KnowBe4
Human error. Conquered.

Guia do Comprador

Treinamento de conscientização em segurança e plataforma de simulação de phishing

Guia do Comprador: Treinamento de conscientização em segurança e plataforma de simulação de phishing

Sumário

A KnowBe4 é a maior plataforma integrada do mundo de treinamento de conscientização em segurança e simulação de phishing. Confira neste guia:

- por que o treinamento de conscientização em segurança é necessário;
- o que a plataforma KnowBe4 oferece;
- atributos essenciais que todo fornecedor de treinamento de conscientização em segurança deve oferecer.

O problema contínuo da engenharia social

Seus funcionários são o elo fraco na segurança de TI, e a engenharia social é a principal ameaça à segurança de qualquer organização. O crescimento dos ataques cibernéticos sofisticados é alarmante e apenas torna o problema ainda pior, já que os criminosos cibernéticos sempre escolhem os frutos mais fáceis de pegar: os funcionários. Conforme constatado em uma infinidade de relatórios e white papers, o número de ataques cibernéticos aos quais as organizações foram expostas nos últimos cinco anos cresceu de forma maciça.

Com seus funcionários na mira dos agentes de ameaças, os treinamentos de conscientização em segurança tornam-se mais do que necessários. O treinamento de conscientização em segurança é uma forma de educar e fornecer aos membros de uma organização as informações necessárias para protegerem a si mesmos e aos ativos de suas empresas contra perdas ou danos.

O objetivo do treinamento de conscientização em segurança é equipar os funcionários com o conhecimento necessário para combater essas ameaças. Não se pode esperar que os funcionários conheçam as ameaças existentes ou saibam como lidar com elas por conta própria. Os funcionários precisam saber o que suas empresas consideram arriscado ou aceitável, como identificar pistas que indiquem a presença de ameaças e como agir quando se virem diante de uma delas.

"As pessoas estão acostumadas a confiar em soluções tecnológicas, [mas] a engenharia social burla todas as tecnologias, incluindo firewalls. A tecnologia é algo importante, porém precisamos ficar atentos a pessoas e processos. A engenharia social é uma forma de ataque que utiliza táticas de influência."

— Kevin Mitnick

A abordagem da KnowBe4: aplicar phishing, treinar, analisar

A KnowBe4 ajuda dezenas de milhares de clientes a lidar com o constante problema da engenharia social. Temos a maior biblioteca mundial de conteúdo de treinamento de conscientização em segurança, abrangendo desde módulos interativos a vídeos, jogos, pôsteres e boletins informativos, e nossa missão é capacitar seus funcionários a tomar decisões mais inteligentes sobre segurança no dia a dia.

A vantagem competitiva da KnowBe4 é dupla. Primeiro, utilizamos uma grande variedade de ferramentas e feeds de informações para oferecer às organizações uma visão rápida e precisa do seu atual perfil de risco. Essa etapa, quase sempre ignorada pela concorrência, é necessária para que seja possível escolher as mitigações defensivas certas e reduzir os riscos com eficácia. Segundo, ao manter o foco na inteligência das ameaças locais, a KnowBe4 permite que você se concentre em deter as ameaças direcionadas ao seu ambiente e que são bem-sucedidas em atingi-lo. A maioria dos fornecedores de treinamento de conscientização em segurança utiliza, basicamente, estatísticas de e-mails de phishing coletadas globalmente de todos os clientes e das tentativas de phishing enviadas por e-mail. Em seguida, eles divulgam as tendências globais como se elas fossem as maiores causas de preocupação. A KnowBe4 apresenta relatórios sobre novas tendências globais, mas capacita os administradores de TI a entender como as tentativas de phishing locais e seus resultados positivos diferem dos verificados em âmbito mundial e quais são as medidas certas a tomar.

A KnowBe4 adota uma abordagem bastante diversificada que parte da compreensão de como sua organização se posiciona diante de certos riscos para, a partir daí, ajudar você a tirar proveito dos rumos globais das tentativas reais de phishing e explorar as ocorrências que conseguiram transpor suas defesas específicas:

Testes de linha de base

Fornecemos testes de linha de base para avaliar a Phish-prone Percentage™ dos seus usuários por meio de um ataque de phishing simulado gratuito.

Treine seus usuários

Aproveite a maior biblioteca do mundo de conteúdo sobre treinamento de conscientização em segurança, que inclui módulos interativos, vídeos, jogos, pôsteres e boletins informativos. Faça uso das campanhas de treinamento automatizadas com e-mails de lembrete agendados.

Aplique phishing em seus usuários

Implante as melhores simulações de ataques de phishing totalmente automatizadas, milhares de modelos de uso ilimitado e modelos de phishing comunitários.

Veja os resultados

Explore relatórios de nível corporativo contendo estatísticas e gráficos de phishing e de treinamento de conscientização em segurança, preparados para a gerência demonstrar seus sucessos e as áreas passíveis de aprimoramento.

—

Continue lendo este guia e conheça melhor nossa série de conteúdo de treinamento e a variedade de recursos disponíveis em nossa plataforma de treinamento e simulação de phishing.

Biblioteca de treinamento e conteúdo de simulação de phishing da KnowBe4

Biblioteca de treinamento

A KnowBe4 disponibiliza a maior biblioteca do mundo de conteúdo sempre atual sobre treinamento de conscientização em segurança, que inclui avaliações, módulos de treinamento interativos, vídeos, jogos, pôsteres e boletins informativos.

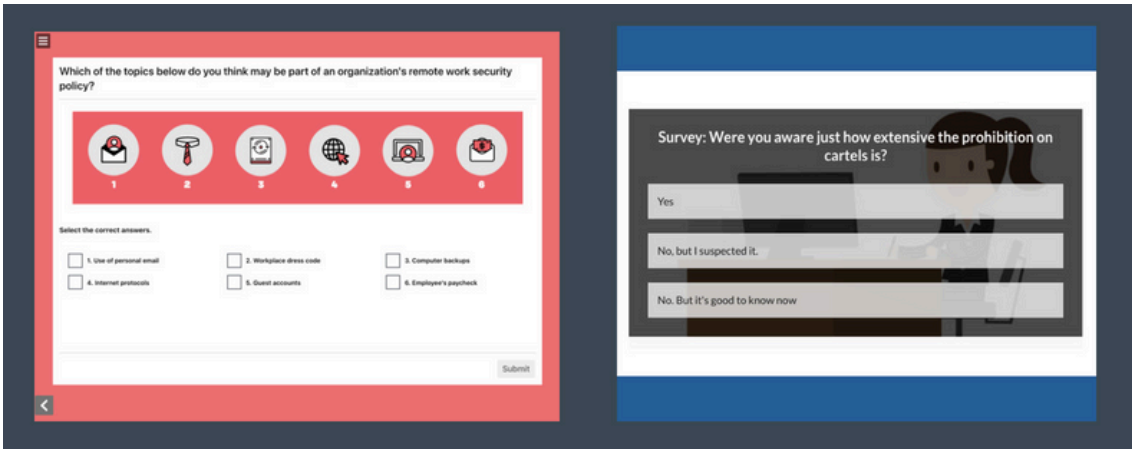
Para disponibilizar com facilidade essa biblioteca de conteúdo aos seus clientes, a KnowBe4 conta com a "ModStore".

Você, cliente, pode usar a ModStore para pesquisar, explorar, visualizar conteúdo e, dependendo do nível de assinatura, adicionar o conteúdo de treinamento escolhido à biblioteca da conta da KnowBe4.

Nossas parcerias com provedores globais de conteúdo voltado para e-learning e conscientização em segurança conferem um toque todo especial ao acervo e garantem campanhas de treinamento sempre atuais, relevantes e envolventes para os usuários. A ModStore contém uma ampla variedade de conteúdo sobre vários tópicos e tipos de conteúdo diferentes.

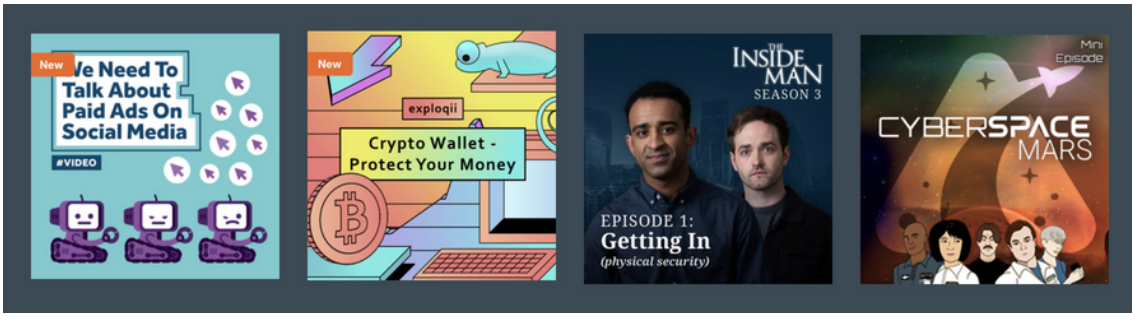
Módulos de treinamento

Os módulos de treinamento são apresentados de forma interativa e abordam uma série bastante ampla de assuntos. Esses módulos são compatíveis com o padrão SCORM e podem ser baixados para uso no seu próprio Sistema de Gestão de Aprendizagem (Learning Management System, LMS). Centenas desses módulos de treinamento são customizáveis.



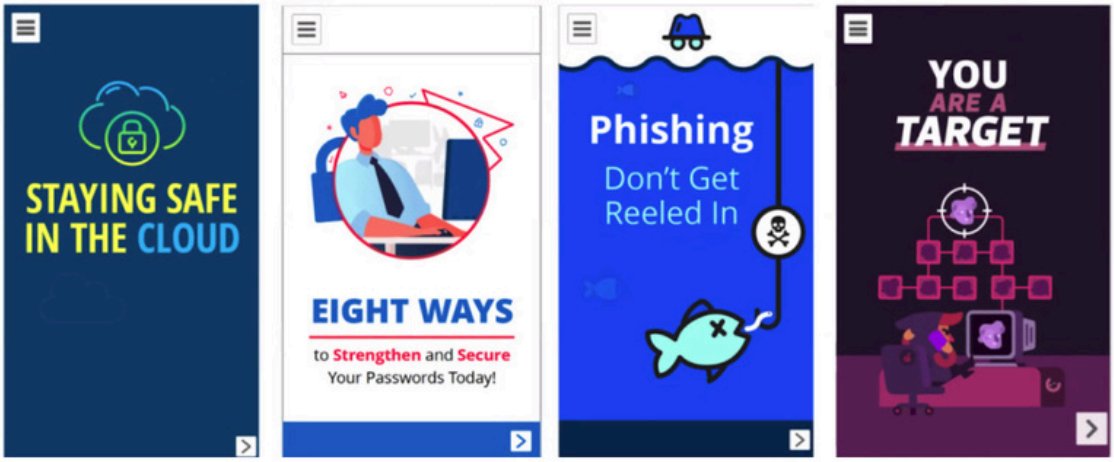
Módulos de vídeo

Os vídeos são arquivos MP4 que podem ser vistos no navegador ou baixados para uso em seu próprio LMS.



