KnowBe4
Human error. Conquered.

Security Awareness Training and Simulated Phishing Platform

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

KnowBe4 Security Awareness Training

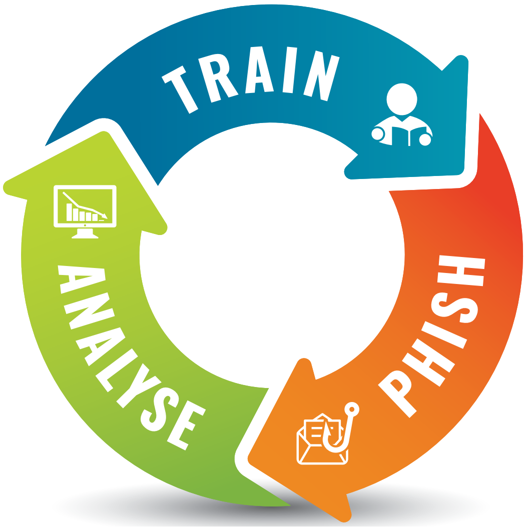
Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

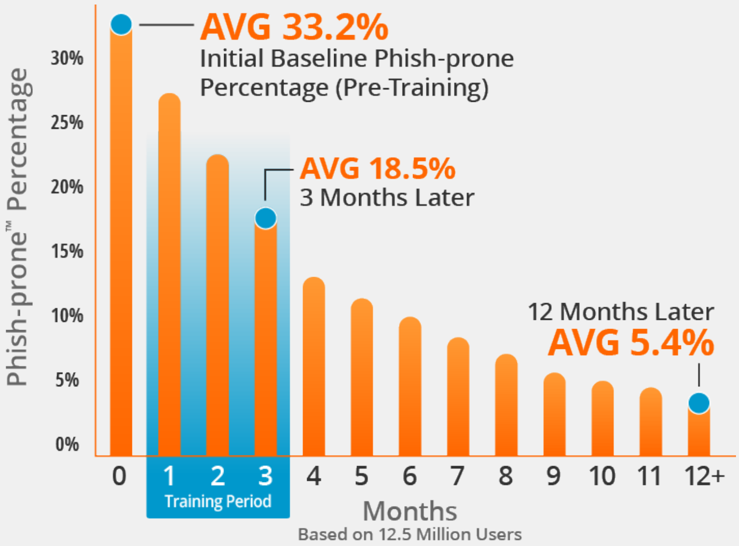
Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

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!





The System Really Works

With KnowBe4's massive database, we analyzed over 12.5 million users over the course of at least 12 months, and our 2023 research continues to uncover alarming results. The overall industry initial Phish-prone Percentage benchmark increased to 33.2%, up nearly one full point from 2022.

Fortunately, the data showed that this 33.2% can be brought down to 18.5% within 90 days after 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 5.4% on average.

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

Source: 2023 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.

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 mobilised their end users as a last line of defence.

KnowBe4 Security Awareness Training Features

Unlimited Use

We offer three Training Access Levels via the KnowBe4 ModStore, 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. Powerful new features added regularly.

Localized Admin Console and Learner Experience

You can set your default language for three localization settings: Phishing, Training, and Admin Console Language. With these localization options, you can enable your Admins to manage the KnowBe4 console in one of ten languages, while delivering a more immersive training experience for your learners in over 34 languages.

Brandable Content

This self-service feature gives you the option to add branded custom content to the beginning and end of select KnowBe4 training modules. You can add your organisation's branding elements including your logo, custom graphics, and corporate 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 organisation's custom training or other corporate training content? With KnowBe4's robust learning management system (LMS), you can upload your own SCORM-compliant training and video content and manage it alongside your KnowBe4 ModStore Training content 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 tens of thousands of easy-to-use system 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.

AI-Driven Phishing and Training Recommendations

Leverage the power of AI to give your users a more personalized experience that adapts to their current level of knowledge. Use AI-driven phishing to automatically choose the best phishing template for each of your users based on their individual training and phishing history. With AI-driven training recommendations, the KnowBe4 ModStore serves up training content customized to your overall organisation's Phish-prone percentage.

User Management

KnowBe4's Active Directory or SCIM 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.

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.

