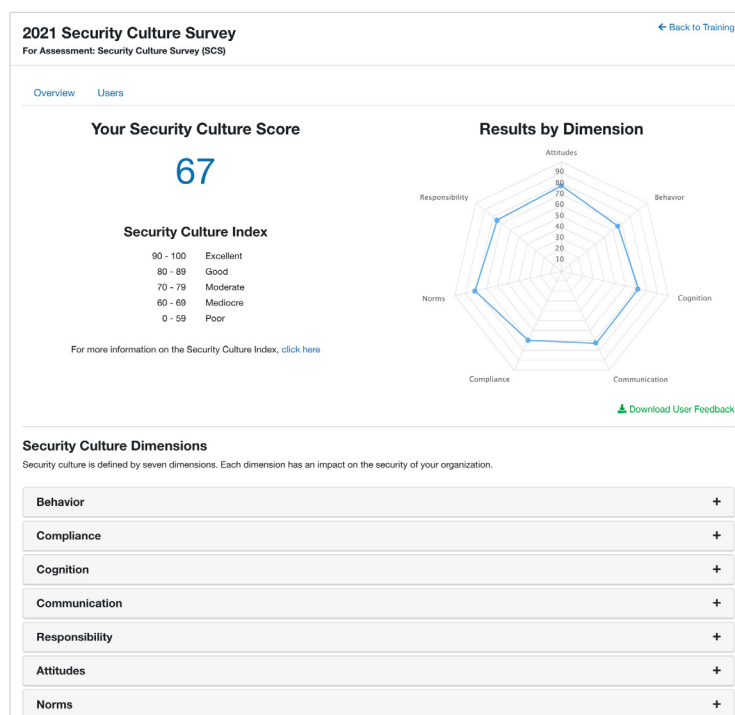
Both SAPA and SCS are rooted in assessment science and allow you to measure the security knowledge and proficiency of your users and measure your organization's overall security culture posture.

Multi-Language Support

Localized phishing and training content is available in 34+ languages, with support for localized Admin Console and Learner Experience in select languages.

The KnowBe4 Console

The KnowBe4 platform is user-friendly, intuitive, and powerful. It was built to scale for busy IT pros who have 16 other fires to put out. Customers with businesses of all sizes can get the KnowBe4 platform deployed into production at least twice as fast as our competitors.

Read on to learn more about all the features the KnowBe4 platform offers.

Automated Security Awareness Program (ASAP)

Many IT pros do not exactly know where to start when it comes to creating a security awareness training and culture program that will work for their organization.

We have taken away all the guesswork with our Automated Security Awareness Program builder (ASAP). ASAP is an in-console tool that helps you build your own customized security awareness program for your organization. ASAP will show you the steps needed to create a fully mature training program in just a few minutes!

By answering seven questions about your goals and organization, the ASAP tool will suggest and schedule a program for you automatically. The program tasks will be based on best practices on how to achieve your security awareness goals.

The program is complete with actionable tasks, helpful tips, training content suggestions and a task 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 to be used for compliance requirements and/or reporting management.