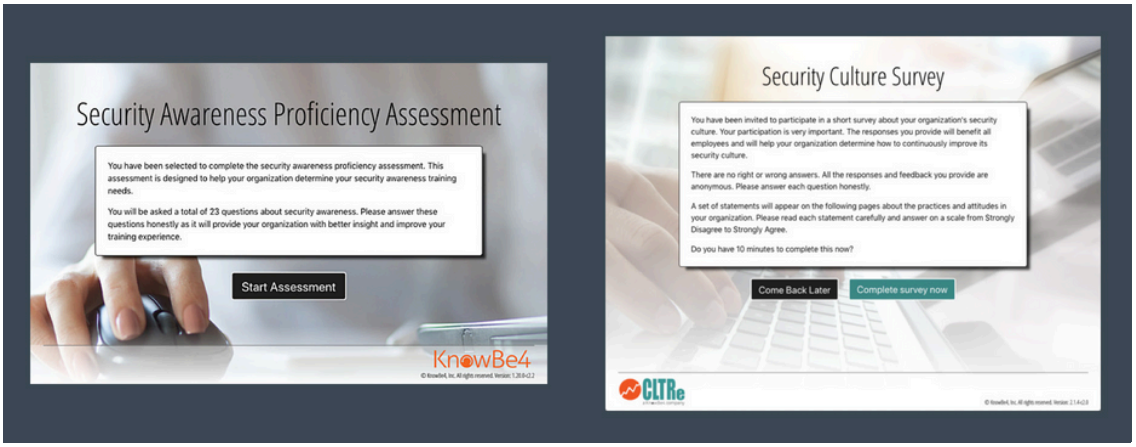
Módulos exclusivos para dispositivos móveis

Os módulos exclusivos para dispositivos móveis são otimizados para visualização e interação em um dispositivo móvel. A duração desses módulos é de menos de cinco minutos e o objetivo deles é envolver os usuários, estejam eles realizando atividades externas ou localizados em regiões com pouca largura de banda. Os módulos exclusivos para dispositivos móveis são customizáveis e compatíveis com o padrão SCORM, ou seja, podem ser baixados para uso em seu LMS.



Avaliações

As avaliações fornecem um detalhamento dos pontos fortes e fracos de sua organização. Use os resultados das avaliações para criar um plano de treinamento de conscientização em segurança mais direcionado.

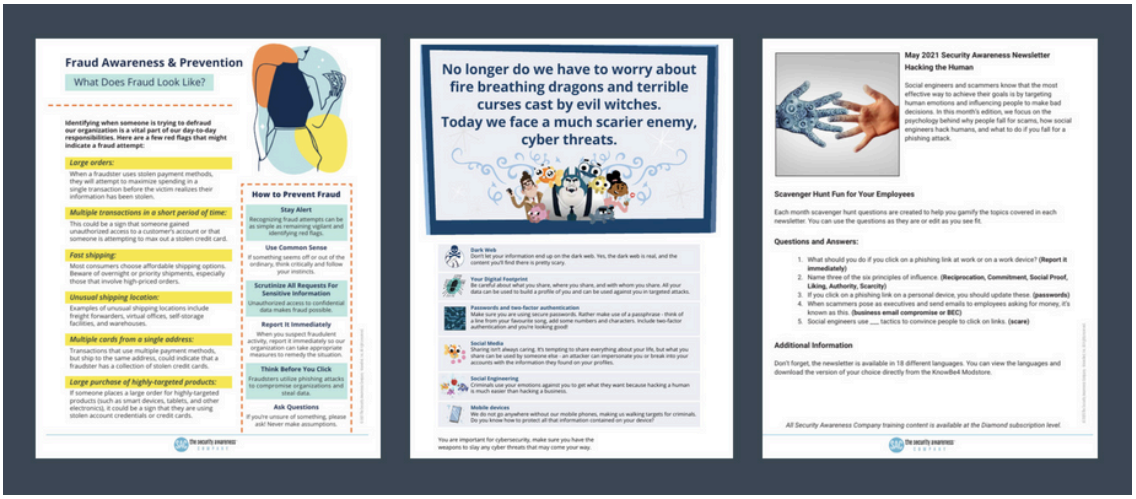


Jogos

Os jogos podem reforçar as habilidades e as informações que seus usuários estão absorvendo de um jeito totalmente novo e interessante. Esses jogos são compatíveis com o padrão SCORM e podem ser baixados para uso em seu LMS.

Boletins informativos e documentos de segurança

Os boletins informativos e os documentos de segurança são arquivos PDF que podem ser impressos ou compartilhados digitalmente com os usuários. Esses documentos abrangem uma grande variedade de tópicos sobre segurança cibernética para ajudar a reforçar as habilidades adquiridas por seus usuários no treinamento.



Pôsteres e arte

Os pôsteres e a arte são imagens de alta qualidade e arquivos PDF que podem ser impressos ou compartilhados digitalmente com os usuários. Sugerimos o uso de pôsteres dentro do escritório ou sua distribuição para os funcionários em home office como lembretes visuais da necessidade de manter a segurança nas tarefas do dia a dia.

Níveis de acesso a treinamentos

Oferecemos três níveis de acesso a treinamentos: I, II e III, dependendo do nível de assinatura. Cada um dos níveis apresenta conteúdo sobre treinamento de conscientização em segurança cuidadosamente organizado e atrelado ao nível anterior, e cada assinatura oferece diferentes níveis de suporte multilíngue e opções de conteúdo ideais para dispositivos móveis. Para ver nossa biblioteca inteira e continuamente atualizada em tempo real, inscreva-se na Prévia de treinamentos da ModStore da KnowBe4!

Nível de acesso a treinamentos I (Prata)

O Nível de acesso a treinamentos I fornece os elementos essenciais necessários para iniciar um programa de treinamento de conscientização em segurança. Ele é ideal para organizações nas quais não há treinamento de conscientização em segurança, mas que estão interessadas em iniciar pelo menos um programa de treinamento anual. Você obtém módulos de treinamento e em vídeo, avaliações e reforços didáticos, como pôsteres e documentos de segurança. Muitos clientes começam no Nível I para oferecer a seus usuários alguns conceitos básicos de conscientização em segurança, o que inclui entender o significado de engenharia social. Quando se sentem preparados, avançam ao próximo nível do conteúdo de treinamento, que aborda mais profundamente outros tópicos sobre segurança cibernética. Se o treinamento anual não for mais suficiente e você estiver pronto para lançar campanhas de treinamento com maior frequência, os Níveis de acesso a treinamentos II e III apresentam orientações de como desenvolver um programa de treinamento de conscientização em segurança mais robusto e totalmente consolidado.

Nível de acesso a treinamentos II (Ouro e Platina)

A biblioteca do Nível de acesso a treinamentos II amplia os conceitos do Nível I para oferecer uma variedade maior de estilos, formatos e tópicos para o conteúdo de treinamento. Utilizando desde animação a produções com atores reais e treinamento no ritmo do próprio usuário, o Nível II capacitará você a oferecer treinamento mais direcionado com base nas funções dos usuários, na sua localização e no setor de atuação da organização. Além disso, a grande variedade de minimódulos de treinamento, com menos de cinco minutos de duração, simplifica a introdução de um ritmo mais frequente para as campanhas de treinamento, que manterá os usuários engajados. Treinamentos mais frequentes ajudam a estimular uma mudança de comportamento na qual a conscientização em segurança é a principal preocupação.

Nível de acesso a treinamentos III (Diamante)

O Nível de acesso a treinamentos III inclui todo o conteúdo de treinamento dos Níveis I e II, além de acesso à mais completa biblioteca de conteúdo sobre treinamento de conscientização em segurança e recursos que aumentarão a capacidade da sua organização de oferecer um programa de conscientização contínuo e altamente consolidado. O Nível III oferece toda uma série de vídeos premiados com alta qualidade de streaming, que combinam cenas de cada episódio a melhores práticas de segurança cibernética. Você aprenderá a tomar decisões mais inteligentes sobre segurança com cenários envolventes e divertidos do mundo real. Com uma ampla variedade de tópicos, formatos, durações e estilos de vários produtores de conteúdo, você terá mais opções de conteúdo para atender às necessidades exclusivas dos usuários e manter-se em sintonia com a cultura corporativa da organização.
No Nível III, você pode experimentar estilos e formatos variados com diferentes públicos para aumentar ainda mais o engajamento dos usuários. Esse nível oferece também a flexibilidade de combinar as informações para aperfeiçoar o conteúdo que repercutirá melhor em diferentes departamentos e localidades regionais. Crie campanhas de treinamento mais curtas e mais frequentes que simplifiquem a implantação do programa de conscientização ao longo do ano. Mantenha seus alunos engajados seguindo um ritmo consistente nas campanhas e utilizando diversos tipos de conteúdo sobre melhores práticas de segurança. Essa combinação de conteúdo novo fixa o aprendizado com o passar do tempo, sem a necessidade de usar o mesmo treinamento repetidas vezes.

Produtores de conteúdo de treinamento

Conheça os produtores de conteúdo abaixo um pouco melhor e encontre a melhor combinação para criar seu próprio programa de treinamento de conscientização em segurança multifacetado e consolidado.

KnowBe4

O conteúdo do treinamento interativo de conscientização em segurança, desenvolvido pela KnowBe4 e por Kevin Mitnick, apresenta situações reais nas quais Kevin, o hacker mais famoso do mundo, revela aos usuários os bastidores da atuação dos criminosos cibernéticos. O conteúdo de treinamento da KnowBe4 inclui a combinação certa de ilustrações e texto para que os alunos não percam o interesse e absorvam as informações. Os vídeos e módulos de treinamento incluem dicas práticas, personagens inesquecíveis e narrativas impactantes.

The Security Awareness Company (SAC)

A SAC oferece treinamento fundamental e diversificado, repleto de informações. O conteúdo foi criteriosamente desenvolvido para maximizar a compreensão, a retenção e a mudança de comportamento por meio de uma série de cursos bem elaborados, que incluem também verificações de conhecimento, interações, quizzes, jogos, documentos e boletins informativos mensais.

Popcorn Training

Todo mundo adora uma boa história! Este treinamento envolve emoções, atiça a imaginação e estimula os alunos a agir. Animações divertidas, videoclipes com atores reais e quizzes ajudam a reforçar o aprendizado e acompanham pôsteres e documentos de segurança complementares para reforçar as mensagens principais.

E xploqii

Treinamento de conscientização em segurança simplificado. Vídeos de treinamento curtos apresentados com animações divertidas e dinâmicas. O foco principal deste conteúdo é passar uma mensagem fácil de assimilar e reter.

Canada Privacy Training

Conteúdo de treinamento adaptado às leis de privacidade do Canadá, incluindo a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (Personal Information Protection and Electronic Documents Act, PIPEDA).

Twist & Shout

Entretenimento educativo com pitadas de humor, que certamente será um sucesso instantâneo. Inspirados em seriados de TV, esses vídeos são organizados de uma forma que torna o treinamento pessoal, empático, real e prazeroso.

El Pescador

Animações divertidíssimas dão vida ao treinamento! As aventuras do inesquecível Capitão El Pescador farão com que os alunos fiquem totalmente atentos aos preciosos conselhos sobre conscientização em segurança por meio de uma variedade de módulos de treinamento, vídeos, pôsteres e documentos.

CLTRe

A pesquisa sobre cultura de segurança da CLTRe oferece um método eficaz e de fácil utilização para avaliar a situação atual da sua cultura de segurança e monitorar mudanças ao longo do tempo. A pesquisa sobre cultura de segurança utiliza princípios e métodos sociocientíficos comprovados para proporcionar resultados confiáveis e baseados em evidência com os quais as organizações poderão avaliar, desenvolver e aprimorar sua cultura de segurança.

Saya University

Os módulos de microaprendizado da Saya University foram originalmente planejados e produzidos para representar as vozes reais e o panorama socioeconômico e de ameaças do Japão, de modo a garantir que cada indivíduo disponha das informações necessárias para se proteger contra as ameaça globais à segurança cibernética.

MediaPRO

Módulos interativos e vídeos curtos são a garantia de aulas envolventes e de informações facilmente retidas, além de abranger tópicos como regulamentos de privacidade de dados, conformidade corporativa e prevenção contra assédio sexual.

Treinamento Compliance Plus

(Disponível como um add-on para qualquer nível de assinatura)

Interativo, relevante e envolvente, o treinamento Compliance Plus da KnowBe4 utiliza simulação de situações reais para ajudar os usuários a aprender como reagir diante de uma condição desafiadora. O conteúdo aborda temas difíceis, como assédio sexual, diversidade e inclusão, discriminação e ética profissional. A biblioteca do Compliance Plus inclui diversos tipos de formatos de mídia e materiais de reforço para dar suporte ao seu programa de treinamento de conformidade.

Conteúdo de simulação de phishing

Com nossa vasta biblioteca de modelos, você poderá usar a plataforma KnowBe4 para aplicar phishings de ação imediata. Em menos de 30 minutos, estará tudo pronto para você entrar em ação.

