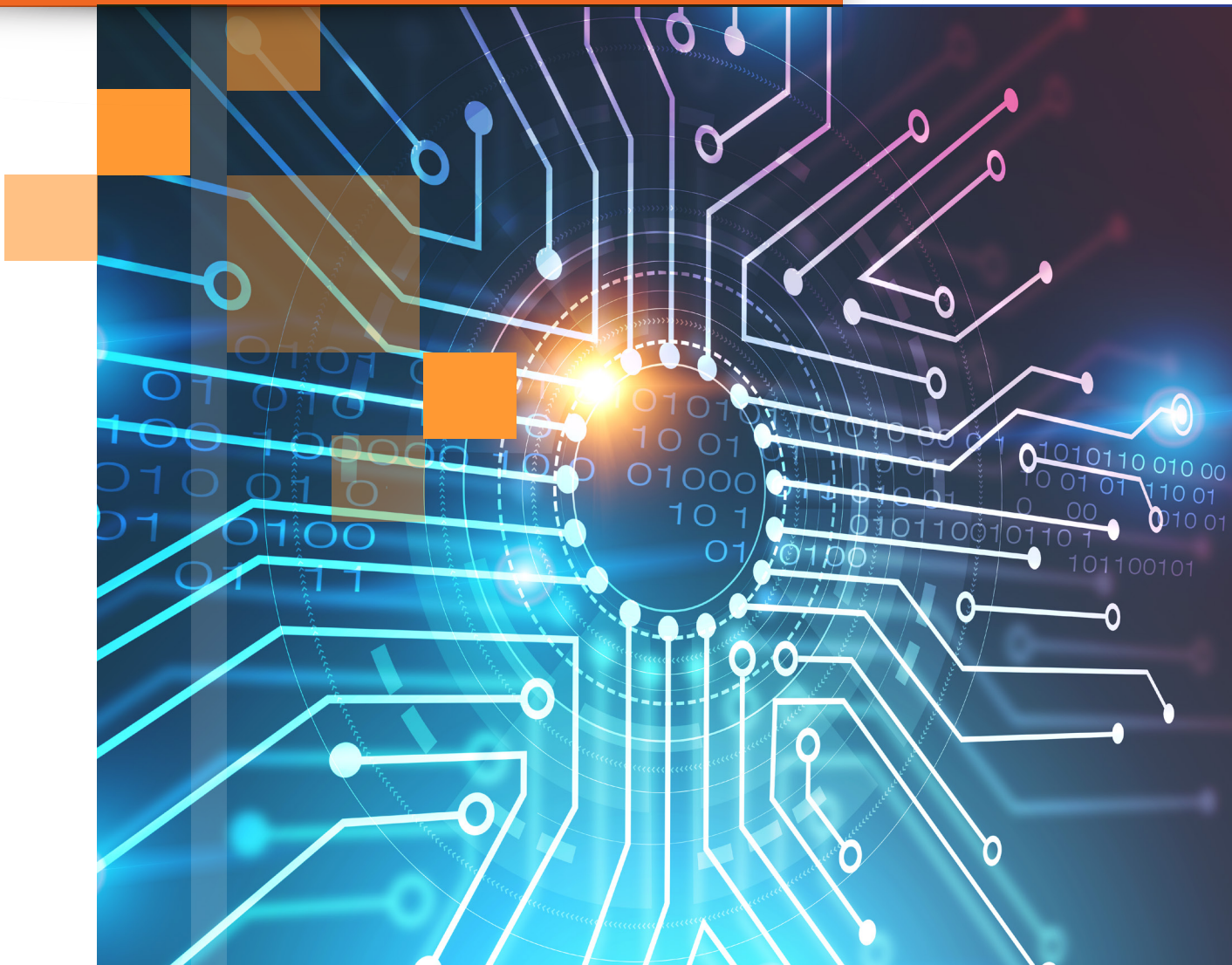


# Buyer's Guide

## Security Awareness Training and Simulated Phishing Platform



# 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 organisation. The alarming growth in sophisticated cyberattacks only makes this problem worse, as cybercriminals go for the low-hanging fruit: employees. Numerous reports and white papers show that organisations have been exposed to a massive increase in cyberattacks over the past five years.

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

The goal of security awareness training is to arm your employees with the knowledge that 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 to be risky or acceptable, the 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 also 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, Analyse

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 twofold. First, using a variety of tools and information feeds, we give the organisation a clear snapshot of their current risk profile. This step, often skipped by competitors, is a necessary part of selecting the right defensive mitigations and efficiently decreasing risk. Secondly, KnowBe4's focus on local threat intelligence allows you to focus more clearly 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 are the threats that you should be the most worried about. KnowBe4 reports on emerging global trends; but also 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 organisation's specific risk posture and then allows you to leverage both the global pulse of the real-world phishing attempts and the ones that have made it past your specific defences:

## 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 are also provided.

## 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 highlight 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

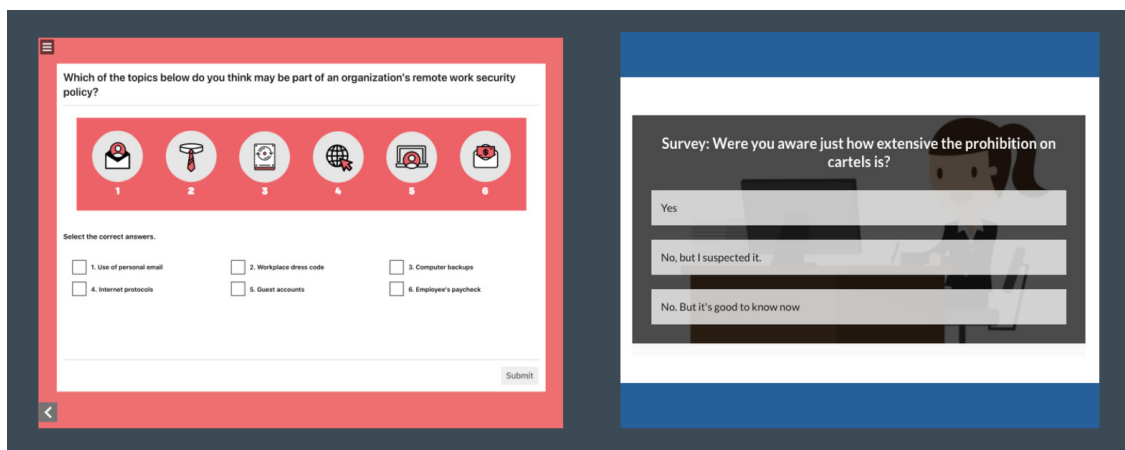
KnowBe4 offers the world's largest library of always-fresh security awareness training content that includes assessments, interactive training modules, videos, games, posters and newsletters.

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 a unique flavour and flair to the collection, ensuring that training campaigns stay current, relevant and engaging for your users. The ModStore contains a wide variety of content spanning many different topics and content types.

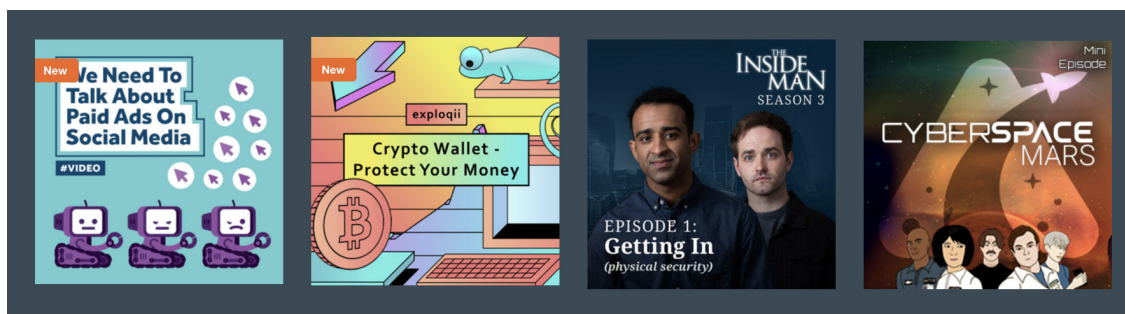
## Training Modules

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.