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.
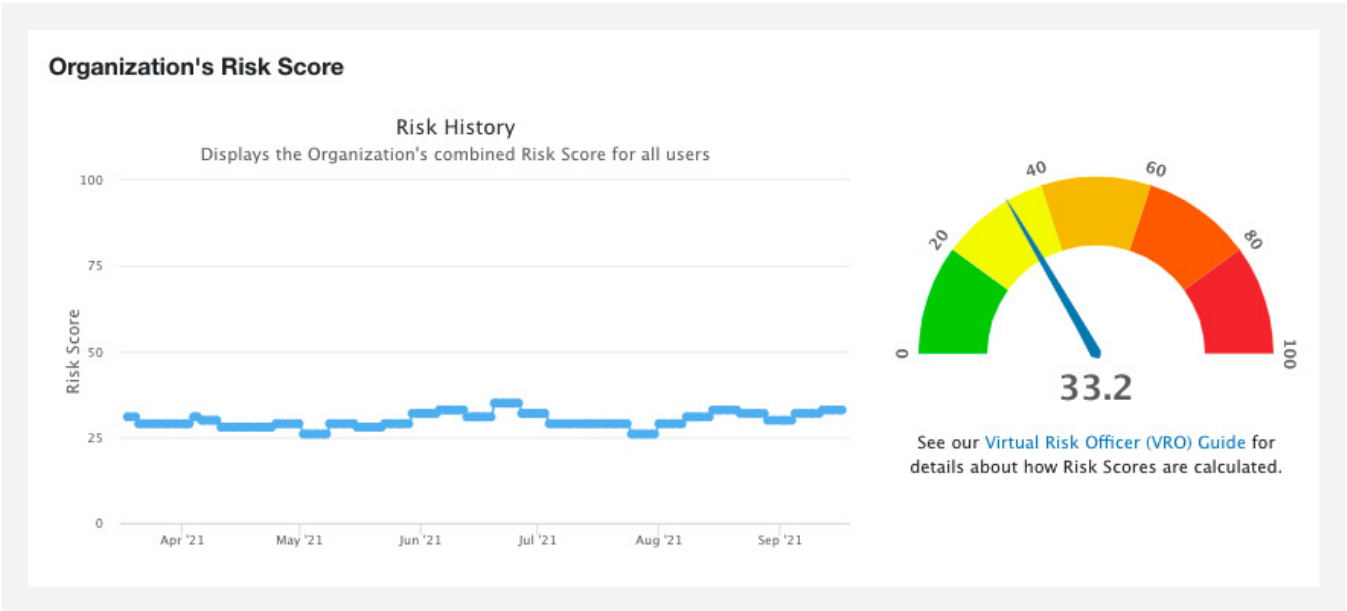
Phish-Prone Percentage Results

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.
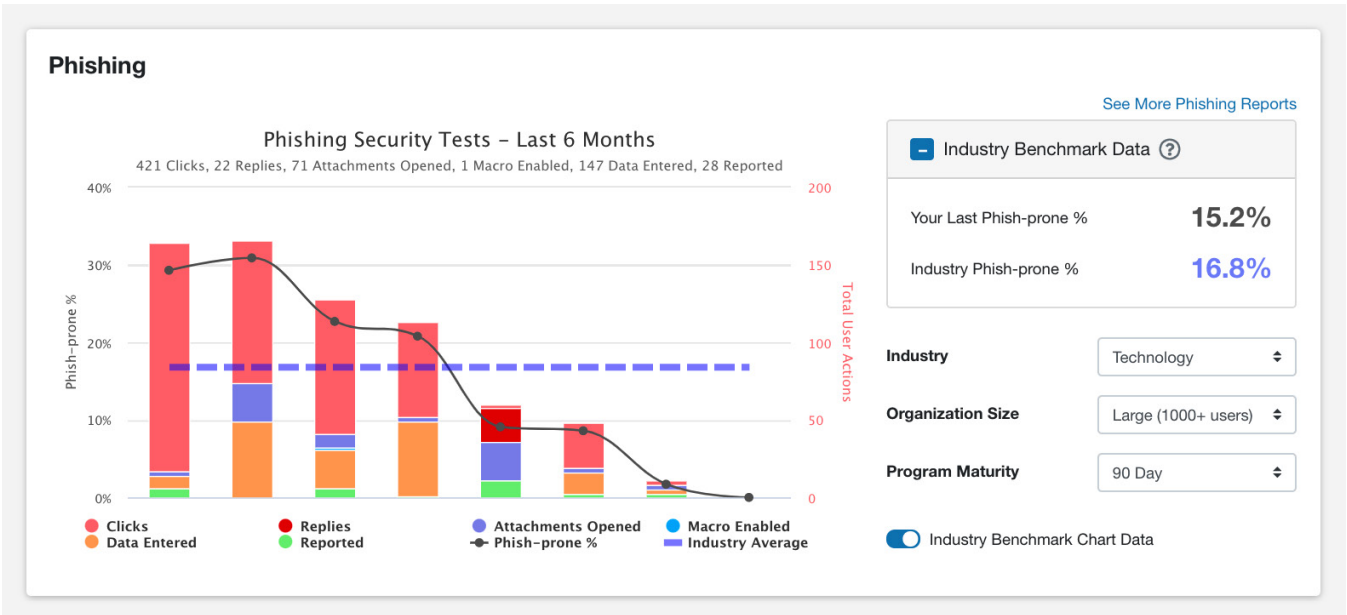
Simulated Phishing Platform

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 10,000 templates available in 34+ 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.