Modelos de e-mail

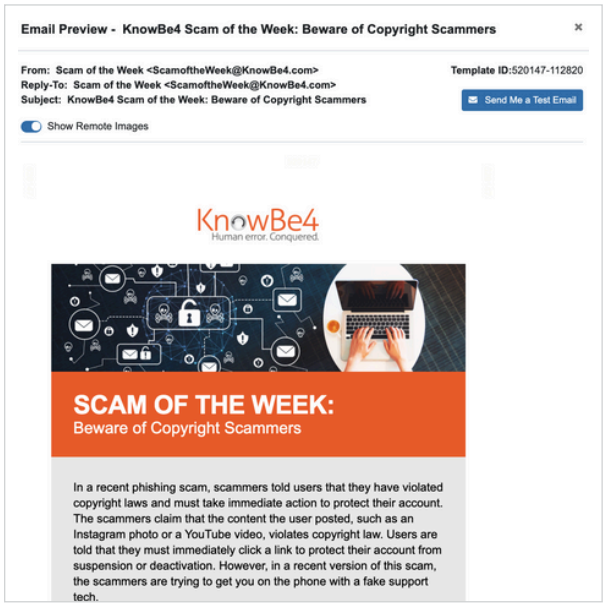
Nossa biblioteca de modelos multilíngues inclui e-mails em mais de 30 categorias, dentre eles: bancos e finanças, redes sociais, TI, governo, serviços on-line, eventos atuais, assistência médica e muito mais. Você também tem acesso a uma seção comunitária na qual poderá trocar modelos com centenas de outros clientes da KnowBe4.

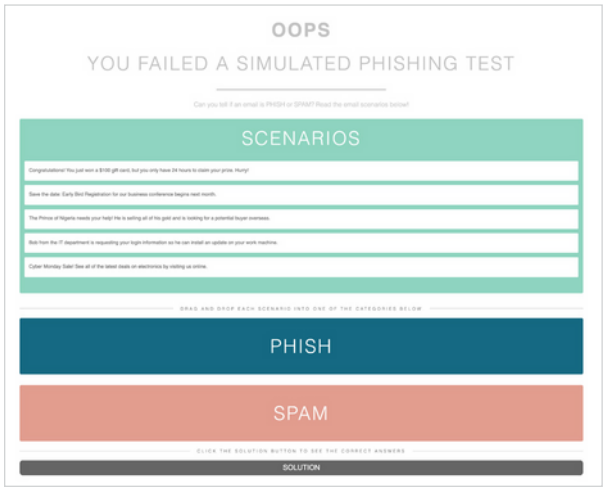
Modelos de páginas de destino

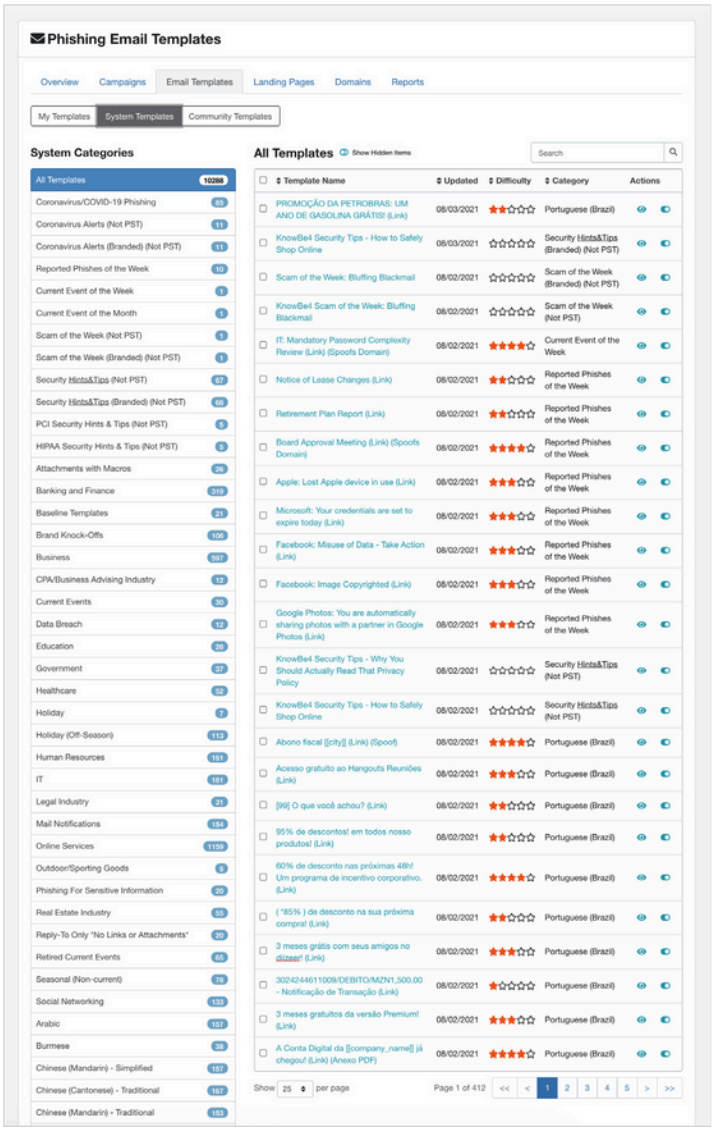
Para cada modelo de e-mail de phishing há também uma página de destino personalizada e exclusiva, que inclui orientações sobre falhas críticas, e páginas de destino que aplicam phishing específico em busca de informações sigilosas. Com mais de 200 páginas de destino à sua escolha, você poderá influenciar a reação dos seus usuários a um teste de phishing. Há três opções para configurar qual página de destino será exibida aos usuários quando eles forem reprovados nos testes de phishing. Com suporte a páginas adaptadas para dispositivos móveis, você pode 1) personalizar sua página de destino padrão, 2) escolher uma página de destino específica de uma campanha ou 3) definir uma página de destino específica de um modelo.

Boletins informativos

Como parte das categorias de modelos de phishing da KnowBe4, você terá acesso a boletins informativos sobre "Golpe da semana" e "Dicas de segurança" que ajudarão a manter seus usuários informados sobre os golpes de phishing mais recentes e reforçar as dicas de segurança básica. Use esses boletins informativos como parte de uma campanha semanal, quinzenal ou mensal ao configurar uma campanha de phishing no console da KnowBe4.







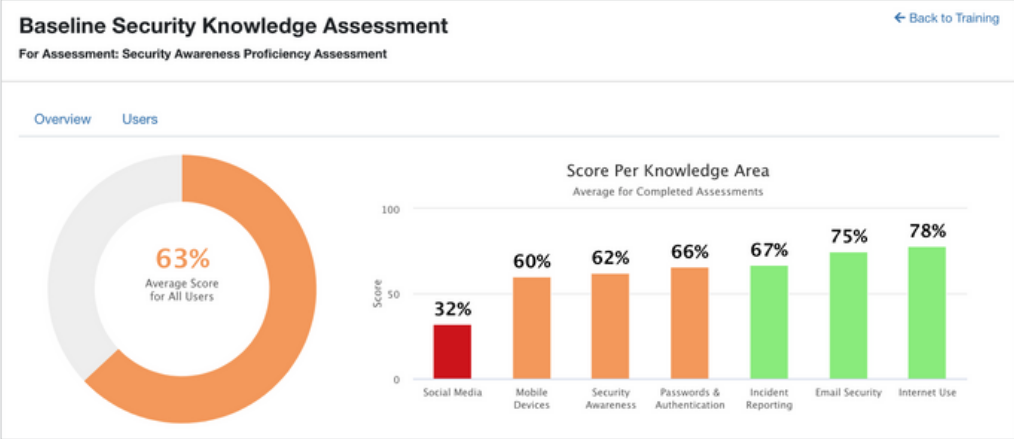
Avaliações

Descubra como seus usuários estão se saindo em relação ao conhecimento de segurança e à cultura de segurança para ajudar a determinar as métricas de segurança de referência que poderão ser aprimoradas com o tempo.

Integradas à plataforma KnowBe4 e incluídas sem custo adicional, as avaliações da KnowBe4 ajudam a identificar os usuários que estão cientes das medidas mais seguras a serem tomadas em situações de risco e que sabem como proceder. Esse conhecimento ajuda a definir uma linha de base para a cultura de segurança que você está tentando implantar em sua organização e a monitorar o sucesso dos seus esforços de treinamento.

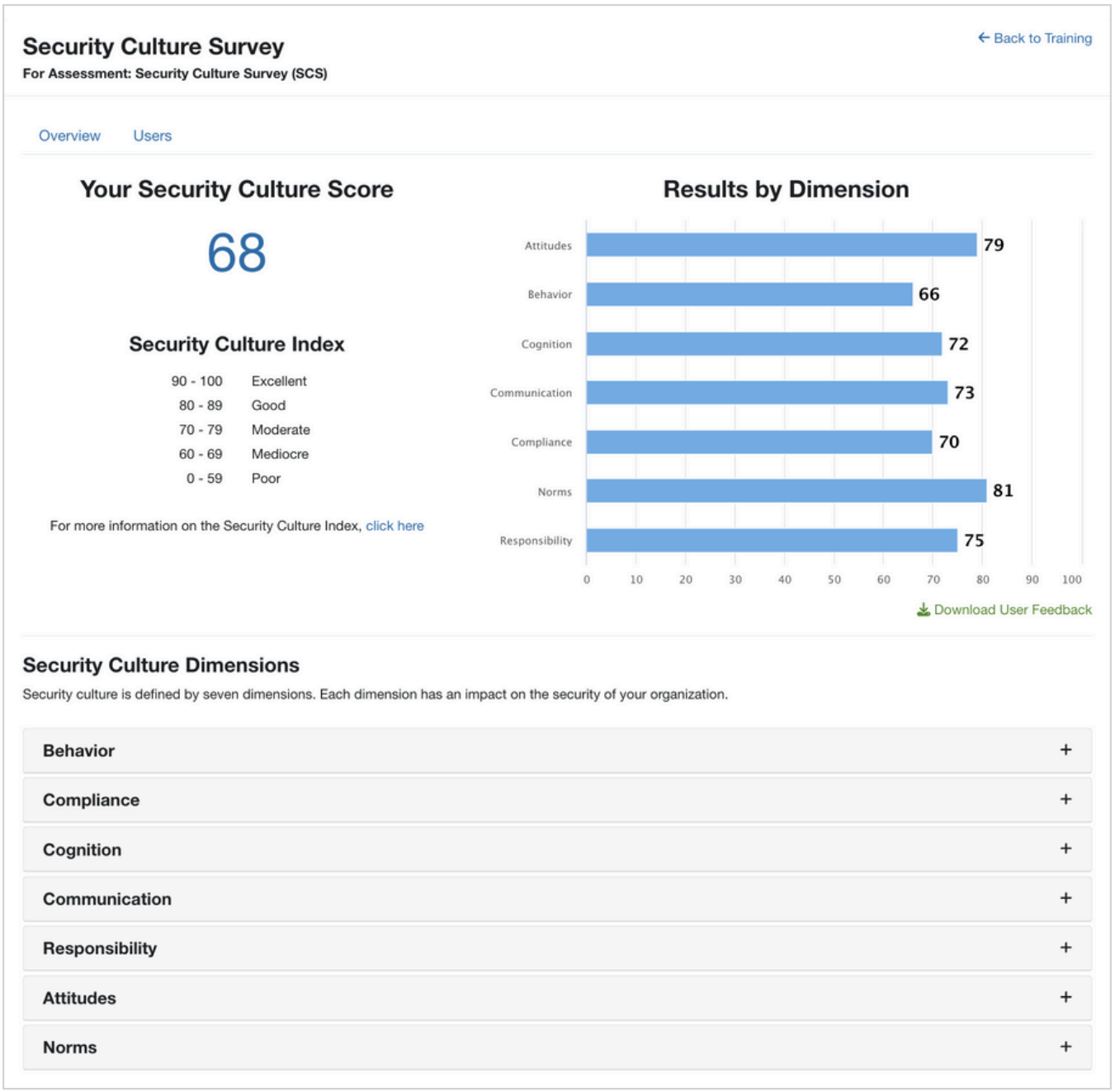
Avaliação de competências no âmbito da sensibilização para a cibersegurança (SAPA)

O SAPA é uma avaliação baseada em habilidades criada para ajudar a organização a determinar suas necessidades de treinamento de conscientização em segurança por meio da identificação de lacunas no conhecimento de usuários individuais e recomendações sobre melhorias no aprendizado.