Virtual Risk Officer™

The innovative Virtual Risk Officer (VRO) functionality uses machine learning to help you predict and identify risk at the user, group and organisational level. This continual learning model enables you to make data-driven decisions when it comes to your security awareness program.

PhishER™

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. Combined with the KnowBe4 training platform, PhishER can automatically flip dangerous attacks into instant real-world training opportunities when you use PhishFlip together with the KnowBe4 platform.

Did you know that 88% of data breaches are caused by human error?

Get your free phishing security test and find out what percentage of your employees are Phish-prone

www.KnowBe4.com/PST

KnowBe4 UK, Ltd. | Osprey and Kestrel, The Hawkhills Estate, Easingwold, York YO61 3FE | Tel: +44 (0) 1347 487512 | www.KnowBe4.com | Email: Sales@KnowBe4.com

PhishER PLUS

Key benefits

- Full integration with KnowBe4's Phish Alert Button allows automatic prioritisation 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 time and resources to identify and manage the 90% of messages that are either spam or legitimate email by reducing the volume of emails that your SOC team has to remediate
- Block email threats that have bypassed all other email security filters or systems before they reach your users' inboxes
- Isolate malicious emails that already bypassed your mail filters through automated quarantine using Global PhishRIP
- Crowdsource threat intelligence from 10+ million KnowBe4-trained users
- Leverage the power of triple-validated threat intelligence to protect your organisation from new attacks
- See clusters or groups of messages based on patterns that can help you to identify a widespread phishing attack against your organisation
- Automated email response templates let you quickly communicate back to your employees about the emails they need in order to continue working
- Create custom workflows for tasks such as prioritisation and alerting so that the IR team can focus on the right messages

Supercharge your anti-phishing defence with PhishER Plus

Email threats get more sophisticated every year. Worrying percentages make it past your secure email gateway (SEG) and into your users' inboxes. Social engineering attacks increasingly target your high-risk users. The 2023 Verizon Data Breach Investigations Report shows that email alone is the highest cause of data breaches. Researchers at ArmorBlox recently reported that 56% of all attacks bypass your legacy security filters. The upshot? Legacy email security layers let these digital time bombs slip into the inboxes of your users.

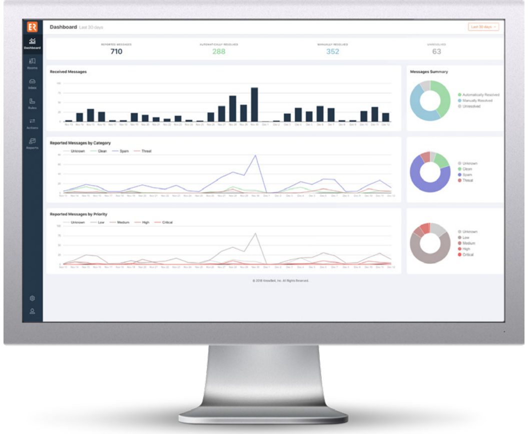
Revolutionary proactive anti-phishing defence

PhishER Plus is the most powerful anti-phishing protection available in the world. PhishER Plus is powered by a unique KnowBe4 global threat feed. This triple-validated phishing threat feed automatically blocks phishing attacks *before* they make it into your users' inboxes by using:

1. KnowBe4's global network of 10+ million highly trained end users and their PhishER administrators
2. PhishML, a unique AI model trained on phishing emails that all other filters missed
3. Human-curated threat intel by KnowBe4's Threat Research Lab

KnowBe4 sees things that no one else can. Users report all the attacks that make it through every other filter out there. These in-the-wild threats are the most dangerous, real-time social engineering attacks at any given point in time.

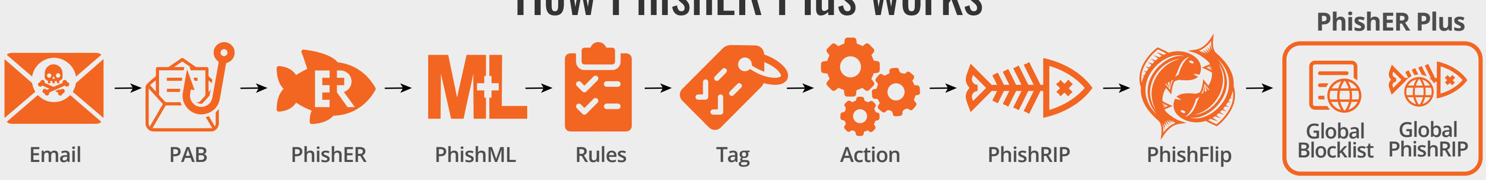
How PhishER Plus works



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! PhishER Plus is available as a standalone product or as an add-on option for KnowBe4 customers.