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.

14

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 2010, 2013, 2016 & Outlook for Microsoft 365, Exchange 2013 & 2016, Outlook on the web (Outlook.com), the Outlook Mobile App (iOS and Android), Chrome 54 and later (Linux, OS X, and Windows), Gmail accounts connected through Google Workspace, Gmail Add-on is compatible with Gmail in browser and mobile clients.
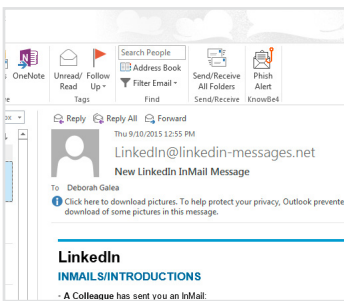
Outlook Toolbar	**Microsoft 365 Add-in Pane**	**Gmail Add-On**	**Gmail Extension**
Adds a Phish Alert Button for your users	Adds a Phish Alert Button for your users	Adds a Phish Alert Button for your users	Adds a Phish Alert Button for your users
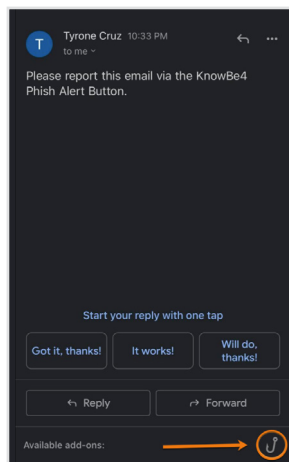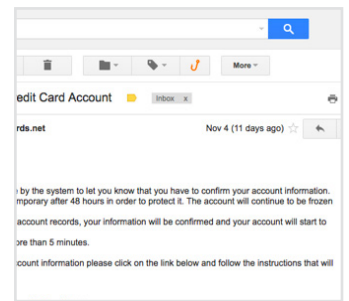
Gmail Mobile (Android)
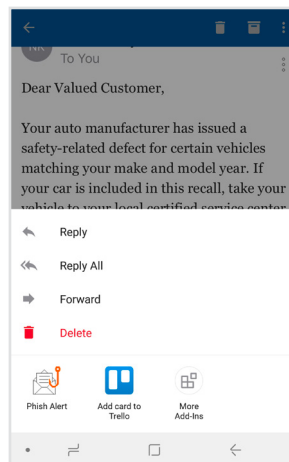
Outlook Mobile (Android)
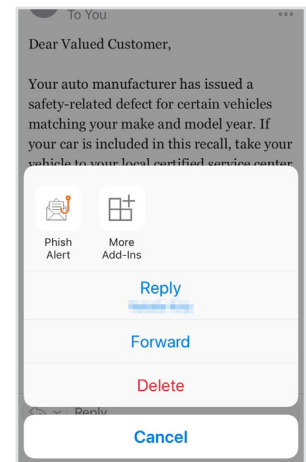
Outlook Mobile (iOS)

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.

	100%	6.1%	0.4%	4.1%	4.6%	0%	0%	0%	2%	0%
538	**538**	**33**	**2**	**22**	**25**	**0**	**0**	**0**	**11**	**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	↩	🗑	✉
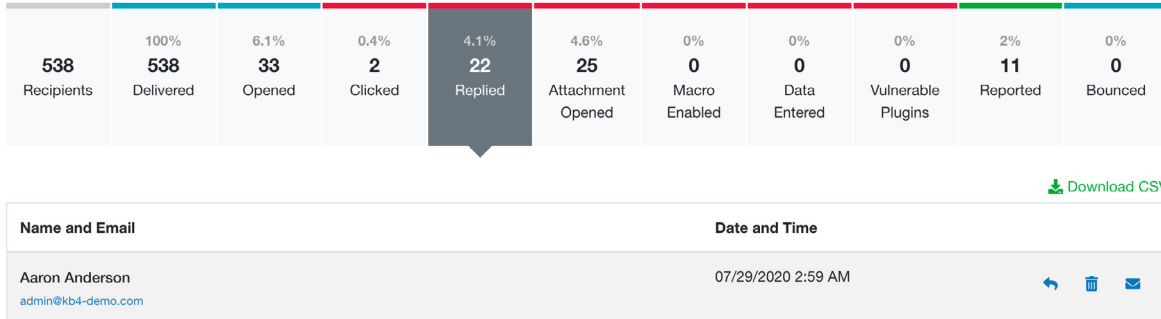
Phishing Reply Tracking is simple to use and on by default for new phishing campaigns via the "Track replies to phishing emails" option.

