KnowBe4
Human error. Conquered.

Security Awareness Training and Simulated Phishing Platform

Helps you manage the ongoing problem of **social engineering**

KnowBe4 Security Awareness Training

Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
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.
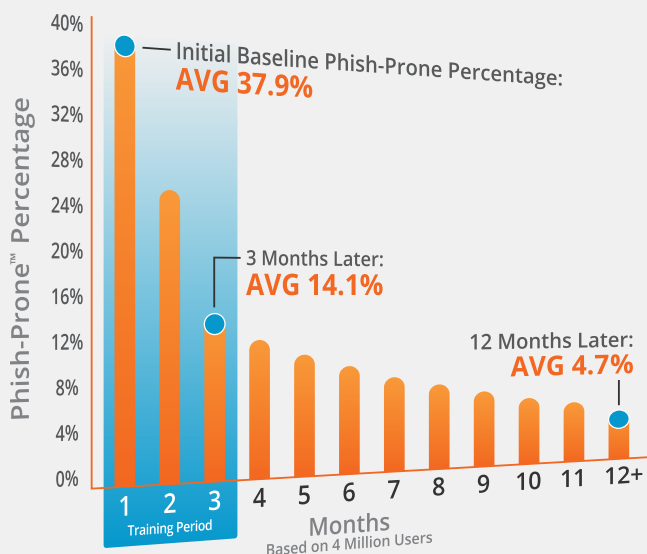
Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

TRAIN · PHISH · ANALYZE

The System Really Works

With KnowBe4's massive database, we analyzed nearly 4 million users over the course of at least 12 months, and our 2020 research continues to uncover alarming results. The overall industry initial Phish-Prone percentage benchmark turned out to be a troubling 37.9%.

Fortunately, the data showed that this 37.9% can be brought down more than half to just 14.1% within 90 days after deploying new-school security awareness training. The results after one year show that by following these best practices, the final Phish-Prone percentage can be minimized to 4.7% on average.

See how your company's Phish-Prone percentage compares to your peers! The **Industry Benchmarking feature** is included with your subscription.

Initial Baseline Phish-Prone Percentage: **AVG 37.9%**

3 Months Later: **AVG 14.1%**

12 Months Later: **AVG 4.7%**

Phish-Prone™ Percentage

Months
Based on 4 Million Users

Training Period

Find Out How **Effective** Our Security Awareness Training Is

KnowBe4 is the world's largest integrated platform for awareness training combined with simulated phishing attacks. Join our tens of thousands of customers who have mobilized their end users as a last line of defense.

KnowBe4 Security Awareness Training Features

Unlimited Use
We offer three Training Access Levels, giving you access to our content library of 1,000+ items based on your subscription level. Unlimited access to all phishing features with flexible licensing. No artificial license ceilings and 10% overage allowance. Powerful new features added regularly.

Engaging, Interactive Browser-based Training
The interactive training gives your users a fresh new learner experience that makes learning fun and engaging. Your users can **choose the language they're most comfortable with** for the entire training interface, helping deliver a more immersive training experience. With the **optional gamification feature**, users can compete against their peers on leaderboards and earn badges while learning how to keep your organization safe from cyber attacks.

Brandable Content
The Brandable Content feature gives you the option to add branded custom content to the beginning and end of select KnowBe4 training modules. This self-service feature enables you to add your organization's branding elements including your logo, custom graphics, and corporate brand colors to tailor any messaging you want to deliver to your users.

Upload Your Own Content
Want to supplement your KnowBe4 security awareness training content with your organization's custom training or other corporate training content? Upload your own SCORM-compliant training and video content and manage it alongside your KnowBe4 ModStore training all in one place—at no extra cost!

Assessments
Find out where your users are in both security knowledge and security culture to help establish baseline security metrics. Use the **skills-based assessment** and the **security culture survey** to measure and monitor your users' security knowledge and sentiment to a security-aware culture over time.

Custom Phishing Templates and Landing Pages
Apart from the thousands of easy-to-use existing templates, you can customize scenarios based on personal information and include simulated attachments to create your own targeted spear phishing campaigns. Each Phishing Email Template can have its own Custom Landing Page, which allows for point-of-failure education.

Phish Alert Button
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!

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

User Management
KnowBe4's **Active Directory Integration** allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes. You can also leverage the **Smart Groups** feature to tailor and automate your phishing campaigns, training assignments and remedial learning based on your employees' behavior and user attributes.