How PhishER Plus works



Automatic Message Prioritisation

PhishER Plus helps you to prioritise every reported message into one of three categories: Clean, Spam or Threat. Using YARA rules, you assign what's most important to you and PhishER Plus helps to develop a process to automatically prioritise as many messages as possible without human interaction. PhishER Plus helps your team to respond to the most dangerous threats more quickly by reviewing the attributes of reported messages and ranking the most critical messages based on priority.

Emergency Rooms

Emergency Rooms help you to identify similar messages reported by your users. PhishER Plus groups these messages by commonalities and includes pre-filtered views for messages by top subject lines, top senders, top attachments and top URLs. Each Emergency Room is interactive, allowing you to drill down into filtered inbox views and take action across all related messages.

Integrations

With PhishER Plus's API integration and support for multiple syslog destinations, you can connect PhishER Plus with your existing security stack products to push data into popular email security, threat intelligence, ticketing and SIEM platforms. Additionally, you can send events from PhishER Plus and add them to your users' timelines in your KnowBe4 platform. You can use these events to help tailor specific phishing and training campaigns that enable your users to better identify and report suspicious emails through the Phish Alert Button. PhishER Plus also integrates with external services such as VirusTotal to help analyse attachments and malicious domains.

Human-Vetted Threat Intelligence

There is strength in numbers. Leverage the power of the KnowBe4 Threat Research Lab and KnowBe4's end-user network around the world to help protect against new and evolving phishing and social engineering attacks.

Microsoft 365 Global Blocklist

With the PhishER Plus Global Blocklist feature, it's easy to create your organisation's unique list of blocklist entries and dramatically improve your Microsoft 365 email filters without ever leaving the PhishER Plus console. Blocklist entries of validated threats crowdsourced from 10+ million trained users are leveraged to automatically block matching new incoming messages from reaching your users' inboxes. This continually updated threat feed is managed by KnowBe4 and syncs with your Microsoft 365 mail server. Alternatively, you can utilise your own private blocklist for Microsoft 365 instead of crowdsourcing.

PhishML™

PhishML is a PhishER Plus machine-learning module that helps you to identify and assess the suspicious messages that are reported by your users, at the beginning of your message prioritisation process. PhishML analyses every message coming into the PhishER Plus platform and gives you the info to make your prioritisation 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 Plus user community! This means that the learning model is being fed new data to constantly improve its accuracy. More messages can be automatically prioritised based upon PhishER Plus categorisation, saving you even more time.

Global PhishRIP™

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.

Global PhishRIP enables you to remove an identified threat from all user inboxes, inoculate unreported threats and protect against future threats by deleting, quarantining or restoring legitimate email. 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. These messages are automatically quarantined by removing them from all of your users' inboxes.

PhishFlip™

PhishFlip is a PhishER feature that automatically turns user-reported phishing attacks targeted at your organisation into safe, simulated phishing campaigns in your KnowBe4 platform. With PhishFlip, you can now immediately 'flip' a dangerous attack into an instant real-world training opportunity for your users.

Crowdstrike Falcon Sandbox Integration

This integration allows admins with a CrowdStrike Falcon Sandbox licence to investigate potentially malicious files faster, and more efficiently, all from a single console. CrowdStrike Falcon Sandbox is a malware analysis tool that provides a safe way to analyse files and URLs for malicious content in a protected, sandbox environment.