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.

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.

AIDA: Artificial Intelligence Driven Agent (Beta)

AIDA uses artificial intelligence to dynamically create integrated campaigns that send emails, text and voicemail to an employee, simulating a multi-vector social engineering attack. AIDA 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. (Available for U.S. and Canada).

Vishing

KnowBe4's vishing supports both domestic and international phone numbers, with an easy-to-use interface that is similar to the phishing templates section in the KnowBe4 console.
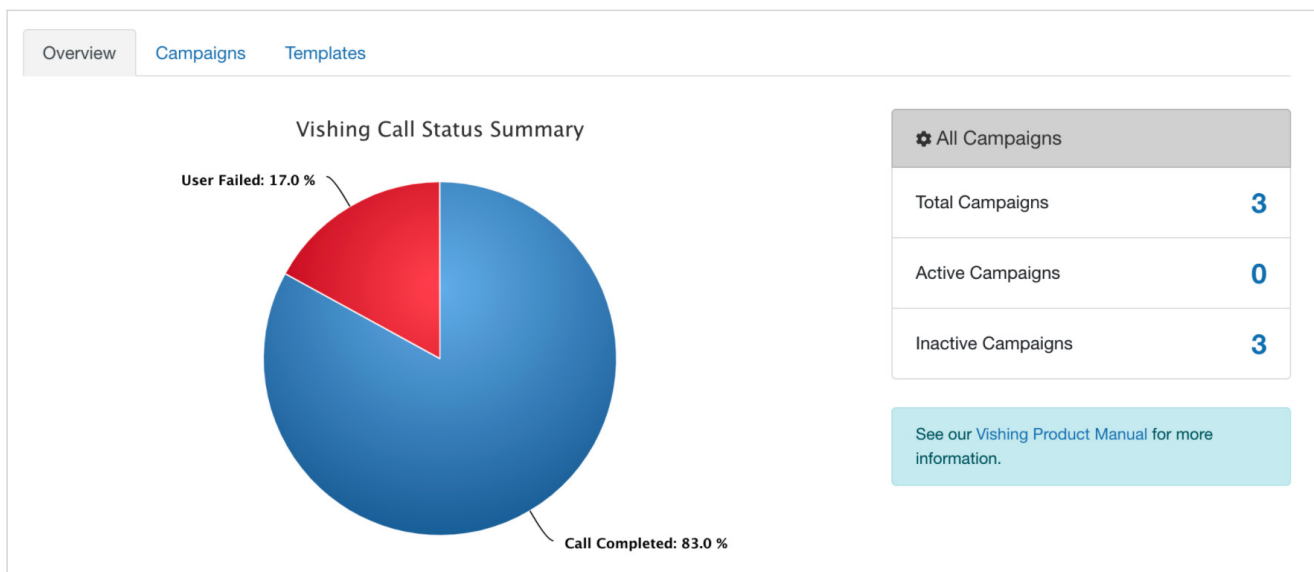
You have the ability to use text to speech, upload your own custom audio, and create your own vishing templates. Set vishing campaigns to wait for prompts and then wait for users to do something and then that is the point of failure:

- Make your own custom failure message

- Point of failure training messages

- Numbers are geolocated, just like the bad actors are doing it

With over 200 built-in vishing templates across 25 languages you are able to deliver random and full random vishing, and specify the time period when you want calls to go out.

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. Give your users a more personalized experience that adapts to their current level of knowledge.