Pesquisa sobre cultura de segurança (SCS)

A pesquisa sobre cultura de segurança avalia as opiniões dos usuários em relação à segurança da sua organização, ou seja, os aspectos psicológicos e sociais que conduzem o comportamento social. A SCS demonstra a eficácia geral do seu programa de cultura de segurança e como essa cultura evolui com o tempo.



O SAPA e a SCS são fundamentados em ciência avaliativa e permitem determinar a proficiência e o conhecimento que seus usuários têm sobre segurança, bem como avaliar o posicionamento geral da sua organização em relação à cultura de segurança.

Suporte multilíngue

A interface localizada do aluno e o conteúdo traduzido de ponta a ponta para campanhas de phishing e treinamento estão disponíveis em 35 idiomas principais para a cobertura global de seus alunos. O console do administrador localizado está disponível em 10 idiomas.

Console da KnowBe4

A plataforma KnowBe4 é rica em recursos, intuitiva e fácil de usar. Ela foi desenvolvida na medida certa para os profissionais de TI superocupados que têm inúmeros problemas a resolver. Os clientes de empresas de todos os portes poderão colocar a plataforma KnowBe4 em operação duas vezes mais rápido do que a concorrência.

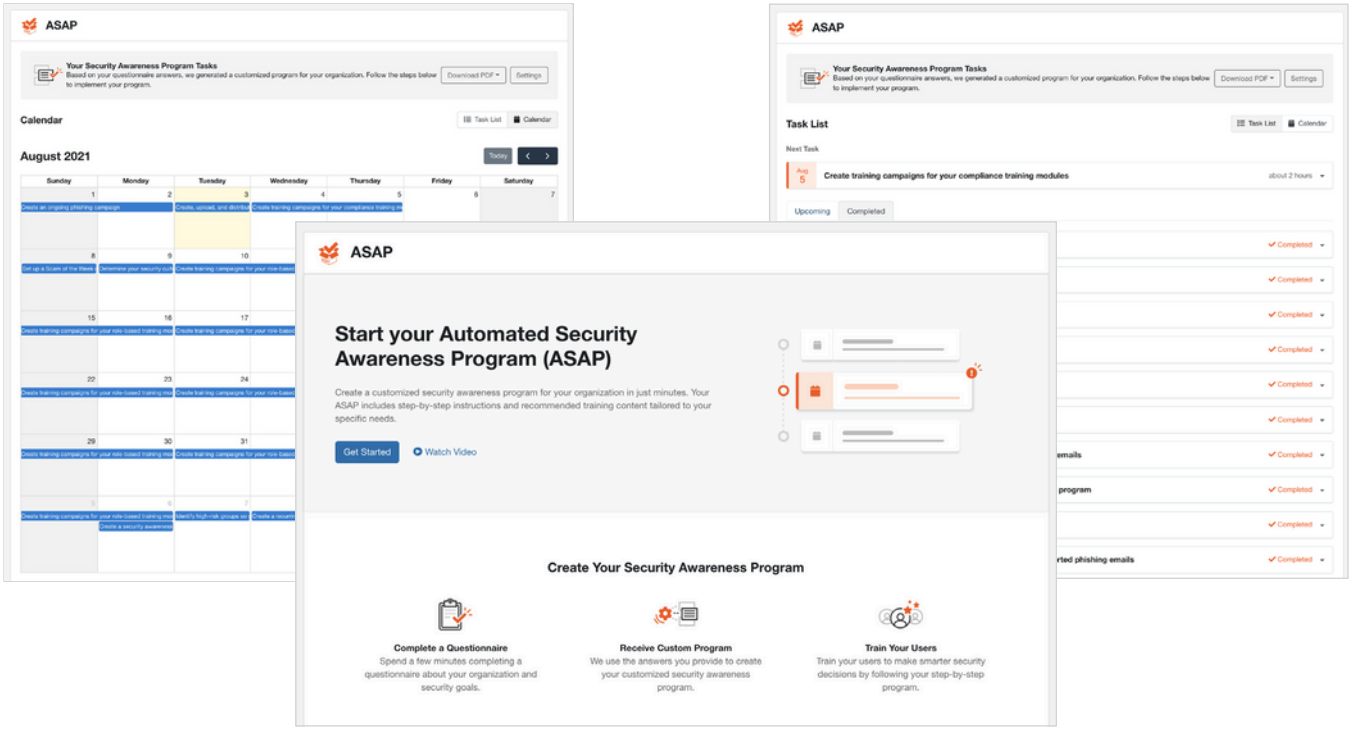
Continue lendo para conhecer todos os recursos oferecidos pela plataforma KnowBe4.

Automated Security Awareness Program (ASAP)

Muitos profissionais de TI não sabem exatamente por onde começar quando o assunto é criar um programa de cultura e de treinamento de conscientização em segurança que funcione em suas organizações.

Com o Automated Security Awareness Program (ASAP), eliminamos todo tipo de suposições. O ASAP é uma ferramenta integrada ao console que ajuda você a criar um programa de conscientização em segurança personalizado para sua organização. O ASAP apresenta as etapas necessárias para criar um programa de treinamento totalmente consolidado em questão de minutos!

Após responder a sete perguntas sobre suas metas e a organização, a ferramenta ASAP recomendará e definirá automaticamente a data de um programa para você. As tarefas do programa se basearão em melhores práticas de como alcançar suas metas de conscientização em segurança.



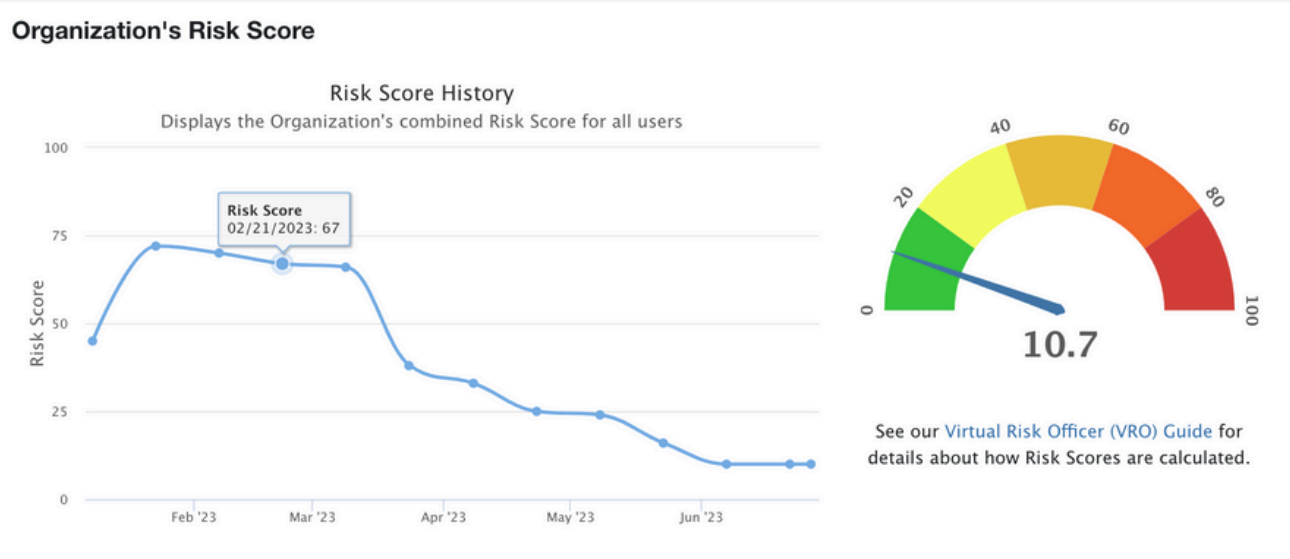
O programa inclui toda uma série de tarefas práticas, dicas úteis, sugestões de conteúdo de treinamento e um calendário de gerenciamento de tarefas. Realize todo o gerenciamento do seu programa personalizado no console da KnowBe4. Você também poderá exportar o programa completo como uma versão detalhada ou um resumo executivo em formato PDF a ser usado para fins de exigências de conformidade e/ou gerenciamento de relatórios.

Painel do console

No painel de phishing e treinamento, é possível visualizar o nível de risco da sua organização e verificar rapidamente o progresso dos seus usuários finais em relação aos colegas de diversos setores, utilizando o benchmark do setor.

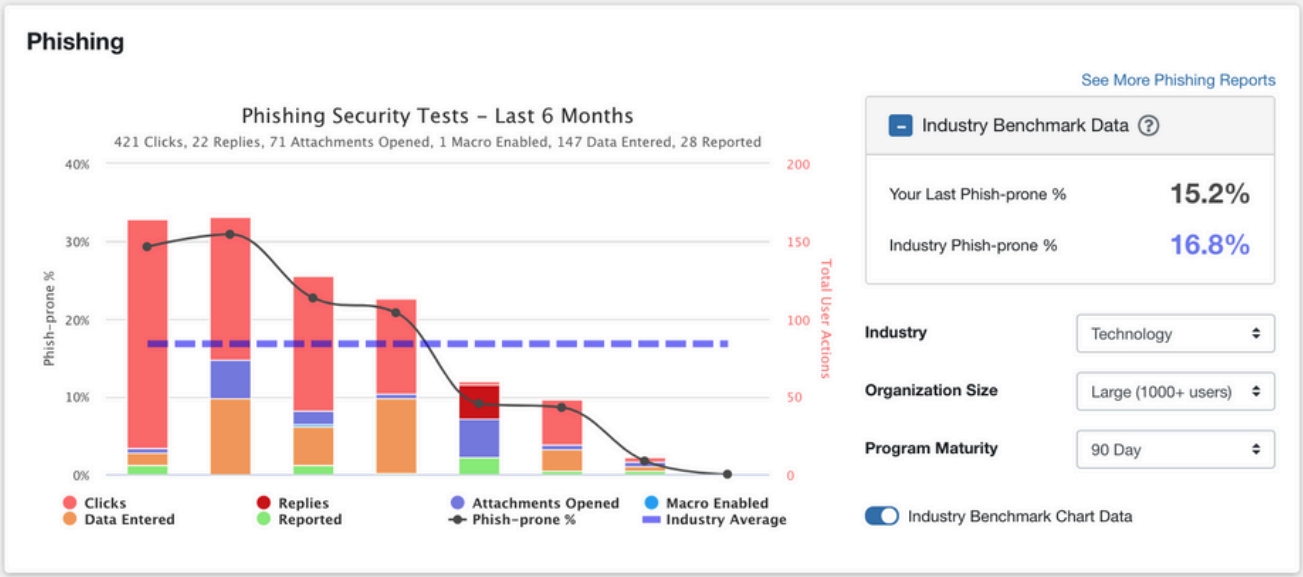
Confira o nível de risco da organização

Veja o nível de risco geral da sua organização com base em níveis de risco combinados de todos os seus usuários.