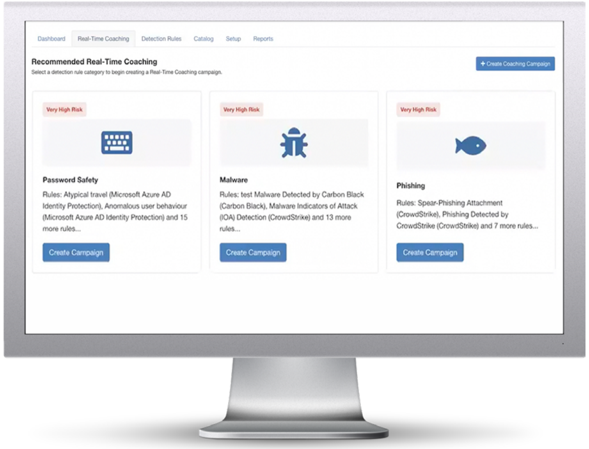
PhishER Plus integrates AI-validated human intelligence crowdsourced from among the best trained and most technically diverse user sets on the planet: KnowBe4's own customers representing more than 65,000 organisations and over 55 million total users. **It's simple. Together we are stronger.**

SecurityCoach

KnowBe4
Human error. Conquered.

Deliver Real-Time Coaching in Response to Risky User Behaviour

Improve the overall security culture and reduce risk



Recommended Real-Time Coaching

Select a detection rule category to begin creating a Real-Time Coaching campaign.

Password Safety

Rules: Atypical travel (Microsoft Azure AD Identity Protection), Anomalous user behaviour (Microsoft Azure AD Identity Protection) and 15 more rules...

Malware

Rules: test Malware Detected by Carbon Black (Carbon Black), Malware Indicators of Attack (IOA) Detection (CrowdStrike) and 13 more rules...

Phishing

Rules: Spear-Phishing Attachment (CrowdStrike), Phishing Detected by CrowdStrike (CrowdStrike) and 7 more rules...

With the ongoing problem of social engineering attacks, bad actors try to exploit your users by looking for any way to breach your organisation's cybersecurity defence layers. According to the 2022 Verizon Data Breach Investigations Report, the human factor is involved in 82% of breaches. And your overwhelmed, stressed-out security teams need relief from the alert noise caused by the repetitive risky behaviours of your employees.

What if you could take user event data detected by your existing security stack and use it to deliver real-time coaching to your users in response to their security mistakes, while also reducing the volume of alert noise for your Security Operations Centre (SOC) team caused by those repetitive risky behaviours? **Now you can with SecurityCoach™.**

Key Benefits

- 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.
- Measure and report on improved real-world security behaviour across your organisation, providing a justification for continued investment
- Reduce the burden on your SOC and improve efficacy by decreasing the alert noise caused by repetitive risky security behaviours

What is 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.**

SecurityCoach helps to strengthen your security culture by enabling real-time security coaching of your users in response to their risky security behaviour. By leveraging your existing security stack, you can configure real-time coaching campaigns to immediately deliver contextual SecurityTips that reinforce your security awareness training and policies for your users. This improves knowledge retention and helps users to understand the risks associated with their behaviours.

SecurityCoach integrates with KnowBe4's new-school security awareness training platform and your existing security stack to deliver real-time coaching in response to risky end-user security behaviour.

Why Choose SecurityCoach?

Your organisation is facing an ever-increasing volume of social engineering attacks targeting your users. Your best defence is to develop a strong security culture across your organisation that engages your users and reinforces the importance of following your organisation's security policies, strengthening your human firewall.