PhishER

PhishER 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. It's your lightweight Security Orchestration, Automation and Response (SOAR) platform to orchestrate your threat response and manage the high volume of potentially malicious email messages reported by your users. When you combine KnowBe4 and PhishER 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. The products work together to not only remove email threats from your users' mailboxes, but also turn those true threats into instant training opportunities for your users.
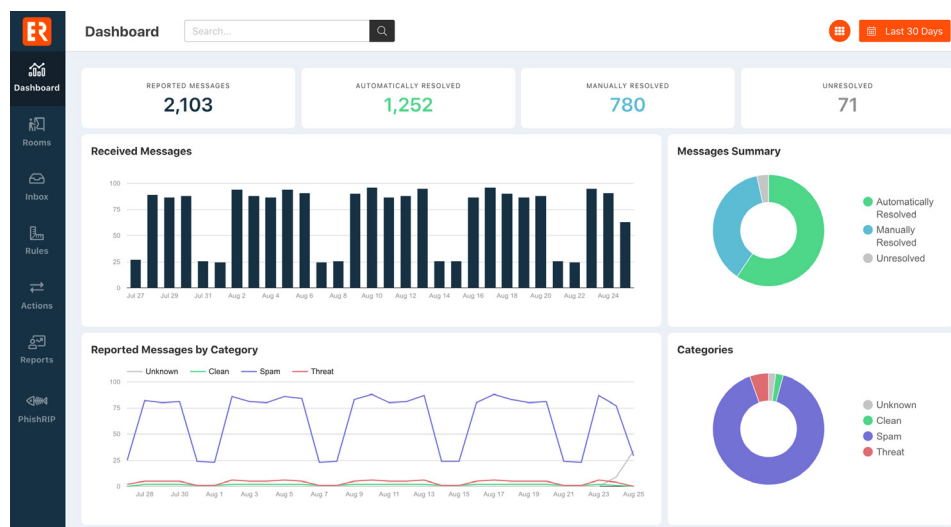
Key benefits of PhishER include:

- 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

- PhishML™ is a PhishER machine-learning module that analyzes every message coming into the PhishER platform and gives you info to make your prioritization process easier, faster, and more accurate

- PhishRIP™ is a PhishER email quarantine feature that integrates with Microsoft 365 and G Suite to help you remove, inoculate, and protect against email threats so you can shut down active phishing attacks fast

- PhishFlip™ is a PhishER 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.
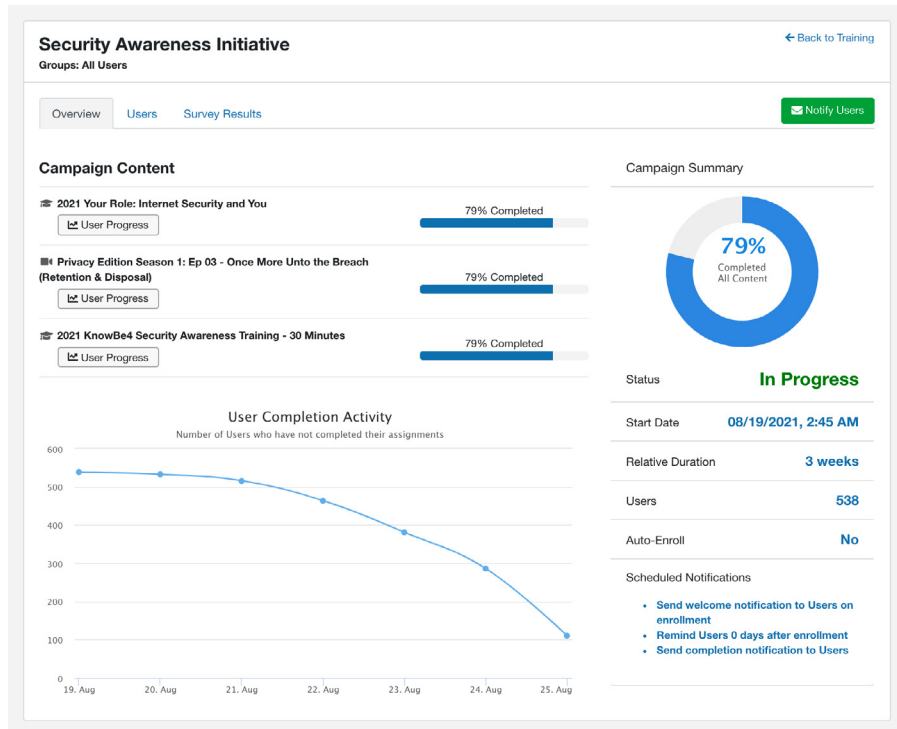
Learning Management System Options

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!