Security Roles
Allows you to define unlimited combinations of level access and administrative ability that you'd like specific user groups to have. With **delegated permissions** you have the ability to limit roles to only display specific data or allow for the phishing, training, and user management of specific groups.

Advanced Reporting Feature
60+ built-in reports provide holistic views and detailed reporting on your key awareness training indicators over time. Leverage Reporting APIs to pull data from your KnowBe4 console and for multiple accounts, Roll-up Reporting makes it easy to view results in aggregate.
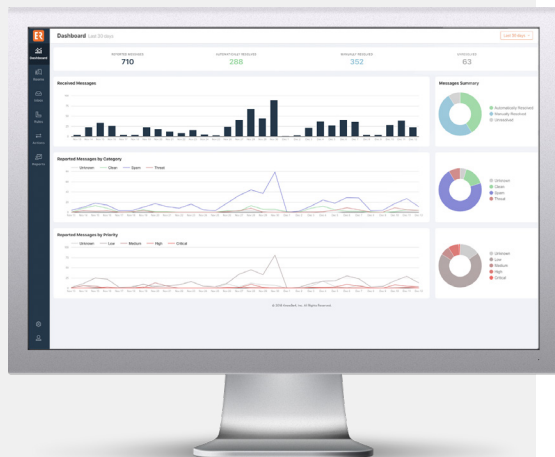
Virtual Risk Officer™
The innovative Virtual Risk Officer (VRO) functionality helps you identify risk at the user, group and organizational level and enables you to make data-driven decisions when it comes to your security awareness plan.

PhishER™
As you phish and train your users they will start reporting potentially dangerous emails to your incident response team. The increase of this email traffic... can present a new problem! PhishER, is an optional add-on for managing the high volume of messages reported by your users and helps you identify and respond to email threats faster.

Identify and respond to email threats faster with PhishER

Because phishing remains the most widely used cyber attack vector, most end users report a lot of email messages they "think" could be potentially malicious to your incident response team. Whether or not you step employees through security awareness training doesn't change the fact that your users are likely already reporting potentially dangerous emails in some fashion within your organization. **The increase of this email traffic … can present a new problem!**

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

What is PhishER?

PhishER is your lightweight SOAR platform to orchestrate your threat response and manage the high volume of potentially malicious email messages reported by your users. And, with automatic prioritization of emails, PhishER helps your InfoSec and Security Operations teams cut through the inbox noise and respond to the most dangerous threats more quickly.

Additionally, with PhishER you are able to automate the management of the 90% of reported emails that are not threats. Incident Response (IR) orchestration can easily deliver immediate efficiencies to your security team, but the potential value is much greater than that. With the right strategy and planning, your organization can build a fully orchestrated and intelligent SOC that can contend with today's threats.
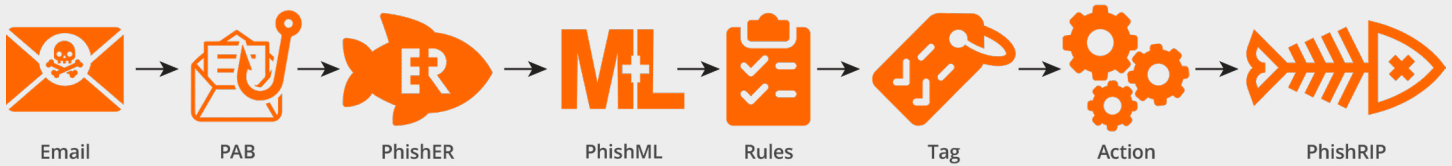
PhishER is a critical element to help your IR teams work together to mitigate the phishing threat and is suited for any organization that wants to automatically prioritize and manage potentially malicious messages - accurately and fast! PhishER is available as a stand-alone product or as an add-on option for KnowBe4 customers.

Why Choose PhishER?

PhishER is a simple and easy-to-use web-based platform with critical functionality that serves as your phishing emergency room to identify and respond to user-reported messages. PhishER helps you prioritize and analyze what messages are legitimate and what messages are not—quickly.

With PhishER, your team can prioritize, analyze, and manage a large volume of email messages—fast! The goal is to help you and your team prioritize as many messages as possible automatically, with an opportunity to review PhishER's recommended focus points and take the actions you desire.