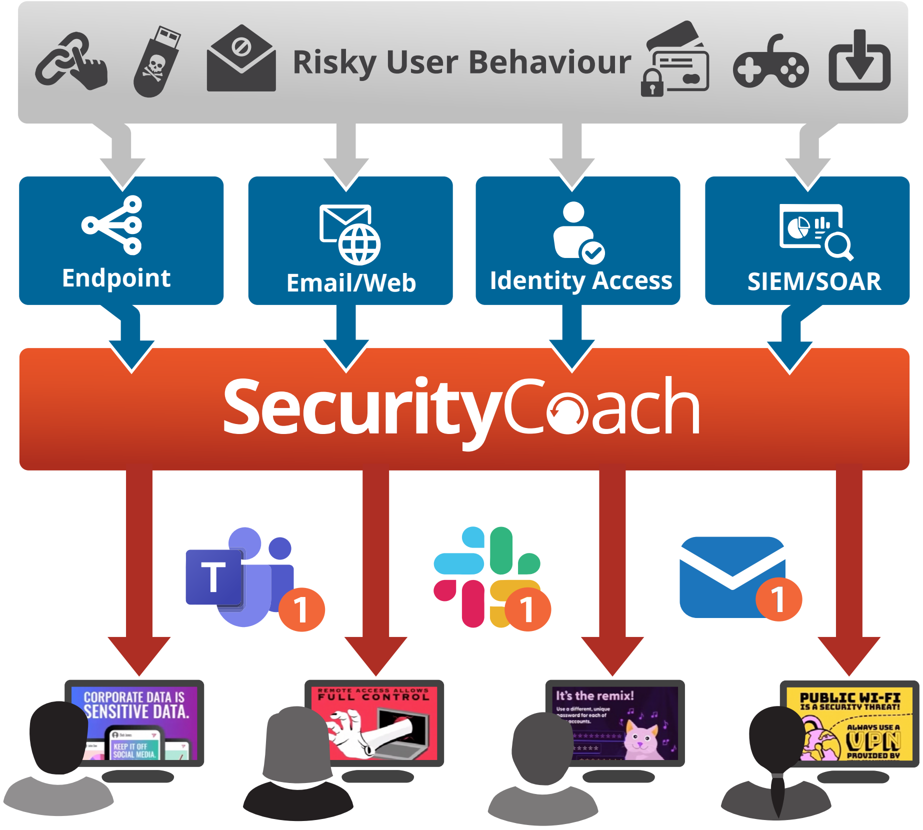
SecurityCoach creates significant time savings for your overburdened SOC team by reducing the volume of alert noise caused by repetitive risky behaviours, allowing the SOC to focus on high-priority threats.

How Does SecurityCoach Work?

SecurityCoach uses standard APIs to quickly and easily integrate with your existing security products from vendors such as Microsoft, CrowdStrike, Cisco and dozens of others. Your security stack generates alerts that are then analysed by SecurityCoach to identify events related to any risky security behaviour from your users.

For example, if a user opens an infected email attachment that might spread ransomware in your network, or tries to visit a website with restricted content on their work computer, your security products detect this and create an event alert. SecurityCoach identifies that event and then, via Microsoft Teams, Slack or email, sends a real-time SecurityTip to that user acknowledging that 'Hey, this is a security risk and here's why.' You can set up coaching campaigns to target risky users based on those events from your network, identity, web security and other vendors within your security stack. These campaigns enable you to coach your users at the moment when the risky behaviour occurs, providing real-time feedback and reinforcing the security awareness training campaigns that you run today. Using your own security policies as a foundation, and assisted by SecurityCoach automation settings, you can easily configure real-time coaching campaigns.

SecurityCoach reinforces the need to follow your organisation's security policies, improving user behaviour and strengthening your overall security culture.


Risky User Behaviour
Endpoint
Email/Web
Identity Access
SIEM/SOAR
SecurityCoach
1
1
1
CORPORATE DATA IS SENSITIVE DATA.
KEEP IT OFF SOCIAL MEDIA.
REMOTE ACCESS ALLOWS FULL CONTROL
It's the remix!
PUBLIC WI-FI IS A SECURITY THREAT!
ALWAYS USE A VPN PROVIDED BY

SecurityCoach Workflow

1. The security stack vendors that you integrate with your KnowBe4 console will monitor for risky activity on your users' devices.
2. Then, alert data is shared with SecurityCoach. SecurityCoach will analyse your alerts and determine which threats provide the best opportunities to coach your users in real time.
3. When risky user behaviour is detected, SecurityCoach automatically sends a real-time SecurityTip notification to that user via Microsoft Teams, Slack or email.

Key Features

Real-Time Coaching

Real-time coaching campaigns allow you to coach your users about risky behaviour in real time. When risky activity is detected, your users will receive a coaching notification with a SecurityTip about the activity and how to avoid it in the future.

SecurityTip Notifications

At the moment when risky behaviour is detected, SecurityCoach sends a real-time SecurityTip directly to that user via Microsoft Teams, Slack or email. These immediate notifications are a powerful enhancement to your security awareness programme.