Resultados da Phish-prone Percentage (porcentagem de propensão ao phishing)

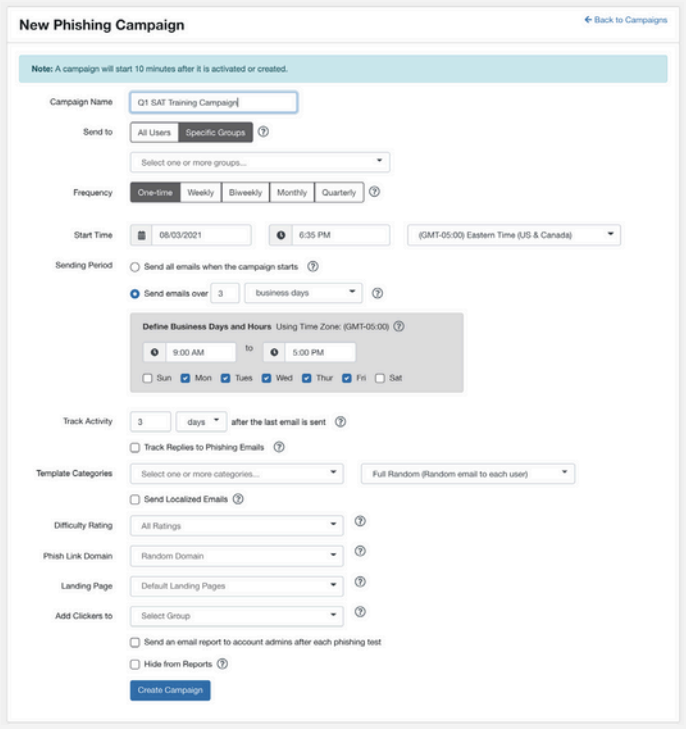
Nossa plataforma oferece diferentes maneiras de medir o progresso dos usuários finais em setores semelhantes com base nos resultados da avaliação e de phishing. Este painel é um recurso com o qual você poderá visualizar a Phish-prone Percentage (porcentagem de propensão ao phishing) de sua organização (ou quantos usuários fatalmente clicarão em um e-mail de phishing) em comparação a concorrentes do seu setor.



Plataforma de simulação de phishing

A KnowBe4 oferece uma abordagem moderna ao treinamento de usuários em ameaças de phishing ao permitir que você crie campanhas de phishing nas quais e-mails de phishing simulados são enviados. Esses ataques simulados imitam ataques de phishing reais e ensinam os usuários a se manterem em alerta.

Os clientes da KnowBe4 podem programar e enviar um número ilimitado de testes simulados de phishing (PSTs) aos seus usuários durante o período da assinatura. Continue lendo para conhecer os recursos mais populares da nossa plataforma de phishing.

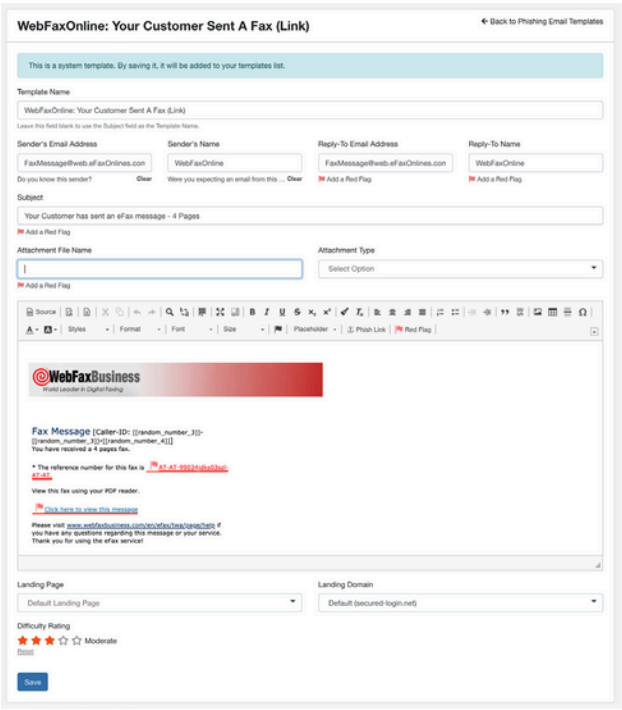


Campanhas de phishing

A plataforma KnowBe4 foi projetada para ajudar você a determinar a quais tipos de ataques seus usuários são mais vulneráveis, a instruir os usuários em como identificar sinais de alerta e a calcular a Phish-prone Percentage da sua organização. Para iniciar seu programa de treinamento, o primeiro passo é criar campanhas de phishing para testar os usuários, de modo que seja possível determinar em que tipo de treinamento eles devem se inscrever.

Programação dos testes de phishing

Você pode programar testes de phishing de nossa vasta biblioteca, composta por mais de 20.000 modelos disponíveis em mais de 40 idiomas, ou escolher uma das opções na seção de modelos da comunidade, que foram criados por administradores para administradores para compartilhamento com outros profissionais. Escolha dentre as opções de ataques simulados de phishing únicos, semanais, quinzenais ou mensais e veja imediatamente quais funcionários caem nesses ataques de engenharia social. Use o exclusivo recurso “antifofoca” da KnowBe4 para enviar modelos de phishing aleatórios em horários imprevisíveis durante uma campanha de phishing, imitando ataques de phishing reais e impedindo um usuário de avisar o outro sobre os testes de phishing.



Personalização dos modelos de phishing

Personalize qualquer modelo de sistema e inclua anexos e macros simulados. Crie do zero modelos de e-mail de phishing personalizados ou modifique os modelos existentes para enviá-los aos seus usuários. Você pode ir além e personalizar cenários com base em informações públicas e/ou pessoais. Para isso, crie campanhas de spear phishing direcionadas, que substituam campos por dados personalizados.

Aproveite o recurso de usar logotipos em e-mails de phishing para criar modelos de e-mail com uma aparência legítima em nossa plataforma. Use os links incorporados aos e-mails que apontam para o endereço do URL original do logotipo. Dessa forma, o proprietário do logotipo ainda será o host e detentor dos direitos da imagem.

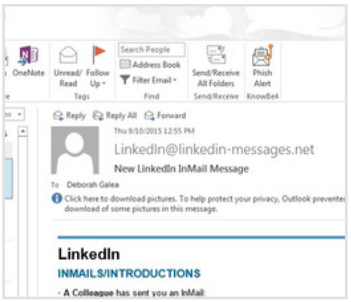
Phish Alert Button

Com apenas um clique, o suplemento Phish Alert Button da KnowBe4 proporciona aos seus usuários uma forma segura de encaminhar ameaças de e-mail para a equipe de segurança para fins de análise e exclui o e-mail da caixa de entrada para evitar uma futura exposição. Tudo isso com apenas um clique. O Phish Alert Button (PAB) do Microsoft 365 permite adicionar idiomas à sua instância do PAB para exibir automaticamente o idioma preferencial com base na configuração de idioma do sistema dos usuários.

- Ao clicar no Phish Alert Button em um teste simulado de phishing, a ação correta desse usuário será informada.
- Quando o usuário clica no Phish Alert Button em um e-mail de phishing não simulado, o e-mail é encaminhado à sua equipe de Resposta a incidentes.
- Inclui o texto do botão totalmente personalizável e caixas de diálogo do usuário.
- Clientes compatíveis: Outlook 2010, 2013, 2016 e Outlook para Microsoft 365, Exchange 2013 e 2016, Outlook na web (Outlook.com), o aplicativo para dispositivos móveis do Outlook (iOS e Android), Chrome 54 e posterior (Linux, OS X e Windows), contas do Gmail conectadas por meio do Google Workspace, o add-on do Gmail é compatível com o Gmail em clientes móveis e no navegador.

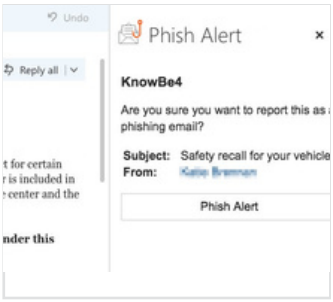
Barra de tarefas do Outlook

Adiciona um Phish Alert Button para os seus usuários



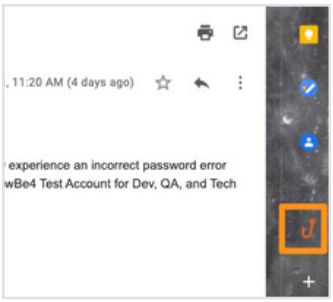
Painel de suplementos do Microsoft 365

Adiciona um Phish Alert Button para os seus usuários



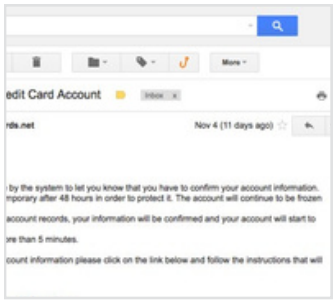
Add-on do Gmail

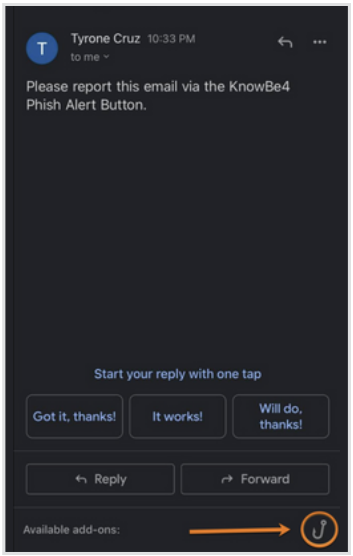
Adiciona um Phish Alert Button para os seus usuários



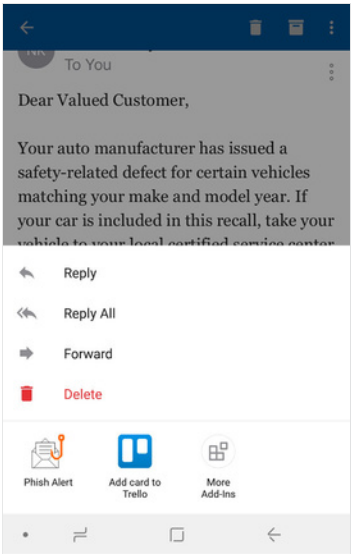
Extensão do Gmail

Adiciona um Phish Alert Button para os seus usuários

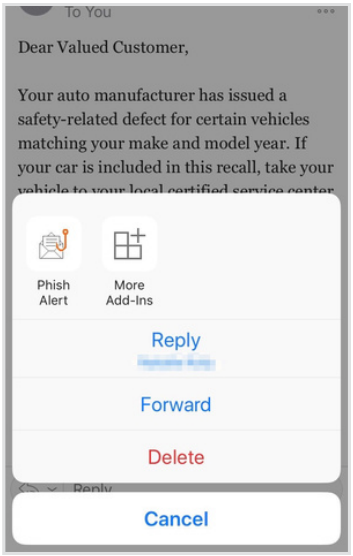




Gmail no celular (Android)



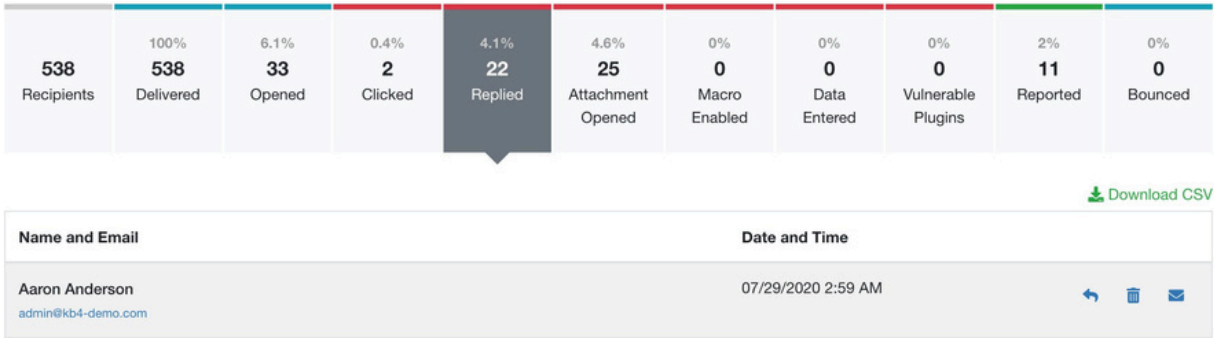
Outlook no celular (Android)



Outlook no celular (iOS)

Acompanhamento de respostas a phishing

Além de permitir que você monitore se o usuário responderá a um e-mail de phishing simulado, o recurso de acompanhamento de respostas a phishing captura as informações da resposta para analisá-las no console da KnowBe4. Disponibilizamos uma categoria de modelos de phishing simulado chamada "Resposta online", cujo objetivo específico é testar se os usuários vão interagir com agentes mal-intencionados no outro lado. Contudo, esse recurso também funciona com qualquer um dos nossos modelos de phishing.