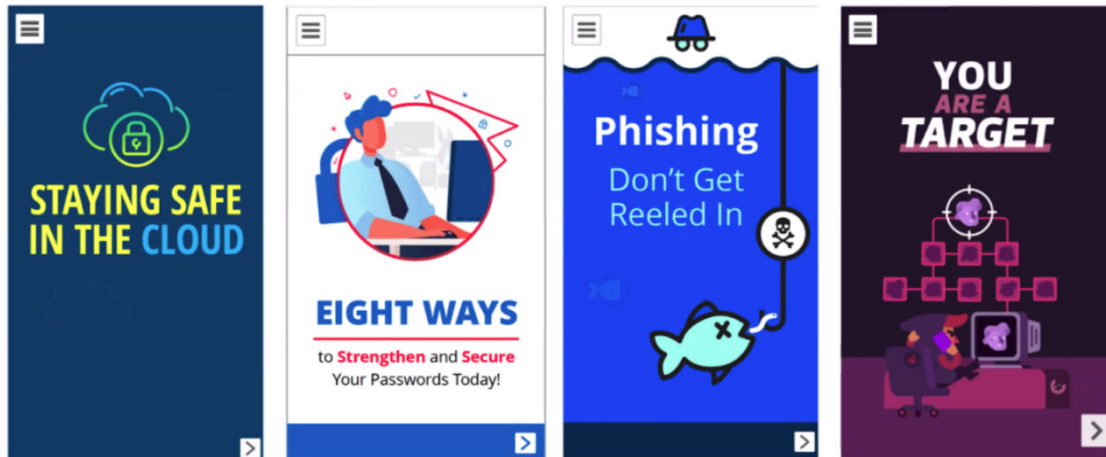
## Video Modules

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



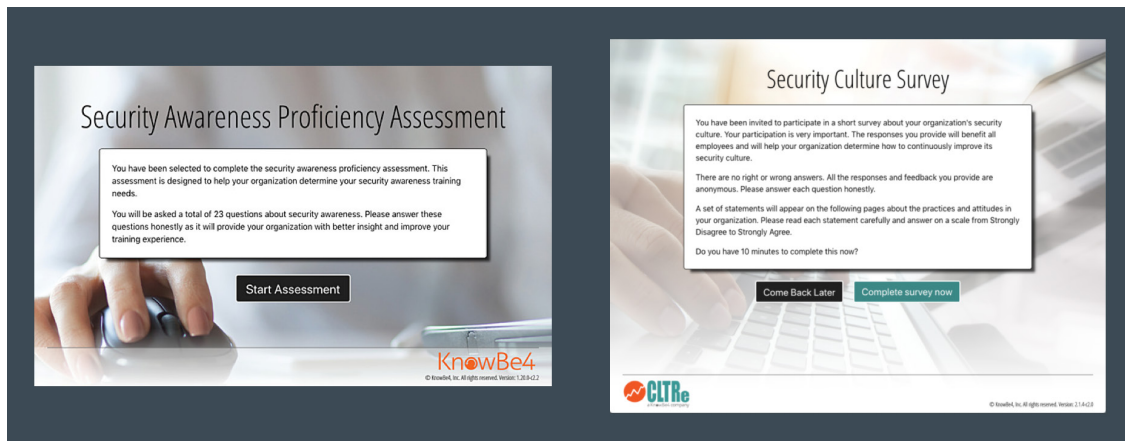
## Mobile-First Modules

Mobile-First Modules are optimised to be viewed and interacted with on a mobile device. These modules last 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.



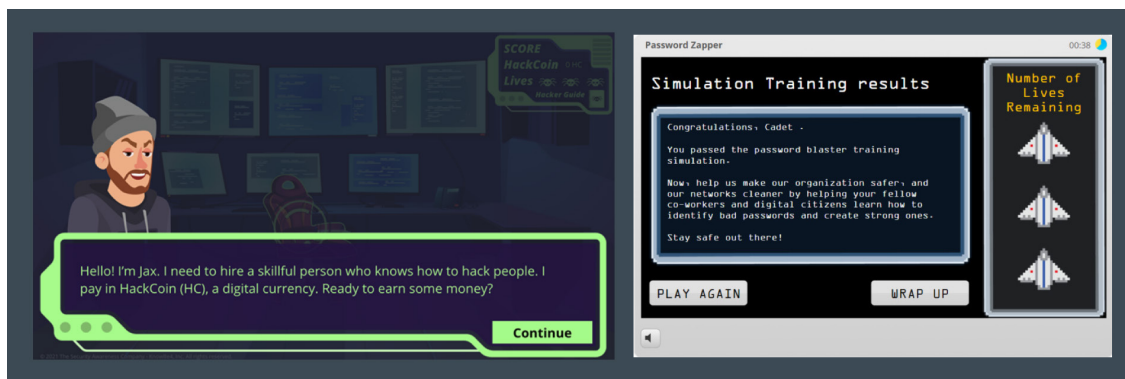
## Assessments

Assessments can provide a breakdown of your organisation'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 that help to reinforce the skills that 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 to 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 that came before 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 programme. It's ideal for organisations that do not have security awareness training in place and want to start at least an annual training programme. You receive training and video modules, assessments and educational reinforcements such as security documents and posters. Many customers start with Level I, so that their users grasp the basics of security awareness, including an understanding of what social engineering is, and then find that they are ready to move on to the next level of training content, which 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, Training Access Levels II and III will set you on a path to develop a more robust and fully mature, security awareness training programme.

## Training Access Level II (Gold and Platinum)

The Training Access Level II library builds on and expands the scope of Level I, 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 locations around the world and your organisation's industry. And, with an assortment of bite-sized training modules that last five 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 to drive behavioural 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 a comprehensive library of security awareness training content, enhancing your organisation's ability to deliver a fully mature awareness programme 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, ensuring that learning how to make smarter security decisions via real-world applications is fun and engaging. With a wide array of topics, formats, lengths and styles from multiple content publishers, you have many content options to meet the unique needs of your users and align with your organisation's corporate culture. With Level III, you can experiment with different styles and formats in different audience segments to maximise user engagement. This level also gives you the flexibility to mix things up and 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 programme 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 reusing 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 multifaceted security awareness training programme.



### KnowBe4

Interactive security awareness training content developed by KnowBe4 and Kevin Mitnick demonstrates 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 that's jam-packed with information. The content is thoughtfully designed to maximise comprehension, retention and behavioural change, with a well-rounded course line-up that also features knowledge checks, course interaction, quizzes, games, documents and monthly newsletters.



### Popcorn Training

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



### Exploqii

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



### Twist & Shout

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



### El Pescador

Colourful animations bring training to life! Adventures with the memorable Captain El Pescador will have learners tuned in for sound advice about 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 organisations to assess, build and improve their security culture.



### Saya University

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



### MediaPRO

Interactive modules and short videos ensure that lessons are engaging and that information is retained, and they 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)*

## Compliance Plus

KnowBe4's Compliance Plus training is interactive, relevant and engaging, including simulated, real-world 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 programme.

## 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 such as: 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 customised 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' reactions 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) customise 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 and Tips' newsletters to keep your users informed on the latest phishing scams and help to reinforce basic security tips. You can use these newsletters as part of a weekly, biweekly or monthly campaign when you set up a phishing campaign in the KnowBe4 console.

**Email Preview - KnowBe4 Scam of the Week: Beware of Copyright Scammers**

From: Scam of the Week <ScamoftheWeek@KnowBe4.com>  
 Reply-To: Scam of the Week <ScamoftheWeek@KnowBe4.com>  
 Subject: KnowBe4 Scam of the Week: Beware of Copyright Scammers

Template ID: 520147-112820

[Send Me a Test Email](#)

☐ Show Remote Images

**SCAM OF THE WEEK:**  
Beware of Copyright Scammers

In a recent phishing scam, scammers told users that they have violated copyright laws and must take immediate action to protect their account. The scammers claim that the content the user posted, such as an Instagram photo or a YouTube video, violates copyright law. Users are told that they must immediately click a link to protect their account from suspension or deactivation. However, in a recent version of this scam, the scammers are trying to get you on the phone with a fake support tech.

**OOPS**  
YOU FAILED A SIMULATED PHISHING TEST

Can you tell if an email is PHISH or SPAM? Read the email scenarios below!