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.

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.

Recommended Training Suggestions

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.

User Management

Active Directory Integration

KnowBe4's Active Directory Integration (ADI) 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, auto-enrollment is set. Your users will be added, changed and archived in sync with changes made within AD automatically. You can also upload users with CSV files. If you use Microsoft Azure AD you can enable automatic user provisioning for the addition and removal of users via KnowBe4's Active Directory Integration.

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.
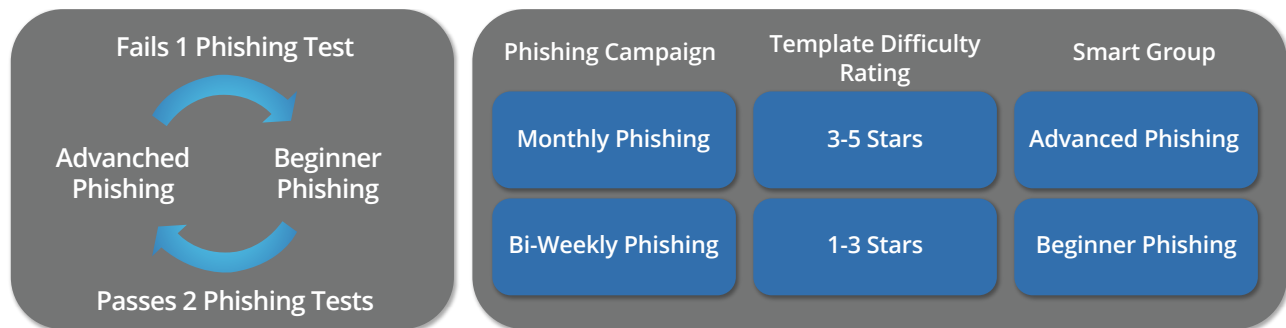
You can create "set-it-and-forget-it" phishing and training campaigns so you can instantly respond to any phishing clicks with remedial training or have new employees automatically notified of onboarding training, and much more. Choose from five key criteria types per Smart Group then add your triggers, 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
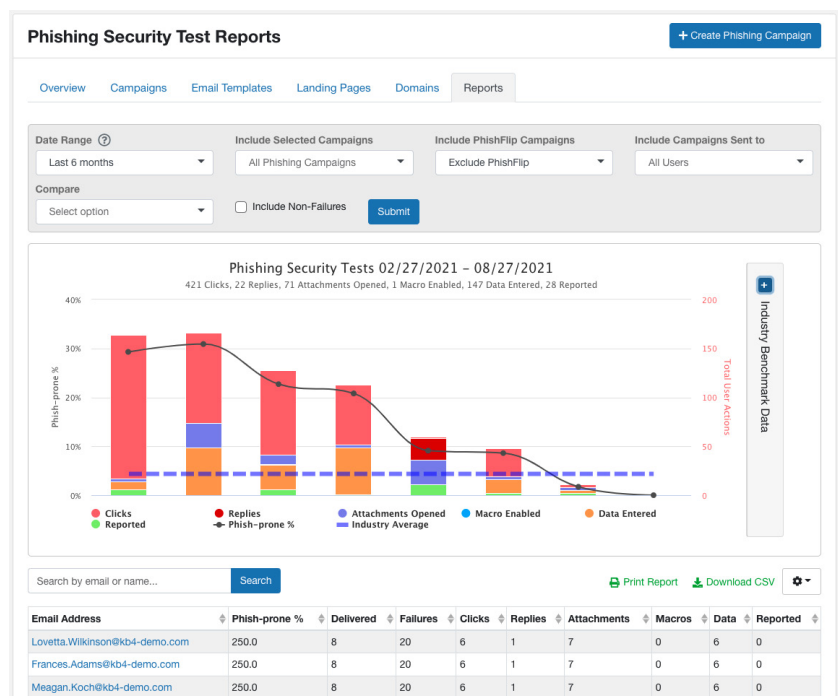
throughout the KnowBe4 console. Each Security Role is completely customizable to allow for the creation of the exact roles needed by your organization.