Fácil de usar, o recurso de acompanhamento de respostas a phishing vem ativado por padrão nas novas campanhas de phishing, por meio da opção "Acompanhar respostas a e-mails de phishing".

Domínios de phishing personalizados

Domínio de phishing é como chamamos o URL preenchido no canto inferior esquerdo da sua tela quando você passa o mouse sobre um link em um e-mail suspeito. Faça sua escolha dentre uma grande variedade de diferentes domínios de phishing, de modo que o URL preenchido mude sempre e mantenha os usuários finais em alerta. Nosso acervo ilimitado de spoofing de domínios permite que você falsifique qualquer endereço de e-mail ao realizar campanhas de phishing simulado.

Recursos avançados de phishing

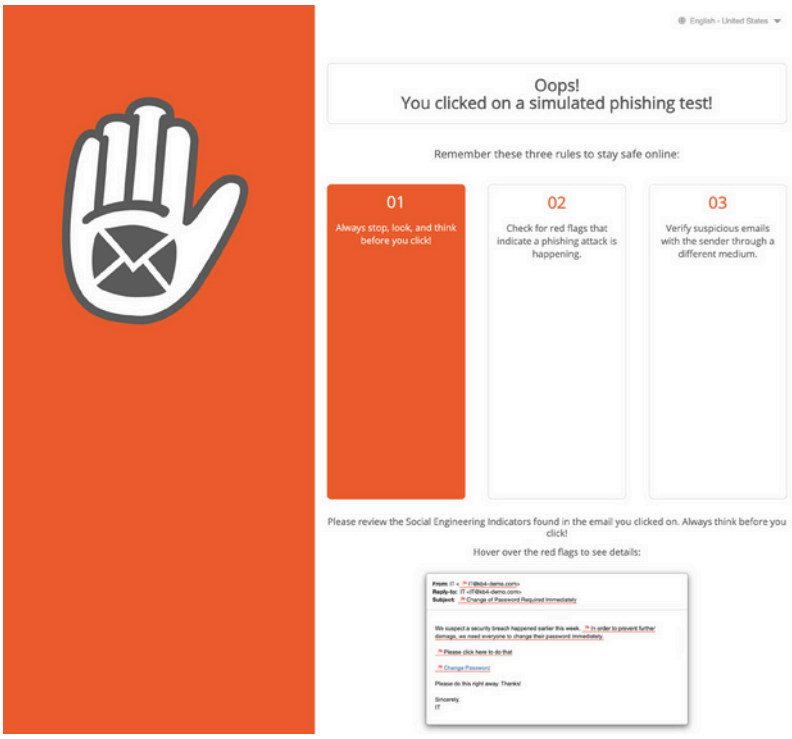
A opção Selecionar níveis de assinatura inclui formas adicionais para tirar o máximo proveito da nossa plataforma de phishing. Continue lendo para conhecer melhor esses recursos.

Indicadores de engenharia social

Nosso recurso Indicadores de engenharia social (IES) é uma tecnologia patenteada que transforma cada e-mail de phishing simulado em uma ferramenta a ser usada pela TI para treinar os usuários instantaneamente.

Quando o usuário clica em qualquer e-mail de phishing simulado da KnowBe4, ele é encaminhado a uma página de destino contendo uma cópia dinâmica do referido e-mail e mostrando todos os sinais de alerta. Você também pode personalizar qualquer e-mail de phishing simulado e criar seus próprios sinais de alerta.

Os usuários podem visualizar imediatamente as possíveis armadilhas e aprender a identificar os sinais que não viram para uso futuro.



Teste de unidade USB

Crie facilmente seu teste de unidade USB no console da KnowBe4 e baixe arquivos especiais e "beaconizados" do Microsoft Office. Renomeie também esses arquivos para instigar os funcionários a abri-los. Em seguida, grave os arquivos em uma unidade USB e deixe-a em uma área local com muito movimento. Se algum funcionário apanhar a unidade USB, inseri-la em sua estação de trabalho e abrir o arquivo, será feita uma "ligação para casa" relatando a falha e passando informações, como a hora do acesso e o endereço IP. Se, além disso, o usuário habilitar as macros do arquivo, dados adicionais, como nome de usuário e nome do computador, também serão rastreados e disponibilizados no console.

Phishing de código QR

Você pode testar seus usuários usando códigos QR em vez de links de phishing ou anexos em e-mails. Os códigos QR, ou códigos de resposta rápida, são códigos de barras que podem ser lidos e contêm dados em um formato compacto. Se os seus usuários lerem um código de barras malicioso, eles poderão ser levados a visitar um site perigoso. Além disso, links maliciosos ocultos em códigos QR podem ser capazes de burlar os filtros de segurança da sua organização.

As campanhas físicas de phishing de código QR permitem testar como os usuários reagirão ao encontrar um código QR inesperado. Por exemplo, se os seus usuários virem um código QR em um cartaz exposto em um local conhecido, eles poderão ler o código e abrir o link sem verificar se é seguro. Os testes de phishing de código QR podem ajudar a preparar os seus usuários para ataques reais de phishing de código QR.

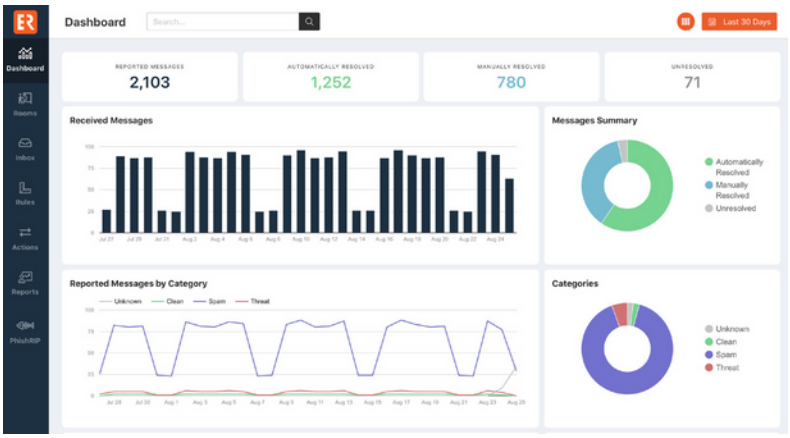
Phishing controlado por inteligência artificial

O phishing controlado por inteligência artificial permite explorar a capacidade da IA de selecionar automaticamente o modelo de phishing de cada um dos seus usuários com base no histórico individual de treinamento e phishing desses usuários. Ao usar dados do AIDA (Artificial Intelligence Driven Agent) da KnowBe4, um mecanismo de recomendação permite automatizar a seleção dinâmica de modelos únicos de testes de phishing para seus usuários.

Pense nisso como seu próprio assistente de phishing por IA que escolhe automaticamente o melhor teste de phishing para cada usuário, naquele momento específico. Quando você usa o phishing controlado por inteligência artificial, você essencialmente cria uma campanha de phishing exclusiva para cada um de seus usuários para garantir que cada um deles receba testes simulados de phishing personalizados de acordo com seu nível individual. Ofereça aos seus usuários uma experiência mais personalizada e adaptável ao nível atual de conhecimento deles.

PhishER Plus

Oferecido como um add-on opcional do produto em qualquer nível de assinatura, o PhishER Plus é uma plataforma com base na Web e de fácil utilização com a qual suas equipes de Segurança das informações e Operações de segurança poderão descartar o que for irrelevante na caixa de entrada e reagir às ameaças mais perigosas mais rapidamente. O PhishER Plus foi criado para ajudar você a turbinar a segurança dos e-mails de sua organização. Ele é a camada final adicional nos casos em que o gateway de segurança de e-mail e outras camadas de segurança cibernética não funcionam. O PhishER Plus possibilita um fluxo de trabalho crítico para ajudar suas equipes de resposta a incidentes a trabalharem juntas para mitigar as ameaças de phishing. Ele é adequado para qualquer organização que queira priorizar e gerenciar de forma automática mensagens potencialmente maliciosas com precisão e rapidez! A combinação entre KnowBe4 e PhishER Plus como parte do seu fluxo de trabalho de segurança de e-mail não só reduz as responsabilidades das suas equipes de Segurança das informações e de Resposta a incidentes durante o trabalho de identificar as ameaças genuínas mais rapidamente, mas também eleva o seu programa de treinamento de conscientização em segurança a um patamar totalmente novo.



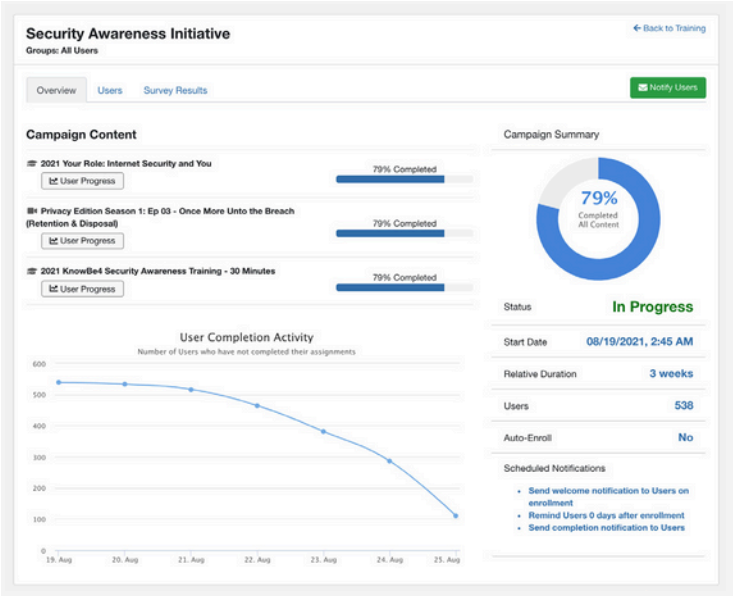
Veja alguns dos principais benefícios do PhishER Plus:

- Libere recursos de resposta a incidentes para identificar e gerenciar os 90% das mensagens que são spam ou e-mails legítimos.
- Visualize conjuntos ou grupos de mensagens com base em padrões que podem ajudar a identificar um ataque amplo de phishing contra sua organização.
- As entradas da Lista de Bloqueio Global contendo ameaças verificadas, obtidas colaborativamente de mais de 10 milhões de usuários treinados, são usadas para bloquear automaticamente novas mensagens recebidas nas caixas de entrada dos seus usuários. Esse feed de ameaças continuamente atualizado é gerenciado pela KnowBe4 e sincronizado com o seu servidor de e-mail do Microsoft 365.
- O PhishML™ é um módulo de aprendizagem de máquina do PhishER Plus que analisa cada mensagem que chega à plataforma do PhishER Plus e dá a você as informações para deixar seu processo de priorização mais fácil, rápido e preciso.
- O PhishRIP Global é um recurso de quarentena de e-mail que se integra ao Microsoft 365 e ao Google Workspace. Assim, sua equipe de resposta a incidentes pode corrigir os problemas com rapidez e facilidade. As mensagens que correspondem a uma ameaça de phishing identificada e que já foi removida das caixas de correio da organização por outros clientes do PhishER Plus são, então, validadas pelo laboratório de pesquisa de ameaças da KnowBe4.
- O PhishFlip™ é um recurso do PhishER Plus que automaticamente transforma os ataques de phishing informados pelo usuário e que foram lançados contra a sua organização em campanhas seguras de phishing simulado.