**SCENARIOS**

Congratulations! You just won a \$100 gift card, but you only have 24 hours to claim your prize. Hurry!

Save the date: Early Bird Registration for our business conference begins next month.

This Prince of Nigeria needs your help! He is willing to let you and is looking for a potential buyer overseas.

Back from the IT department is requesting your login information so he can install an update on your work machine.

Cyber Monday Sale! Take all of the latest deals on electronics by visiting us online.

**PHISH**

**SPAM**

CLICK THE SOLUTION BUTTON TO SEE THE CORRECT ANSWERS

**SOLUTION**

**Phishing Email Templates**

Overview Campaigns Email Templates Landing Pages Domains Reports

My Templates System Templates Community Templates

**System Categories**

- All Templates 10288
- Coronavirus/COVID-19 Phishing 69
- Coronavirus Alerts (Not PST) 11
- Coronavirus Alerts (Branded) (Not PST) 11
- Reported Phishes of the Week 10
- Current Event of the Week 1
- Current Event of the Month 1
- Scam of the Week (Not PST) 1
- Scam of the Week (Branded) (Not PST) 1
- Security Hints&Tips (Not PST) 17
- Security Hints&Tips (Branded) (Not PST) 18
- PCI Security Hints & Tips (Not PST) 5
- HIPAA Security Hints & Tips (Not PST) 5
- Attachments with Macros 26
- Banking and Finance 319
- Baseline Templates 21
- Brand Knock-Offs 106
- Business 577
- CFA/Business Advising Industry 12
- Current Events 30
- Data Breach 12
- Education 26
- Government 57
- Healthcare 52
- Holiday 7
- Holiday (Off-Season) 113
- Human Resources 151
- IT 151
- Legal Industry 31
- Mail Notifications 154
- Online Services 1129
- Outdoor/Sporting Goods 5
- Phishing For Sensitive Information 20
- Real Estate Industry 55
- Reply-To Only "No Links or Attachments" 20
- Retired Current Events 55
- Seasonal (Non-current) 76
- Social Networking 133
- Arabic 127
- Burmese 38
- Chinese (Mandarin) - Simplified 157
- Chinese (Cantonese) - Traditional 157
- Chinese (Mandarin) - Traditional 151

**All Templates** ☐ Show Hidden Items

Template Name	Updated	Difficulty	Category	Actions
PROMOÇÃO DA PETROBRAS: UM ANO DE GASOLINA GRÁTIS (Link)	08/03/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
KnowBe4 Security Tips - How to Safely Shop Online	08/03/2021	☆☆☆☆	Security Hints&Tips (Branded) (Not PST)	<a href="#">View</a> <a href="#">Edit</a>
Scam of the Week: Bluffing Blackmail	08/02/2021	☆☆☆☆	Scam of the Week (Branded) (Not PST)	<a href="#">View</a> <a href="#">Edit</a>
KnowBe4 Scam of the Week: Bluffing Blackmail	08/02/2021	☆☆☆☆	Scam of the Week (Not PST)	<a href="#">View</a> <a href="#">Edit</a>
IT: Mandatory Password Complexity Review (Link) (Spoofs Domain)	08/02/2021	☆☆☆☆	Current Event of the Week	<a href="#">View</a> <a href="#">Edit</a>
Notice of Lease Changes (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Retirement Plan Report (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Board Approval Meeting (Link) (Spoofs Domain)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Apple: Lost Apple device in use (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Microsoft: Your credentials are set to expire today (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Facebook: Misuse of Data - Take Action (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Facebook: Image Copyrighted (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
Google Photos: You are automatically sharing photos with a partner in Google Photos (Link)	08/02/2021	☆☆☆☆	Reported Phishes of the Week	<a href="#">View</a> <a href="#">Edit</a>
KnowBe4 Security Tips - Why You Should Actually Read That Privacy Policy	08/02/2021	☆☆☆☆	Security Hints&Tips (Not PST)	<a href="#">View</a> <a href="#">Edit</a>
KnowBe4 Security Tips - How to Safely Shop Online	08/02/2021	☆☆☆☆	Security Hints&Tips (Not PST)	<a href="#">View</a> <a href="#">Edit</a>
Abono fiscal [city] (Link) (Spoof)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
Acesso gratuito ao Hangouts Reuniões (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
[99] O que você achou? (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
95% de desconto! em todos nossos produtos! (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
60% de desconto nas próximas 48h! Um programa de incentivo corporativo. (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
("85%") de desconto na sua próxima compra! (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
3 meses grátis com seus amigos no pizza! (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
302424611008/DEBITO/MZN1.500.00 - Notificação de Transação (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
3 meses gratuitos da versão Premium! (Link)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>
A Conta Digital da [company_name] já chegou! (Link) (Anexo PDF)	08/02/2021	☆☆☆☆	Portuguese (Brazil)	<a href="#">View</a> <a href="#">Edit</a>

Show 25 per page Page 1 of 412

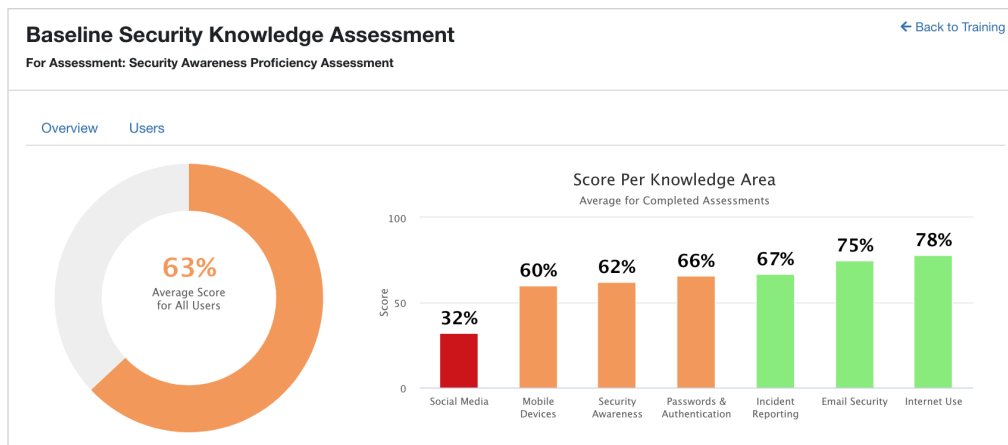
# Assessments

Find out where your users are regarding both security knowledge and security culture to help establish baseline security metrics that you can improve over time.