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.

Group Report Card

Group Risk Score
This report displays the average Risk Score of all users within the selected group.

Group Phish-prone Percentage
This report displays the average Phish-prone Percentage for users within the selected group.

User Counts
This report displays the number of active users in the selected group.

Top 5 Clicked Emails
This report displays the five most clicked phishing email templates for the selected group.

Subject	Clicks
IT: IT Notice (Link) (Spoofs Domain)	73
Facebook: Your active ad was rejected (Link)	18
Facebook: Important message regarding your Facebook profile (Link)	14
Billing Dept: Invoice is days past due (Attachment)	9
Ricky Blickger: New Invoice (Attachment)	6

Training Status Overview By Campaign
This report is organized by campaigns and displays the training statuses for users in the selected group.

Not Started In Progress Completed

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.

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.

Example of a Personal Risk Score from KnowBe4's Virtual Risk Officer

Personal Risk Score

66.3

See our Virtual Risk Officer (VRO) Guide for details about how Risk Scores are calculated.

Risk Score Factors

Training — Booster — Exposure — Job Function — Behavior

Risk Score – Last 6 Months
Displays the user's Risk Score over time.
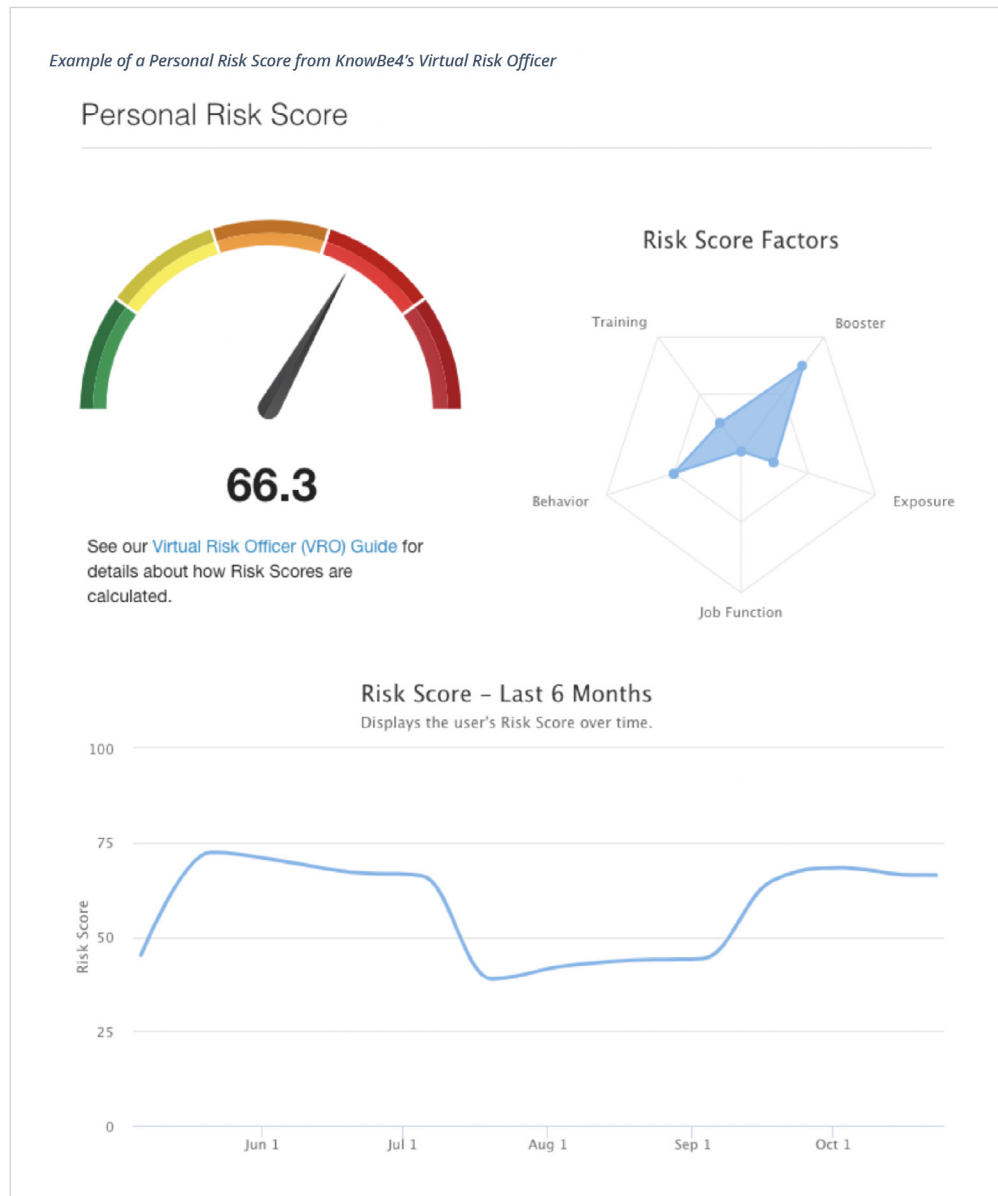
Flexible APIs