API-Based Integrations

Utilise vendor APIs to quickly and easily integrate with your existing security stack vendors such as Microsoft, Cisco, Netskope, Zscaler and more. Our ecosystem of technology partnerships is rapidly expanding to support our customers and strengthen the human firewall.

Built-In Detection Rules

Detection rules specify what risky activity you want to track using the data provided by your integrated security vendors. SecurityCoach recommends detection rules based on the most common security topics in order of priority, with ‘Very High’ and ‘High Risk’ rules presented first.

Campaign Recommendations

SecurityCoach recommends real-time coaching campaigns best suited for your detection rules. You can select SecurityTips from different categories of risky behaviour.

Easy User Mapping

User data from your identity provider or directory is combined with your security event logs to create user mapping rules. With a variety of built-in user mapping rules and the ability to create custom rules, you can easily configure these rules to automatically map users.

Dashboard and Detailed Reporting

The built-in dashboard provides an overall summary of your coaching campaigns, detection rules and detected security events. The detailed reports provide insights into your organisation’s security risks and help to track trends in your users’ risky activity over time.

Rule-Based Automation

Based on the rules in your existing security software stack and defined high-risk users or roles, you can configure your real-time coaching campaign to determine the frequency and type of SecurityTips that risky users will receive.

Robust SecurityTip Catalogue

You can create campaigns using our extensive and continually growing catalogue of 200 SecurityTips covering 60 different topics, many of which are available in 34 languages.

Powerful Security Integrations

SecurityCoach uses standard APIs to quickly and easily integrate with your existing security products from vendors such as CrowdStrike, Microsoft, Cisco, Netskope, Zscaler and more. Our ecosystem of technology partnerships is rapidly expanding to support our customers and strengthen the human firewall.

To allow SecurityCoach access to your security platforms, you'll set up an integration in your KnowBe4 console. These integrations allow SecurityCoach to track when certain actions are detected. Setting up an integration is a quick and easy process, and we provide integration guides for each vendor on our knowledge base. Once integrated, events and other data from your security platforms will be displayed on your SecurityCoach dashboard.

Endpoint Security	Carbon Black. CROWDSTRIKE CYLANCE Microsoft SONICWALL SentinelOne Malwarebytes SOPHOS
Identity and Access Management	Google okta Microsoft
Communications	slack Microsoft Teams
Email and Web Security	cisco Google Microsoft netskope proofpoint. zscaler CLOUDFLARE

To learn more about how these vendor integrations work with SecurityCoach, visit www.knowbe4.com/integrations.

Compliance Plus

KnowBe4
Human error. Conquered.

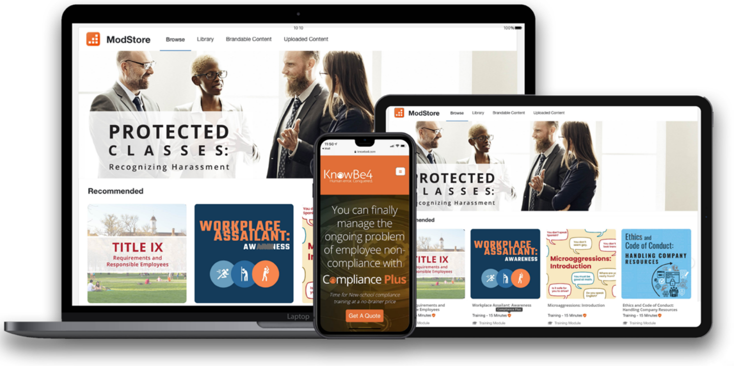
Compliance Plus training is interactive, relevant and engaging with real-life simulated scenarios to help teach your users how to respond in challenging situations. Created in collaboration with legal experts to provide your organization accurate, up-to-date content on compliance topics that require training that sticks.

Compliance Plus gives you:

- A whole new library with 400+ items of fresh compliance content updated regularly
- Full coverage of legislative and data privacy requirements, such as HIPAA, PCI, GDPR and many others
- New-school, high-quality brandable modules with the ability to include your organization's policies and procedures
- Short, interactive modules to keep learners focused
- The ability to upload your organization's custom SCORM-compliant training and video content to the KnowBe4 LMS
- Supplemental learning aids such as newsletters, documents and posters are all included
- Completely automated compliance training campaigns with world-class support and extensive reporting

Finally, you can deliver employee compliance training that is engaging, relevant and makes learning fun!