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

## Security Awareness Proficiency Assessment (SAPA)

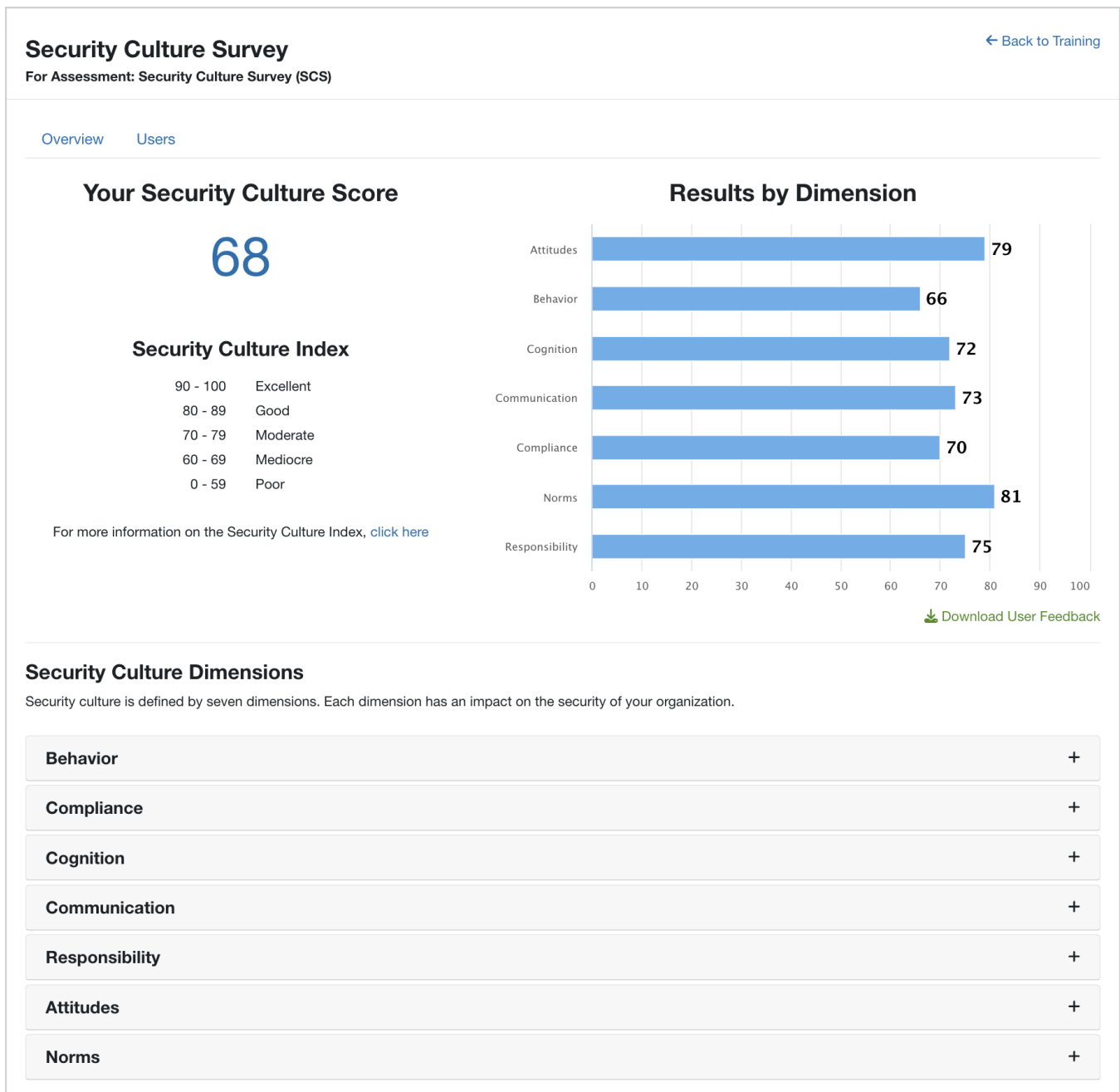
SAPA is a skills-based assessment designed to help your organisation to determine your security awareness training needs, by identifying gaps in individual users' knowledge, as well as recommended learning improvements.



## Security Culture Survey (SCS)

The Security Culture Survey measures the sentiments of your users towards security in your organisation – the psychological and social aspects that drive social behaviour. The SCS shows you the overall effectiveness of your security culture programme 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 organisation's overall security culture posture.

## Multi-Language Support

Localised 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 localised Admin Console is available in 10 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 quickly as our competitors.

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

## Automated Security Awareness Programme (ASAP)

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

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

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

**ASAP**

**Your Security Awareness Program Tasks**  
Based on your questionnaire answers, we generated a customized program for your organization. Follow the steps below to implement your program. [Download PDF] [Settings]

**Calendar** [Task List] [Calendar]

**August 2021** [Today] [Previous] [Next]

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

**Task List** [Task List] [Calendar]

Next Task: **Create training campaigns for your compliance training modules** (about 2 hours)

Upcoming Completed

**Start your Automated Security Awareness Program (ASAP)**

Create a customized security awareness program for your organization in just minutes. Your ASAP includes step-by-step instructions and recommended training content tailored to your specific needs.

[Get Started] [Watch Video]

**Create Your Security Awareness Program**

- Complete a Questionnaire**  
Spend a few minutes completing a questionnaire about your organization and security goals.
- Receive Custom Program**  
We use the answers you provide to create your customized security awareness program.
- Train Your Users**  
Train your users to make smarter security decisions by following your step-by-step program.

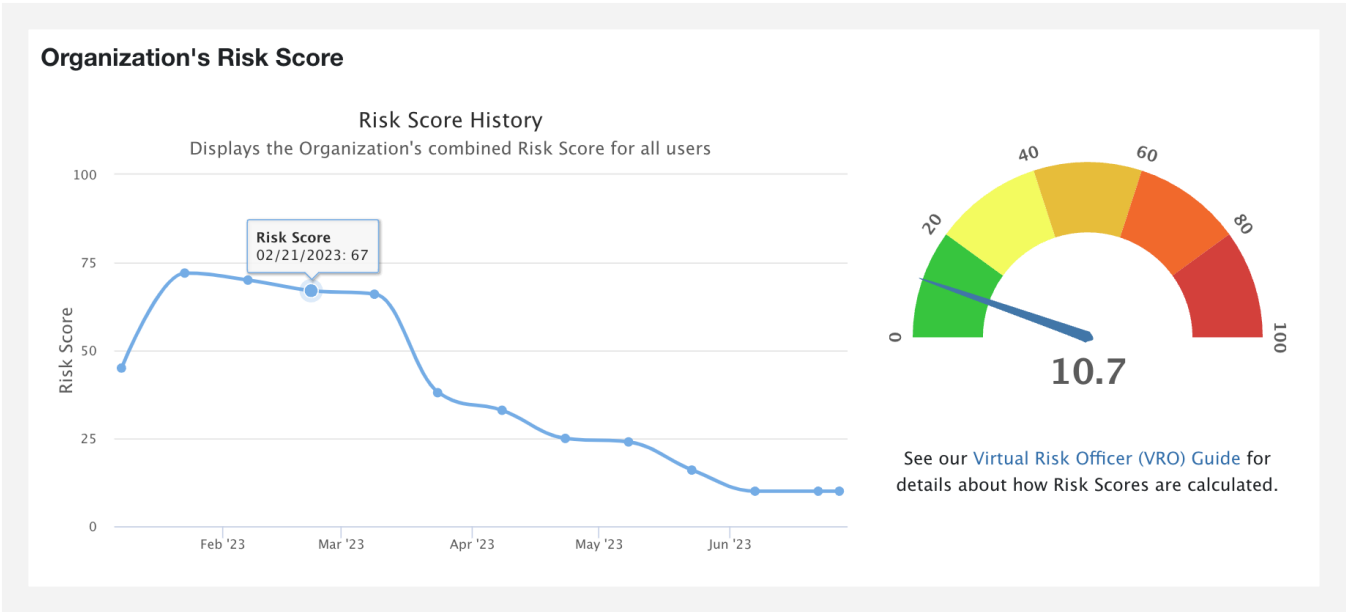
The programme comes complete with actionable tasks, helpful tips, training content suggestions and a task management calendar. Your customised programme can then be fully managed from within the KnowBe4 console. You also have the ability to export the full programme as a detailed or executive summary 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 organisation's Risk Score and see how your end users are doing at a glance, and compare their results to your peers across industries with Industry Benchmarking.