Plataforma de treinamento

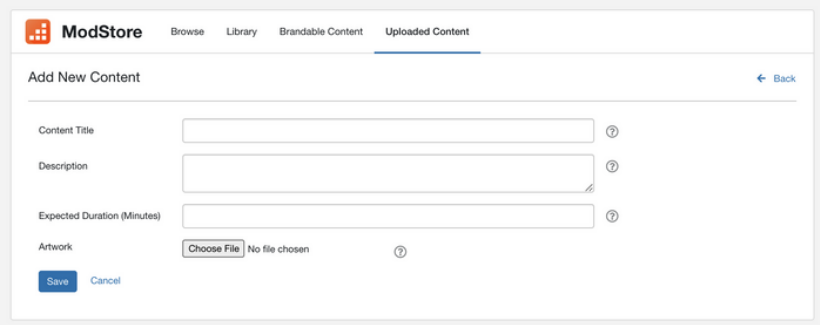
Campanhas de treinamento

No console da KnowBe4, é possível criar rapidamente campanhas contínuas ou com limitação de tempo, selecionar módulos de treinamento por grupos de usuários, inscrever automaticamente novos usuários e automatizar e-mails de "lembrete" para os usuários que não concluíram o treinamento. É possível também editar modelos de notificação de treinamento, preparar políticas para confirmação dos usuários e visualizar relatórios de treinamento. As campanhas de treinamento são usadas para personalizar e gerenciar o conteúdo de treinamento dos usuários no Learner Experience.



Opções do LMS

Com o robusto LMS da KnowBe4, você pode enviar seu próprio conteúdo de vídeo e treinamento compatível com o padrão SCORM, em qualquer idioma que quiser, e gerenciá-lo com o conteúdo de treinamento da ModStore da KnowBe4 em um único lugar e sem custos extras!



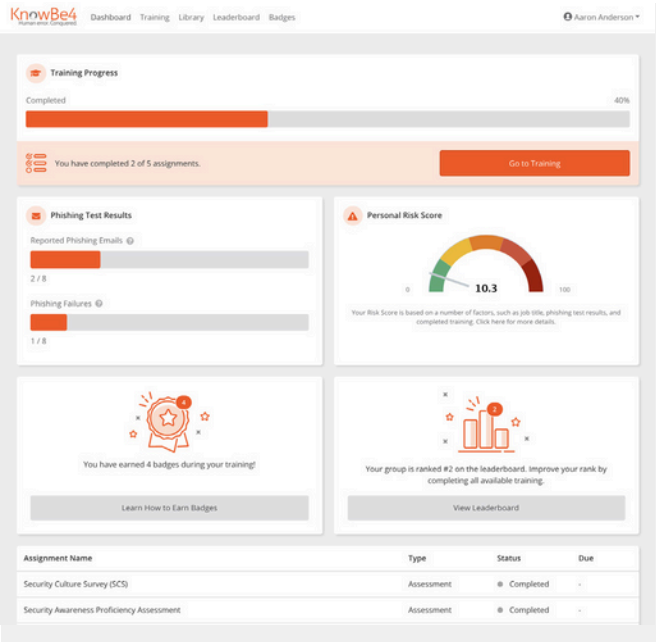
Learner Experience

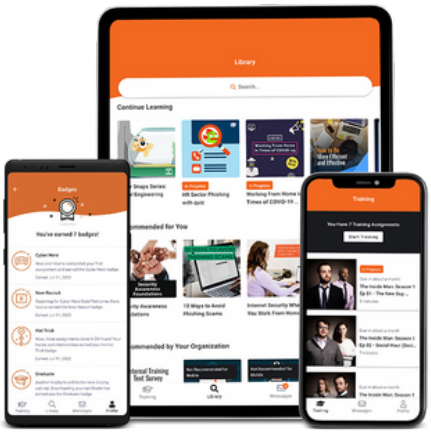
O Learner Experience (LX) da KnowBe4 enriquece o seu plano de treinamento de conscientização em segurança com personalizações e recursos envolventes e divertidos de gamificação.

Os usuários podem competir entre si na classificação geral e ganhar medalhas enquanto aprendem a proteger a si mesmos e a organização contra ataques cibernéticos. Oferecemos também um tour informativo opcional para apresentar aos usuários o novo ambiente de aprendizado e deixá-los à vontade nele.

A interface do LX também inclui um Painel do aluno.

Aqui, os usuários poderão ver um resumo da conclusão do treinamento que fizeram, incluindo o status e as datas finais. Como opção, escolha como apresentar os resultados dos testes de phishing, o nível de risco pessoal e as estatísticas de gamificação dos seus usuários.





Aplicativo KnowBe4 Learner

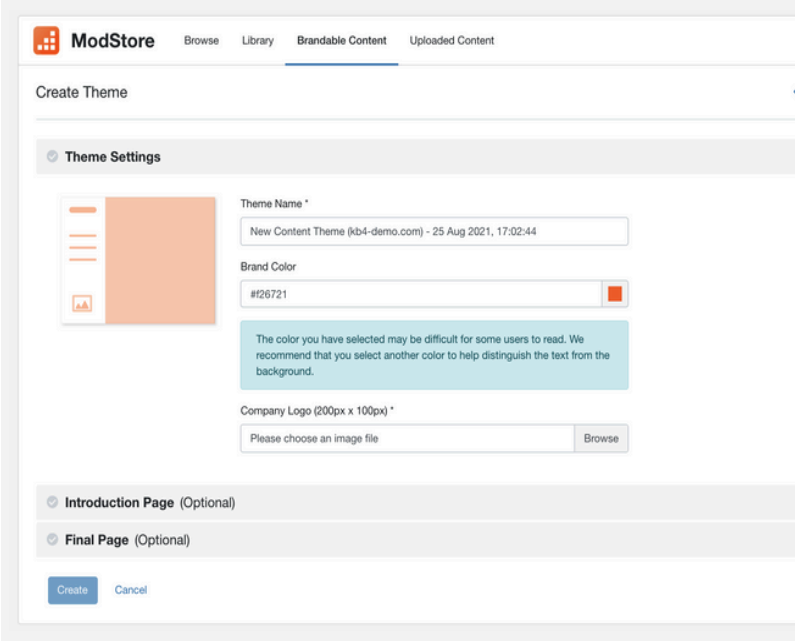
O aplicativo KnowBe4 Learner permite que seus usuários concluam o treinamento designado a eles de forma conveniente em seus tablets, smartphones e outros dispositivos móveis. Amplie a proteção da sua maior superfície de ataque e inclua funcionários que normalmente não têm acesso a um desktop ou laptop com um aplicativo desenvolvido pensando no usuário e também no administrador.

O aplicativo KnowBe4 Learner está incluído na sua assinatura de treinamento sem custo adicional e oferece aos seus usuários a flexibilidade e a conveniência do aprendizado 24 horas por dia, 7 dias por semana. O aplicativo, disponível para iOS e Android, oferece suporte a notificações por push para anúncios personalizados, atualizações sobre treinamentos atribuídos e boletins informativos da KnowBe4.

Conteúdo customizável

Com o recurso de conteúdo customizável, é possível criar temas customizados e aplicá-los às campanhas de treinamento ativas utilizando conteúdo qualificado. Clique na guia Conteúdo customizável para definir a cor da marca, enviar o logotipo da empresa e acrescentar uma introdução e uma página final. Essas páginas opcionais incluem o logotipo da empresa, texto personalizado e uma imagem à sua escolha.

Use esse recurso para criar um conceito com o qual os funcionários da sua empresa se identifiquem. Você também poderá enviar os certificados customizados da sua organização para a plataforma KnowBe4. Os certificados de conclusão personalizados podem ser entregues aos usuários ao fim de cada módulo de treinamento.



Treinamento recomendado pela IA

A ModStore da KnowBe4 utiliza aprendizagem de máquina para oferecer sugestões de treinamento inteligentes com base nas métricas de desempenho dos usuários obtidas das campanhas de teste de phishing. Personalizada de acordo com a Phish-prone Percentage geral da sua organização, a ModStore apresentará opções de módulos de treinamento recomendáveis com as quais você poderá reduzir as taxas de cliques dos usuários.

Aprendizado opcional para usuários

Com o aprendizado opcional, você poderá oferecer conteúdo de treinamento adicional da ModStore da KnowBe4 aos seus usuários. Basta criar campanhas de treinamento específicas utilizando o conteúdo opcional que você gostaria de disponibilizar aos usuários para eles mesmos escolherem. Você também pode aproveitar o recurso avançado de aprendizado opcional recomendado pela IA, disponível para clientes Diamante, para recomendar e implantar conteúdo de treinamento adicional para seus usuários com base em cursos anteriores concluídos por eles, sem a necessidade de criar uma campanha de treinamento separada.

Security Coach

O SecurityCoach é o primeiro produto de coaching de segurança em tempo real criado para ajudar as equipes de TI e operações de segurança a proteger ainda mais a maior superfície de ataque da sua organização: os funcionários. Ao introduzir uma nova categoria de tecnologia de Detecção e Resposta Humana (Human Detection and Response, HDR), o SecurityCoach ajuda a fortalecer a cultura de segurança, permitindo um coaching em tempo real para os usuários como resposta ao comportamento de risco deles.

O SecurityCoach se integra à plataforma atualizada de treinamento de conscientização em segurança da KnowBe4 e aos seus recursos de segurança existentes para fornecer feedback imediato aos seus usuários no momento em que ocorre um comportamento de risco. O SecurityCoach é um add-on opcional para os clientes da KnowBe4 que têm uma assinatura de treinamento de conscientização em segurança de nível Platina ou Diamante. O SecurityCoach usa APIs padrão para integrar de forma rápida e fácil os produtos de segurança existentes da sua organização ao console da KnowBe4. Seus recursos de segurança geram alertas que são analisados pelo SecurityCoach para identificar eventos relacionados a qualquer comportamento de risco à segurança vindo dos usuários.

Os principais benefícios do SecurityCoach são:

- Reforce a compreensão do usuário e a retenção do treinamento de segurança e das políticas de segurança estabelecidas com o coaching em tempo real sobre o comportamento em situações reais.
- Aproveite seus recursos de segurança existentes para fornecer coaching em tempo real aos seus usuários com risco e agregue um valor adicional aos investimentos existentes.
- Crie campanhas personalizadas para funções ou usuários de alto risco que são considerados grandes alvos de criminosos cibernéticos ou que continuam repetindo comportamentos de risco.
- Acompanhe e reporte o comportamento de segurança aprimorado do mundo real na sua organização, fornecendo uma justificativa para o investimento contínuo.
- Reduza os riscos de forma mensurável e desenvolva uma cultura de segurança madura em menos tempo.
- Reduza a sobrecarga da central de operações de segurança e melhore a eficácia diminuindo os alertas gerados por repetitivos comportamentos de risco relacionados à segurança.

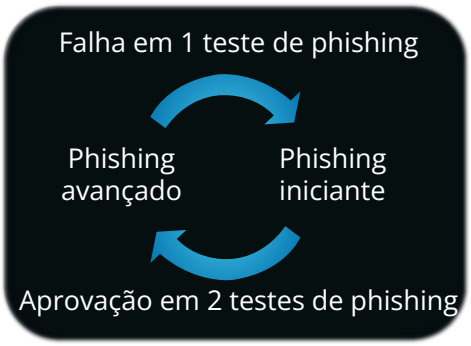
Gerenciamento de usuários

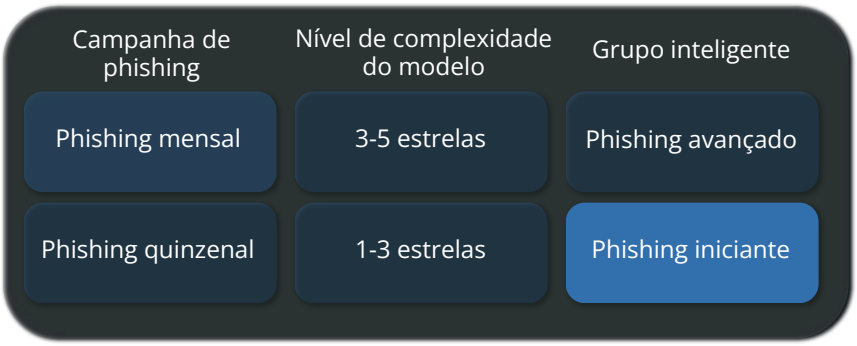
Provisionamento de usuários via Integração com o Active Directory ou com o SCIM

A KnowBe4 facilita o gerenciamento de usuários utilizando a Integração com o Active Directory (ADI) ou a Integração com o SCIM para identificar fornecedores, como Azure, Okta ou OneLogin. Tanto a Integração com o Active Directory quanto a Integração com o SCIM permitem carregar ou sincronizar dados do usuário em seu console da KnowBe4 e economizar tempo, eliminando a necessidade de gerenciar manualmente as alterações de usuários.