Compliance Plus is new-school compliance training at a no-brainer price


ModStore
PROTECTED CLASSES:
Recognizing Harassment
Recommended
TITLE IX
Requirements and Responsible Employees
WORKPLACE ASSAILANT:
AWARENESS
KnowBe4
You can finally manage the ongoing problem of employee non-compliance with Compliance Plus
Get A Quote
Microaggressions: Introduction
Ethics and Code of Conduct:
HANDLING COMPANY RESOURCES

Is your compliance training putting your organization at risk?

We know that delivering effective compliance training has been a struggle for Risk, Compliance, and HR executives for years. Boring training is easily forgotten, unrelatable, and rarely completed. Without sufficient training, employees may not understand security risks or violations of the law, and an inadequately trained workforce can quickly become a major liability. Once your employees learn how to identify these scenarios, they are more likely to report harassment, discrimination or failure to accommodate reasonable requests.

Compliance Plus goes beyond simply checking the box, it's also a catalyst for behavior change and minimizing risk.

Compliance Plus is "new-school" training that is fresh and educational with live-action video scenarios and interactive aids to help your users recognize and identify situations and issues that threaten the compliance landscape in your workplace. Our team consults with legal experts to provide the most current, relevant content covering statutory and regulatory changes in compliance topics while maintaining our high standards for quality and learner retention and engagement.

Up until now, compliance training has had a reputation for being time-consuming to build, expensive to buy, and difficult to deliver effectively. Compliance Plus makes it easy to provide concise, relevant, memorable training at a no-brainer price.

Time for new-school compliance training: Meet Compliance Plus

Compliance Plus Training Topics Include:

Business Ethics

Our business ethics training content allows you to educate your users on the key legal requirements and ethical principles involved in working for your organization. The goal is to set a solid ethical framework and foundation to orient employees to do the right thing.

Data Privacy

Our data privacy training content lays out the importance of data privacy, the inherent risk of mishandling personal data, and the potential consequences of non-compliance with data privacy rules, such as HIPAA, FERPA, PCI, GDPR and more.

Data Protection

The overall goal of these courses is to create informed employees that can identify personally identifiable information (PII), understand how to handle it, and make better privacy decisions that ultimately reduce risk to your organization.

Diversity, Equity & Inclusion

Our diversity, equity and inclusion content meets learners exactly where they are in their DEI journey. Our training on topics such as unconscious bias and inclusive language serves as a catalyst for behavior change by providing information that is informative, relatable and thought provoking.

Employment Law

Our employment law training covers the federal and state laws that govern the workplace, including topics like discrimination, harassment, wage and hour laws, FMLA, and reasonable accommodations under the ADA.

Harassment and Discrimination

Our anti-discrimination training content teaches your users what discrimination looks like, how to avoid and stop it, and what steps managers should be taking to ensure a respectful and encouraging workplace for all. Our harassment prevention training covers sexual harassment and other harassment prevention topics like protected classes, Title IX and more.

Workplace Safety

Creating a safe workspace begins with training employees on how to identify potential hazards and what to do to address them. From preparing for a workplace assailant to preventing workplace injuries, our training offers best practices to maintain a safe and productive work environment.

Professional Development

Employees are better served when they feel their organization is invested in improving their skills and experience. To that end, our professional development training offers varied opportunities to provide courses on corporate process improvements, efficiencies and other related topics.

The End of Expensive, Time-Consuming Compliance Training is Here

When you combine the power of the KnowBe4 platform with Compliance Plus, your organization can set up a fully automated compliance training program in a matter of minutes for a no-brainer price!

Compliance Plus can help you better equip your users with the knowledge and awareness to comply with regulatory laws, protect themselves and the organization from unprofessional and unsafe work environments, and safeguard your organization's reputation.

The Compliance Plus library is available as an add-on across any existing KnowBe4 Subscription Level.

For more information, visit: www.KnowBe4.com/compliance-plus

For more information, visit: www.KnowBe4.com/compliance-plus

KnowBe4
Human error. Conquered.