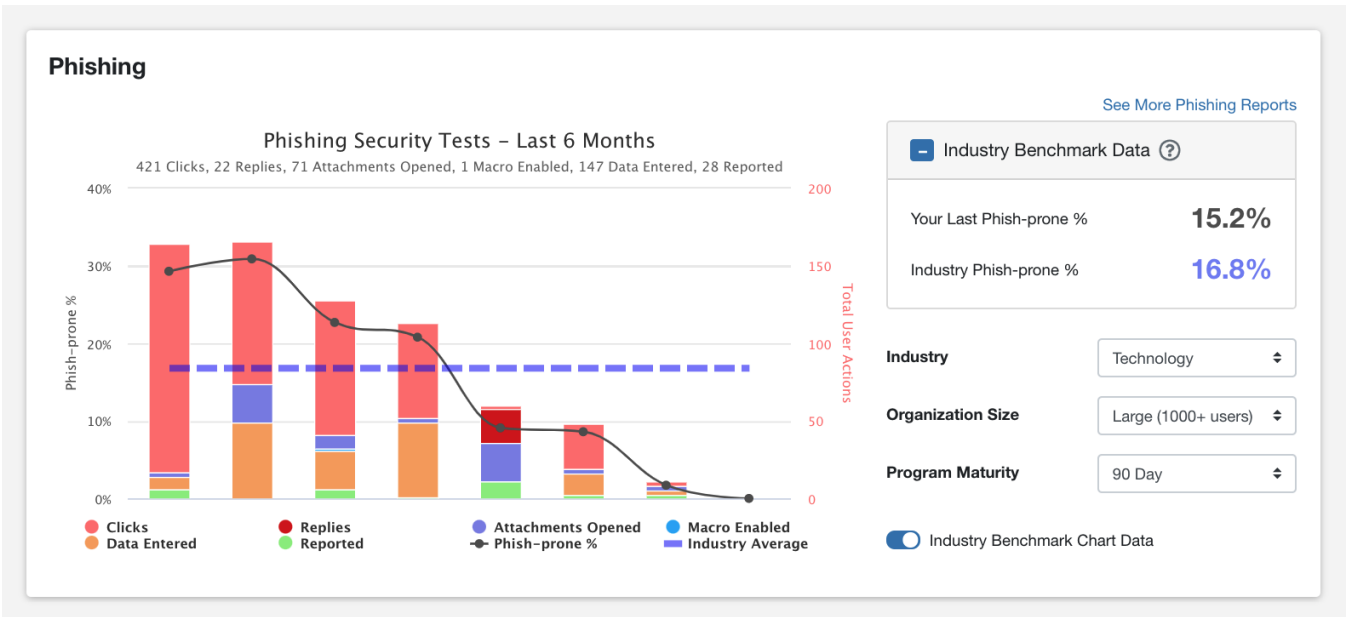
## View Organisation Risk Score

View your organisation'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 allows you to see your organisation'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 organisation's Phish-Prone Percentage. To get started with your training programme, create your phishing campaign – this is the first step to testing your users so that you can determine what training they 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-off, weekly, biweekly 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 and preventing users from giving each other advance notice of a phishing test.

The 'New Phishing Campaign' form includes the following fields and options:

- Campaign Name:** Q1 SAT Training Campaign
- Send to:** All Users (Selected), Specific Groups
- Frequency:** One-time (Selected), 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 (Unselected), Send emails over 3 business days (Selected)
- 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 (Selected), Track Replies to Phishing Emails (Unselected)
- Template Categories:** Select one or more categories... (Unselected), Full Random (Random email to each user) (Selected)
- Send Localized Emails:** (Unselected)
- Difficulty Rating:** All Ratings (Selected)
- Phish Link Domain:** Random Domain (Selected)
- Landing Page:** Default Landing Pages (Selected)
- Add Clickers to:** Select Group (Selected)
- Send an email report to account admins after each phishing test:** (Unselected)
- Hide from Reports:** (Unselected)
- Create Campaign:** (Button)

The 'WebFaxOnline: Your Customer Sent A Fax (Link)' template includes the following fields and options:

- Template Name:** WebFaxOnline: Your Customer Sent A Fax (Link)
- Sender's Email Address:** FaxMessage@web.ofaxOnline.com
- Sender's Name:** WebFaxOnline
- Reply-To Email Address:** FaxMessage@web.ofaxOnline.com
- Reply-To Name:** WebFaxOnline
- Subject:** Your Customer has sent an eFax message - 4 Pages
- Attachment File Name:** [Redacted]
- Attachment Type:** Select Option
- Body:** Your Customer has sent an eFax message - 4 Pages. [Redacted] \* The reference number for this fax is [Redacted] at 47-999999999999. View this fax using your PDF reader. [Redacted] Please visit [Redacted] if you have any questions regarding this message or our service. Thank you for using the eFax service!
- Landing Page:** Default Landing Page
- Landing Domain:** Default (secured-login.net)
- Difficulty Rating:** ★★☆☆ Moderate
- Save:** (Button)

## Phishing Template Customisation

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



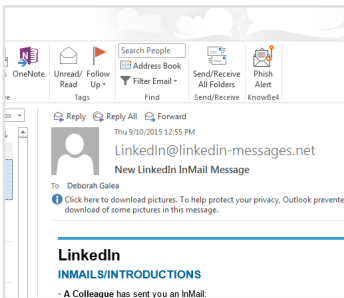
## Phish Alert Button

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 settings.

- When the user clicks on the Phish Alert Button in a simulated Phishing Security Test, this user's correct action is reported
- When the user clicks on the Phish Alert Button in a non-simulated phishing email, the email will be directly forwarded to your Incident Response team
- Has fully customisable button text and user dialogue boxes
- Clients supported: Outlook 2016, 2019, 2021 and Outlook for Microsoft 365, Exchange 2016, 2019 and 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.

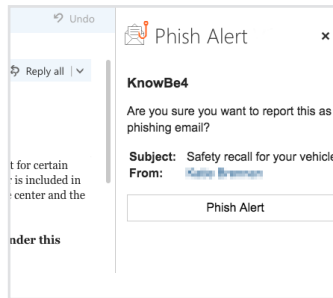
### Outlook Toolbar

Adds a Phish Alert Button for your users



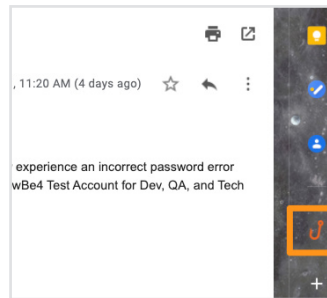
### Microsoft 365 Add-in Pane

Adds a Phish Alert Button for your users



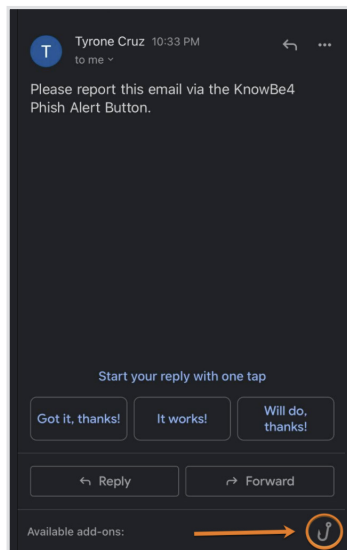
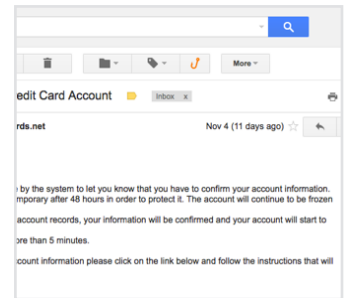
### Gmail Add-On

Adds a Phish Alert Button for your users

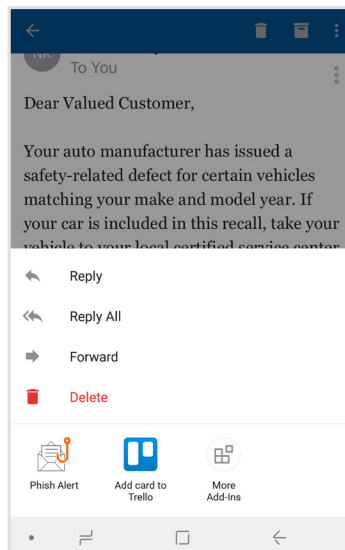


### Gmail Extension

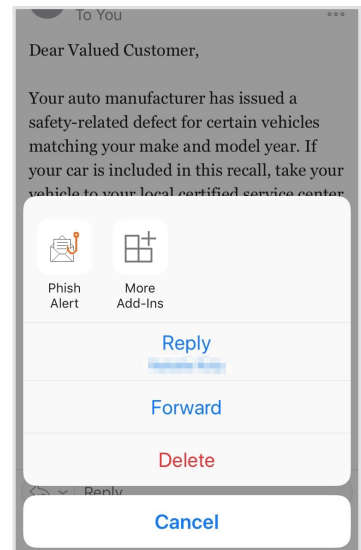
Adds a Phish Alert Button for your users



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 also provide 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 Recipients	100% 538 Delivered	6.1% 33 Opened	0.4% 2 Clicked	4.1% 22 Replied	4.6% 25 Attachment Opened	0% 0 Macro Enabled	0% 0 Data Entered	0% 0 Vulnerable Plugins	2% 11 Reported	0% 0 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 is enabled by default for new phishing campaigns via the 'Track replies to phishing emails' option.

## Custom Phish Domains

Phish Domain is the name that 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 also 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 to learn more about these features.