Key Benefits

- Full integration with KnowBe4's Phish Alert Button allows automatic prioritization of emails that are not threats

- Cut through the IR-inbox noise and respond to the most dangerous threats more quickly and efficiently

- Free up IR 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

- Meet critical SLAs within your organization to process and prioritize threats and legitimate emails

- Automated email response templates let you quickly communicate back to your employees about the emails they need in order to continue working

- You can create custom workflows for tasks such as prioritization and alerting so that the IR team can focus on the right messages

How PhishER Works

Email	PAB	PhishER	PhishML	Rules	Tag	Action	PhishRIP

PhishER processes user-reported phishing and other suspicious emails by grouping and categorizing emails based on rules, tags, and actions. PhishML, the custom machine-learning module, analyzes messages and generates confidence values which are used to tag messages. PhishRIP helps you easily find and quarantine suspicious messages still sitting in mailboxes across your entire organization.

Automatic Message Prioritization

PhishER will help you prioritize every reported message into one of three categories: Clean, Spam, or Threat. Through rules you set, PhishER helps you develop your process to automatically prioritize as many messages as possible without human interaction.

With automatic prioritization of emails that are not threats, PhishER helps your team respond to the most dangerous threats more quickly. PhishER easily integrates with KnowBe4's email-add in button, Phish Alert and also works by forwarding to a dedicated mailbox.

Emergency Rooms

PhishER features "Emergency Rooms" to help you identify similar messages reported by your users. Emergency Rooms consist of pre-filtered views of your messages that are unresolved in your PhishER inbox. These messages are dynamically grouped by commonalities and include system pre-filtered views for messages by Top Subject Lines, Top Senders, Top Attachments, and Top URLs.

Each room is interactive, allowing you to drill down into filtered inbox views of the messages and take action across all associated messages at the same time.

SIEM Integrations

PhishER integrates into your organization by pushing data into popular SIEM platforms such as Splunk and QRadar. With support for multiple syslog destinations available it's also possible to push data into as many other systems as you like.

PhishML™

PhishML is a PhishER machine-learning module that helps you identify and assess the suspicious messages that are reported by your users, at the beginning of your message prioritization process. PhishML analyzes every message coming into the PhishER platform and gives you the info to make your prioritization process easier, faster, and more accurate.

PhishML is constantly learning based on the messages that are tagged, not only by you but also by other members of the PhishER user community! That means that the learning model is being fed new data to constantly improve its accuracy and more messages can be automatically prioritized based upon PhishER categorization, saving you even more time.

Simple and Advanced Rule Creation

You can create custom rules, use the built-in YARA-based system rules, or edit existing YARA rules. You can use system rules to help simplify your rules requirements or copy and modify to customize rules depending on the proficiency of your incident response team.

Data Enrichment Intelligence

PhishER integrates with external services like VirusTotal to help analyze attachments and malicious domains. Using URL Unwinding, PhishER automatically expands shortened URLs to help see the potential threat level of the final destination.

PhishRIP™

PhishRIP is an email quarantine feature that integrates with Microsoft Office 365 to help you remove, inoculate, and protect your organization against email threats so you can shut down active phishing attacks fast.

PhishRIP looks at any user-reported message in PhishER and searches and optionally quarantines similar messages across all your users' mailboxes. Any messages found are then ready for further analysis, quarantine, or permanent deletion by your incident response team.
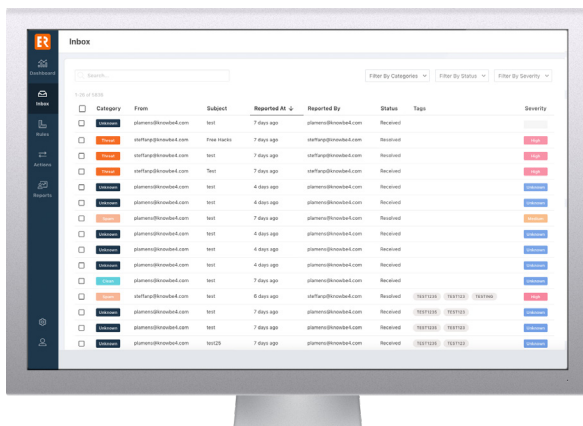
KnowBe4 Subscription Levels

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

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

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 900+ items including interactive modules, videos, games, posters and newsletters. In addition, you will have access to our cutting-edge Artificial Intelligence-driven Agent (AIDA™), currently in beta that allows for simulated multi-faceted social engineering attack using email, phone, and SMS messaging. (available for U.S. and Canada)

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