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.

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, and Enterprise-strength Reporting for the length of your subscription.

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

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

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

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

# "Social Engineering is information security's weakest link."
– Kevin Mitnick, 'The World's Most Famous Hacker', IT Security Consultant

Visible Proof the KnowBe4 System Works

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

The results of the 2021 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 31.4%. Fortunately, the data showed that this 31.4% can be brought down almost in half to 16.4% 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 4.8% on average.
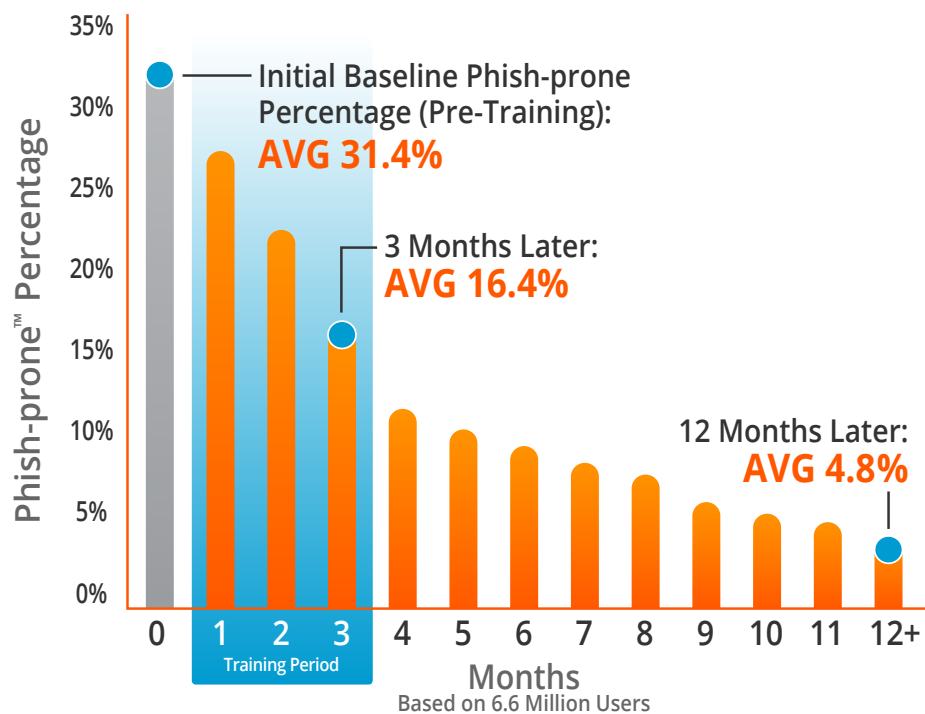
2021 KnowBe4 Phishing by Industry Benchmarking Report

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
Human error. Conquered.

01B09K04