### Social Engineering Indicators

Our Social Engineering Indicators (SEI) feature is patented technology that turns every simulated phishing email into a tool that 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 customise any simulated phishing email and create your own red flags.

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



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 own USB Drive Test from the KnowBe4 console and download the special 'beaconised' 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 into 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 bar codes that contain data in a compact format. If your users scan a malicious bar code, they could be prompted to visit a dangerous website. Additionally, malicious links hidden in QR codes may be able to bypass your organisation'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 to 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.

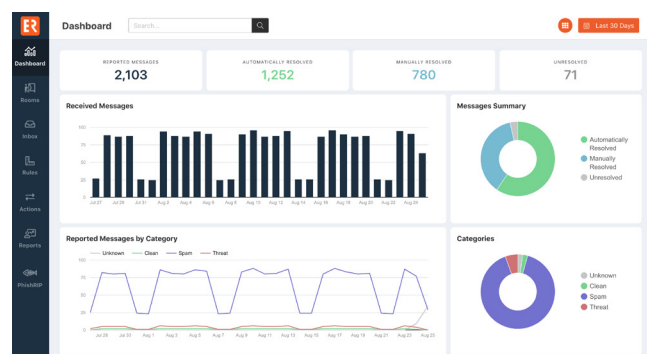
Think of it as your own AI phishing assistant that automatically chooses the best phishing test for each user, at that moment. When you use AI-Driven Phishing, you essentially create a unique phishing campaign for each of your users to make sure that every user receives simulated phishing tests personalised to their individual level. Give your users a more personalised 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 to cut through the inbox noise and respond to the most dangerous threats more quickly. PhishER Plus was developed to help you supercharge your organisation's email security defences 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 organisation that wants to automatically prioritise and manage potentially malicious messages – accurately and fast! When you combine KnowBe4 and PhishER Plus as part of your email security workstream, not only can you reduce the burden on your InfoSec and IR teams while identifying real threats more quickly, but you can also take your security awareness training programme 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 to identify a widespread phishing attack against your organisation
- 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 email server.
- PhishML™ is a PhishER Plus machine-learning module that analyses every message that comes into the PhishER Plus platform and gives you info that makes your prioritisation 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 that other PhishER Plus customers have 'ripped' from their organisation's inboxes 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 organisation into safe, simulated phishing campaigns.

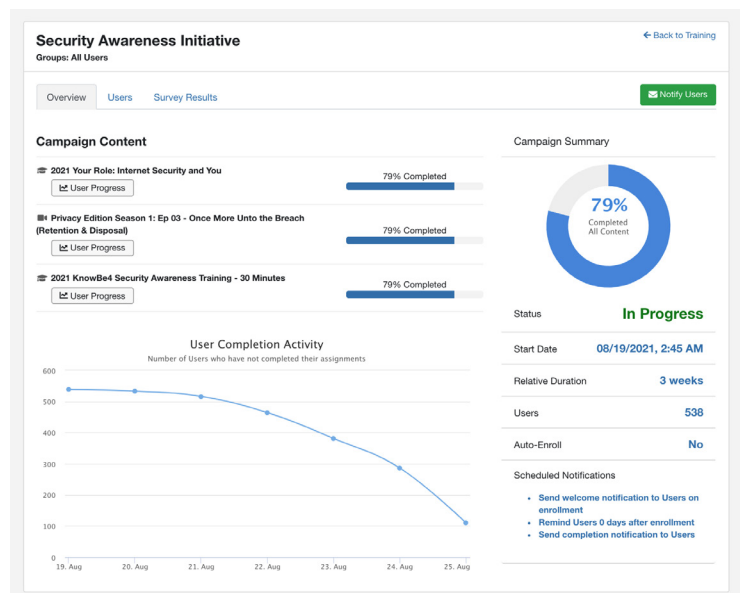
## Training Platform

### Training Campaigns

In the KnowBe4 console, you can quickly create ongoing or time-limited campaigns, select training modules by user groups, auto-enrol new users and automate 'nudge' emails to 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 customise 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 that you choose and manage it alongside your KnowBe4 ModStore Training content all in one place – at no extra cost.



The screenshot shows the 'ModStore' 'Add New Content' form. It includes fields for Content Title, Description, Expected Duration (Minutes), and Artwork. The Artwork field has a 'Choose File' button and a 'No file chosen' status. There are 'Save' and 'Cancel' buttons at the bottom.

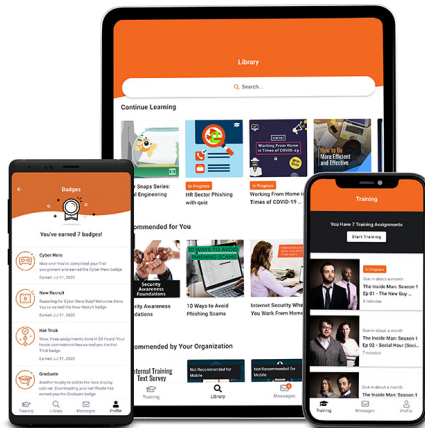
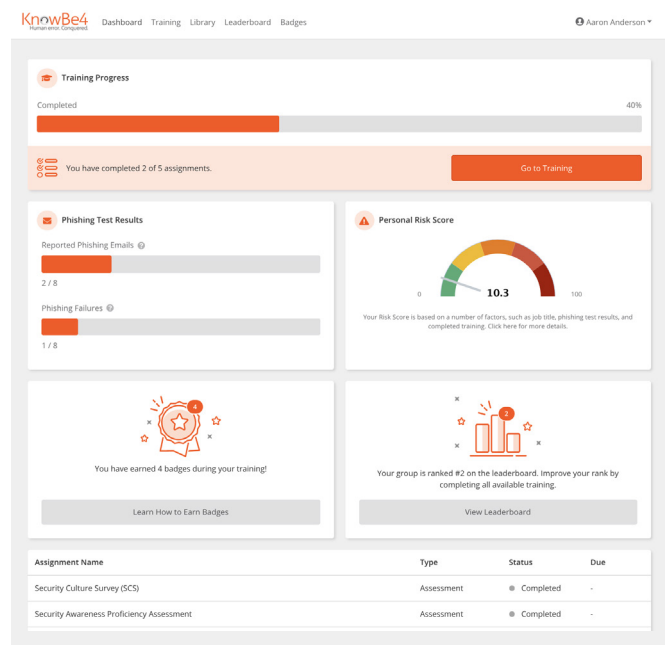


## Learner Experience

KnowBe4's learner experience (LX) adds customisation abilities, as well as engaging and fun gamification to your security awareness training plan.

Your users can compete against their peers on leader boards and earn badges, while learning how to keep themselves and your organisation safe from cyberattacks. An optional, informative tour is also provided to show your users around and to 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 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 and 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 colour, upload a company logo and add an introduction and closing page. These optional pages include your company logo, customised 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 organisation's Branded Certificates onto the KnowBe4 platform. These customised certificates of completion can be made available to your users at the end of each training module.

The screenshot shows the 'ModStore' 'Create Theme' interface. The 'Brandable Content' tab is selected. The 'Theme Settings' section includes:

- Theme Name:** A text field with the value 'New Content Theme (kb4-demo.com) - 25 Aug 2021, 17:02:44'.
- Brand Color:** A color picker showing the selected color '#f26721'.
- Company Logo:** A text field with the value 'Please choose an image file' and a 'Browse' button.

Below the 'Theme Settings' section, there are two optional sections:

- Introduction Page (Optional):** A checkbox that is checked.
- Final Page (Optional):** A checkbox that is checked.

At the bottom, there are 'Create' and 'Cancel' buttons.

## Content Manager

With Content Manager, you can effortlessly customise your training content preferences. 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. Personalised to your organisation's overall Phish-Prone Percentage, the ModStore will present recommended training modules that 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 that 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 to further protect your organisation's largest attack surface – your employees. Introducing a new category of technology called Human Detection and Response (HDR), SecurityCoach helps to strengthen your security culture by enabling real-time coaching of your users in response to their risky security behaviour.

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 when risky behaviour 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 organisation's existing security products with your KnowBe4 console. Your security stack generates alerts that are then analysed by SecurityCoach to identify events related to any risky security behaviour 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 behaviour
- 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 for those that keep repeating risky behaviours.
- Track and report on improved real-world security behaviour across your organisation, 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 the alert noise caused by repetitive risky security behaviours

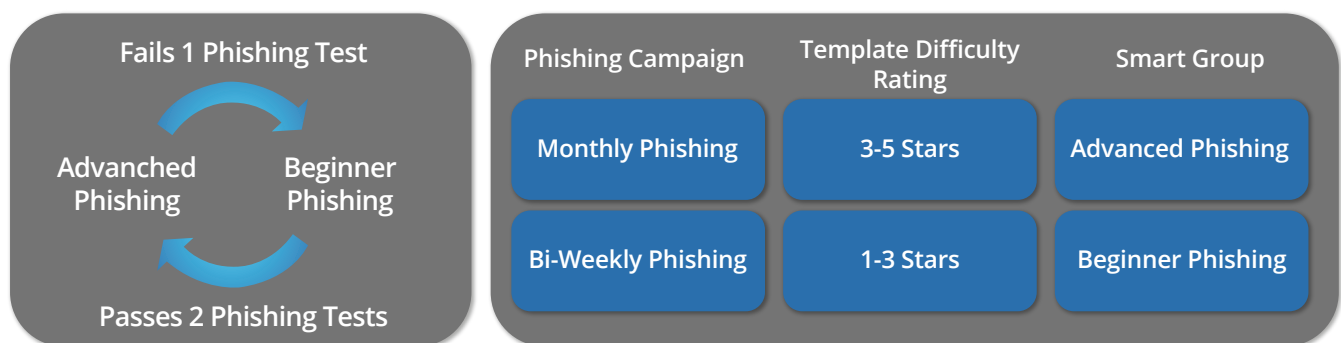
# User Management

## 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, which is available to Platinum and Diamond customers, allows you to deliver dynamic phishing campaigns by creating groups based on the criteria that 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 behavioural 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 that 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 that 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 customisable, which allows for the creation of the exact roles needed by your organisation.

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 only give users access to the portions of the KnowBe4 console that they need 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 an insight into the effectiveness of your security awareness training programme. 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 organisation'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 customised 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.

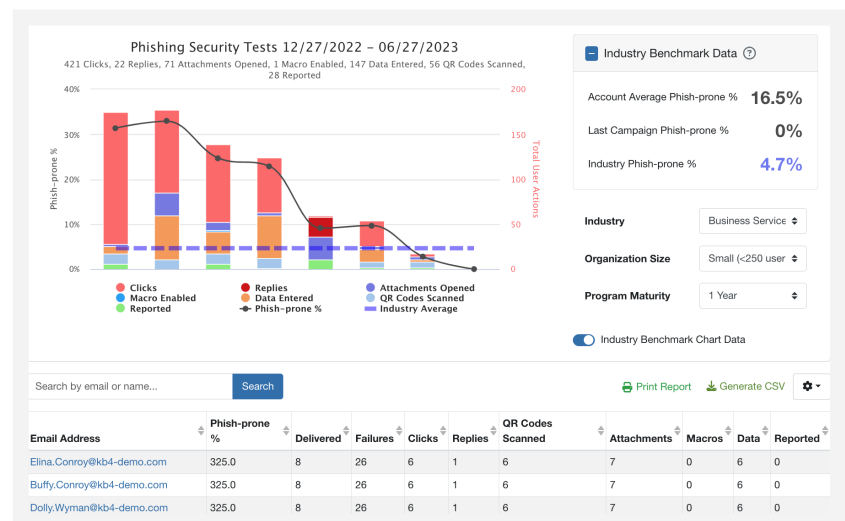
The **Dashboard** of your console contains your organisation's Risk Score and Phishing reports. These reports provide general information about your organisation's Phish-Prone Percentage at the time of the phishing campaign and also your users' actions during the campaign. You can hover over the points 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 totalling 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 and reported phishing emails (emails reported using the Phish Alert Button) or compare results by group.



## 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 just 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

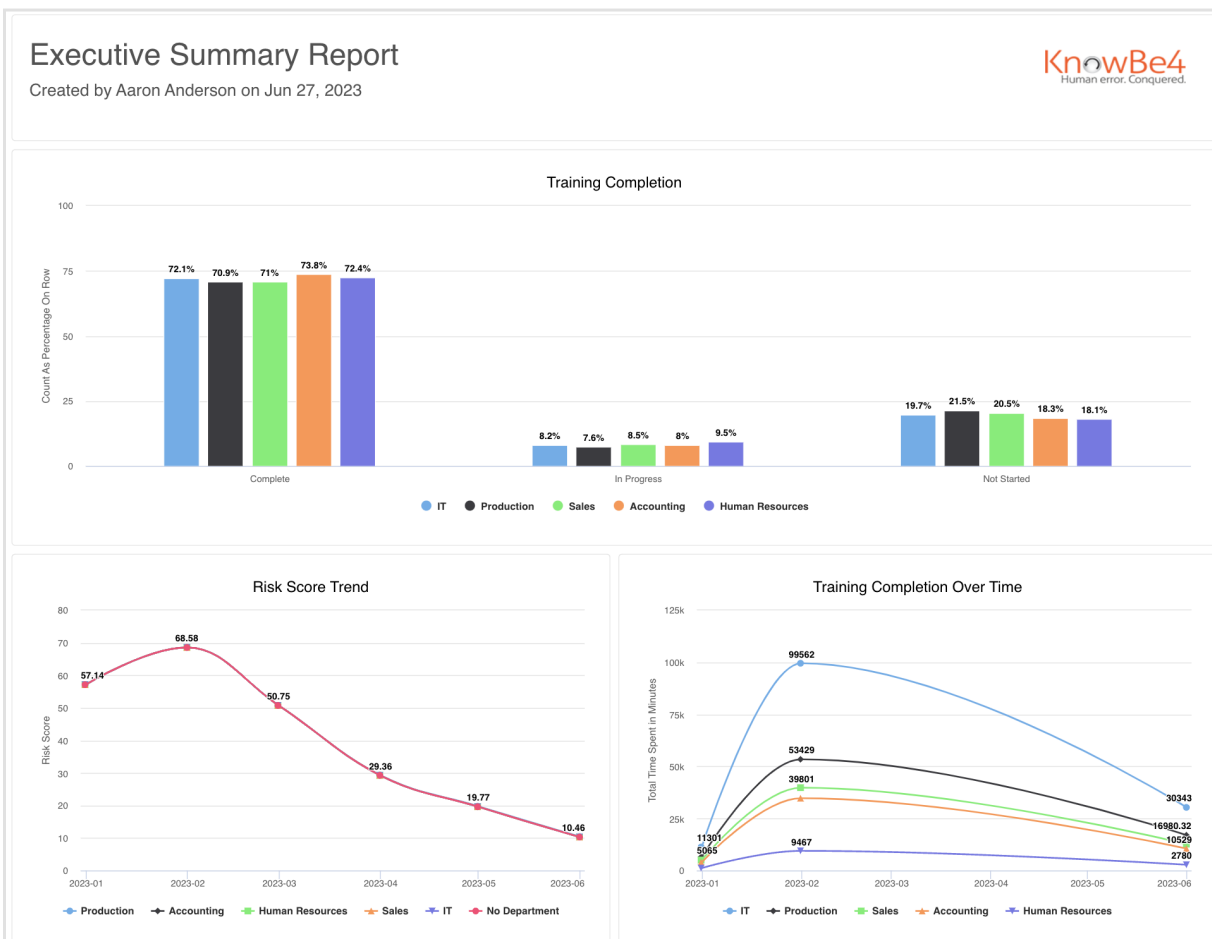
Available in the Gold and above subscription levels, the Email Exposure Check (EEC) Pro tool identifies the at-risk users in your organisation, by crawling business social media information and thousands of breach databases.

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 are: **Very High Risk**, **High Risk** and **Medium Risk**, and are based on how much data was gathered on that specific user.

## Advanced Reporting

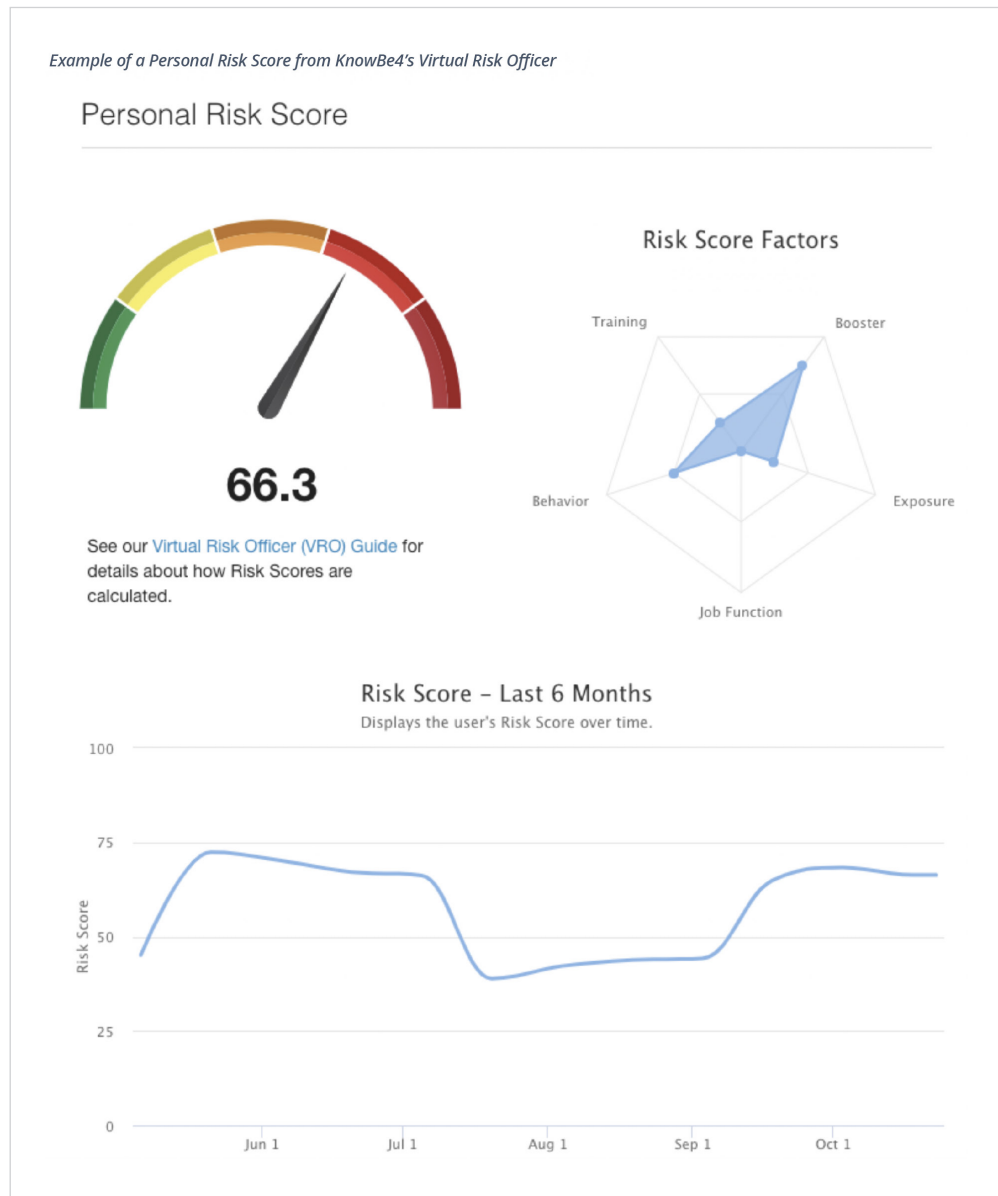
Advanced Reporting provides actionable metrics and insight into the effectiveness of your security awareness training. You can use Advanced Reporting to create many types of reports, to meet the needs of your organisation. This feature comes with a collection of 60+ built-in reports, with insights that provide a holistic view of your entire organisation 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 programme.



## Virtual Risk Officer

The Virtual Risk Officer (VRO) functionality helps you to identify risk at the user, group and organisational 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 organisation 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 and/or 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 organisation 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 in 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 the 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 personalise phishing tests per user, enable AI-Recommended Optional Learning for your users, and use PasswordIQ to continuously monitor your organisation 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, using simulated, real-world 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 programme.

**PhishER Plus:** Available as a stand-alone product or as an optional add-on across all subscription levels. PhishER Plus is a lightweight SOAR platform that automatically analyses and prioritises reported email messages to identify and quarantine malicious emails across an organisation. In addition, it 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 to further protect your organisation's largest attack surface – your employees. Introducing a new category of technology called Human Detection and Response (HDR), SecurityCoach helps to strengthen your security culture by enabling real-time coaching of your users in response to their risky security behaviour.

# ‘Social Engineering is information security’s weakest link.’

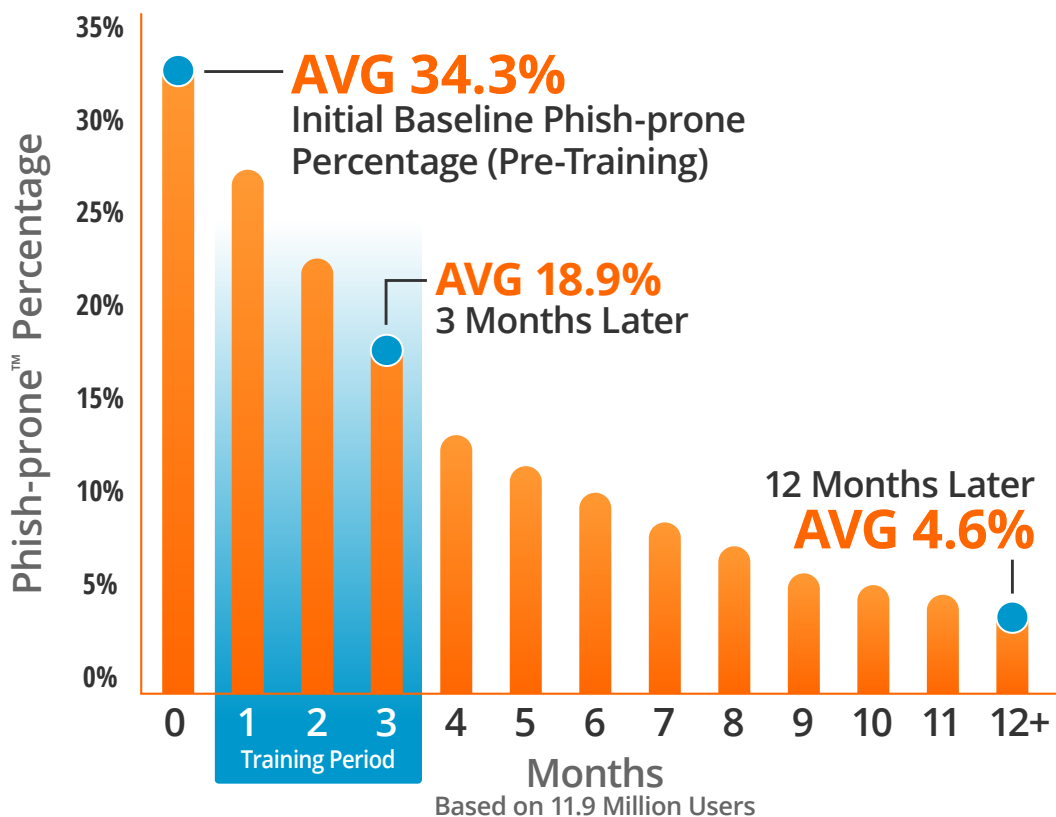
– Kevin Mitnick, ‘The World’s Most Famous Hacker’, IT Security Consultant

## Visible Proof that the KnowBe4 System Works

When you invest in Security Awareness Training and Phishing Security Testing you see value and ROI – quickly.

The results of the 2024 KnowBe4 Phishing Industry Benchmarking Report clearly show where organisations’ 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 minimised 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**  
Human error. Conquered.

KnowBe4 UK, Ltd. | 1 Leeds City Office Park, Leeds, LS11 5BD | Tel: +44 (0) 1347 487512 | [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.