Grupos inteligentes

Coloque o phishing, os treinamentos e a geração de relatórios no piloto automático com os Grupos inteligentes. Automatize o processo que seus funcionários seguem para tomar decisões de segurança mais inteligentes. Nosso recurso de Grupos inteligentes, disponível para clientes Platina e Diamante, permite desenvolver campanhas dinâmicas de phishing por meio da criação de grupos com base em critérios de sua escolha. Nos Grupos inteligentes, os usuários são adicionados e removidos dinamicamente com base nesses critérios. As campanhas são consideradas dinâmicas porque os usuários passam por testes com certa frequência, de acordo com a necessidade, dependendo do seu desempenho nas campanhas de phishing. Recomendamos o uso desse recurso nos testes de phishing, nas campanhas de treinamento e na geração de relatórios exclusivos. Com o avançado recurso de Grupos inteligentes, é possível usar o comportamento dos funcionários para criar campanhas de phishing, tarefas de treinamento, aprendizado preventivo e relatórios, tudo isso sob medida.





Crie campanhas de phishing e de treinamento sem dificuldades para responder instantaneamente a quaisquer cliques de phishing com o treinamento preventivo ou notifique automaticamente os novos funcionários sobre treinamentos de integração, e muito mais. Escolha dentre cinco tipos de critérios principais por Grupo inteligente e adicione disparos, condições e ações para enviar os e-mails de phishing certos ou o treinamento ao funcionário certo no momento adequado.

O melhor de tudo é que você poderá filtrar e gerar relatórios com base nos diferentes critérios usados nas regras do Grupo inteligente. Por exemplo, filtre critérios específicos de "Eventos de phishing" e crie um relatório mostrando quais usuários estão se aprimorando ou não como resultado dos testes de phishing realizados. Isso permitirá atribuir campanhas de treinamento preventivo ou testes avançados de phishing para o Grupo inteligente em questão.

Funções de segurança

Use o recurso Funções de segurança da KnowBe4 para atribuir acesso granular a todo o console da KnowBe4. Cada função de segurança é totalmente personalizável para que você possa criar as funções exatas e necessárias à sua organização.

Visto que as funções não são apenas um conjunto de permissões predefinidas, é possível criar o modelo exato de permissões, adequado às suas necessidades. Veja abaixo algumas situações comuns nas quais as Funções de segurança permitirão que o administrador do console conceda aos usuários acesso exclusivo às partes do console da KnowBe4 necessárias para obter os resultados de que precisam:

- Auditores que precisam revisar o histórico de treinamento.
- Departamentos de RH que desejam consultar resultados de usuários individuais.
- Grupos de treinamento que desejam revisar o conteúdo do treinamento antes da implantação.

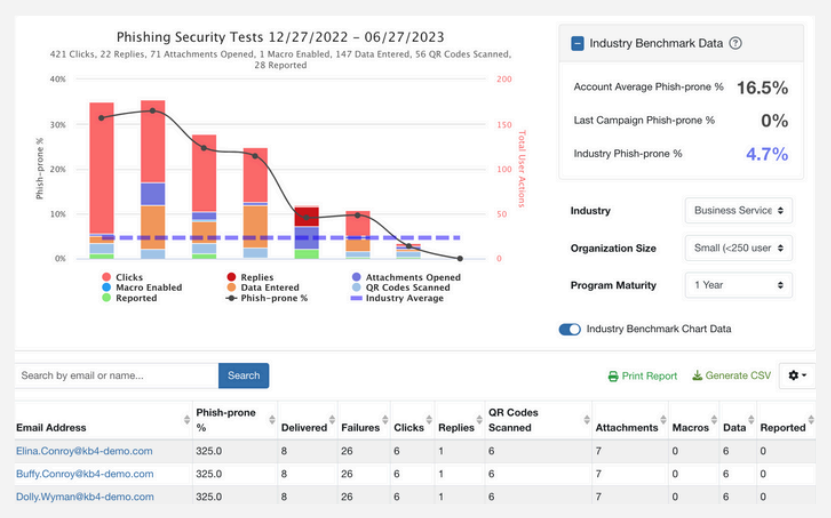
Relatórios

A plataforma de treinamento de conscientização em segurança da KnowBe4 oferece uma ampla variedade de relatórios contendo insights sobre a eficácia do seu programa de treinamento de conscientização em segurança. Você pode baixar todos os relatórios disponíveis no console como arquivo CSV ou PDF, dependendo do tipo de relatório. Obtenha mais informações sobre as diversas categorias e tipos de relatórios aqui.

Os relatórios executivos e empresariais oferecem visibilidade do desempenho de toda a sua organização em termos de conscientização em segurança, com insights sobre dados correlacionados de simulações de treinamento e phishing ao longo de um período específico. É possível até mesmo salvar os relatórios para serem visualizados posteriormente ou enviar relatórios salvos para outros usuários. Você também tem a opção de programar relatórios para serem gerados e enviados em uma frequência definida, por exemplo, trimestralmente. Use as APIs de relatórios para criar seus próprios relatórios personalizados a serem integrados a outros sistemas de Business Inteligence. Se você gerencia várias contas da KnowBe4, o recurso Agrupar relatórios simplifica a seleção de relatórios e compara os resultados de forma global entre contas e escritórios em vários locais.

O **Painel** do console contém seus relatórios de Phishing e de Nível de risco da organização. Esses relatórios fornecem informações gerais sobre a Phish-prone Percentage da sua organização no momento em que a campanha de phishing foi lançada, bem como as ações dos usuários durante as campanhas. Passe o cursor sobre os pontos da tabela para obter mais detalhes sobre campanhas de phishing específicas, saber para quantos usuários cada um dos testes foi enviado e analisar as ações dos usuários.

Continue lendo para obter mais detalhes sobre a variedade de recursos de geração de relatórios disponíveis.



Relatórios de phishing

A seção Relatórios de phishing do console da KnowBe4 oferece acesso a relatórios considerados úteis para contabilizar as ações dos usuários em várias campanhas (por exemplo, quantas vezes cada usuário clicou em um link de phishing?).

Filtre o relatório por intervalo de datas específico, campanhas específicas e campanhas enviadas a determinados usuários. Compare também falhas, e-mails de phishing denunciados (e-mails denunciados com o Phish Alert Button) ou compare os resultados por grupos.

Relatórios de treinamento

A seção Relatórios de treinamento do console da KnowBe4 oferece acesso a relatórios que mostram quais usuários fizeram login pelo menos uma vez e um relatório de quais usuários nunca fizeram login. É possível também criar relatórios com base nos cursos específicos oferecidos no console. O relatório pode ser filtrado para incluir Todos os usuários ou determinados grupos, bem como uma data de início ou de término específicas; há também a opção de incluir usuários arquivados.

Esses relatórios fornecem as seguintes informações sobre os seus usuários:

- Usuários que iniciaram seus cursos no intervalo de datas determinado
- Usuários inscritos no intervalo de datas determinado, mas que ainda não iniciaram seus cursos
- Usuários que iniciaram seus cursos no intervalo de datas determinado, mas que ainda não os concluíram
- Usuários inscritos no intervalo de datas determinado, mas que ainda não iniciaram ou não concluíram seus cursos
- Usuários que concluíram seus cursos no intervalo de datas determinado

- Usuários inscritos no intervalo de datas determinado, mas que ainda não reconheceram as políticas anexadas aos seus cursos
- Usuários que reconheceram as políticas anexadas aos seus cursos no intervalo de datas determinado

Email Exposure Check Pro

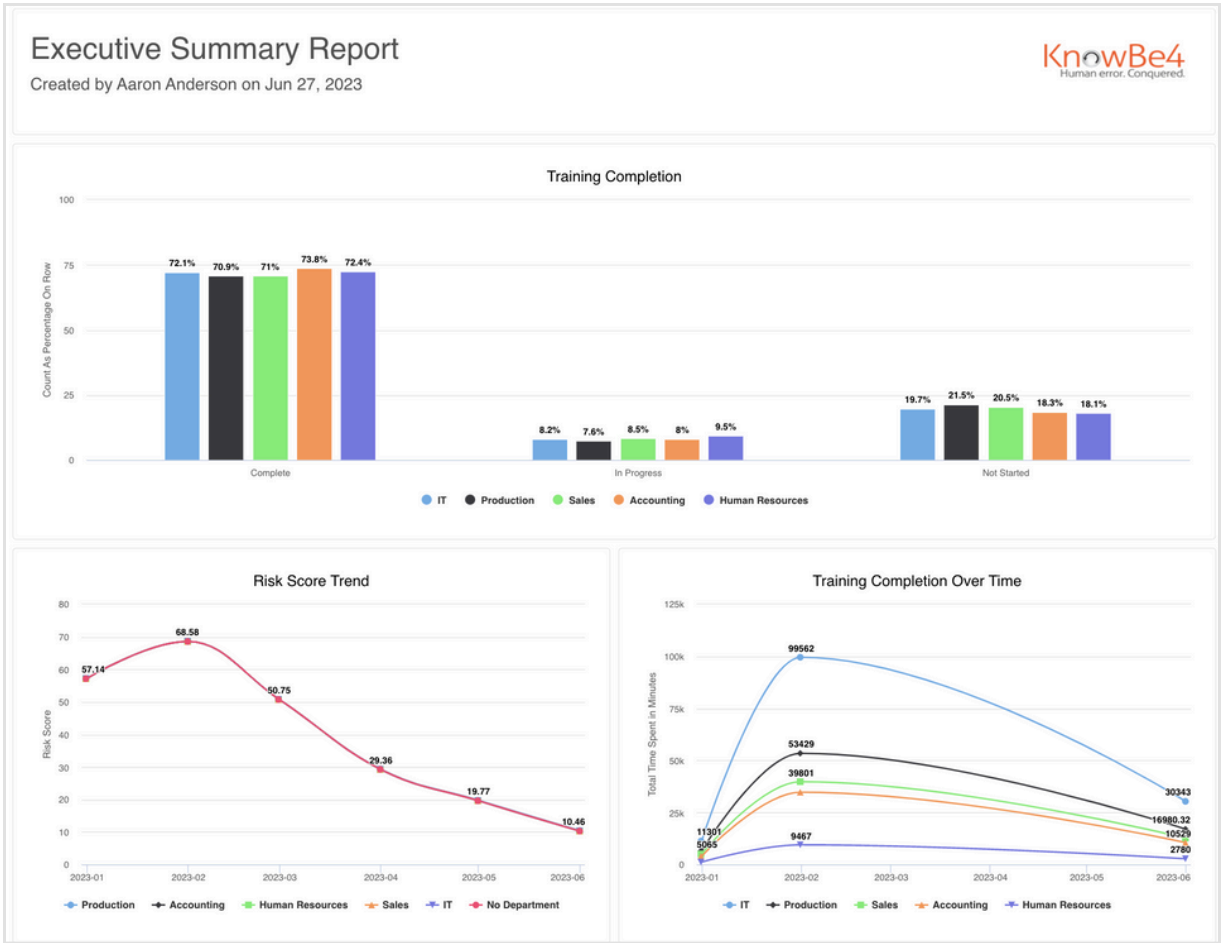
Disponível nos níveis de assinatura Ouro e superior, a ferramenta Email Exposure Check (EEC) Pro rastreia informações nas redes sociais corporativas para identificar usuários da sua organização em situação de risco e vasculha milhares de bancos de dados de violações.

Os usuários são colocados em um grupo de Distribuição de risco depois que a ferramenta EEC Pro reúne dados das pesquisas realizadas. As divisões em grupos **Risco altíssimo**, **Risco alto** e **Risco médio** se baseiam na quantidade de dados obtida sobre um usuário específico.

Relatórios avançados

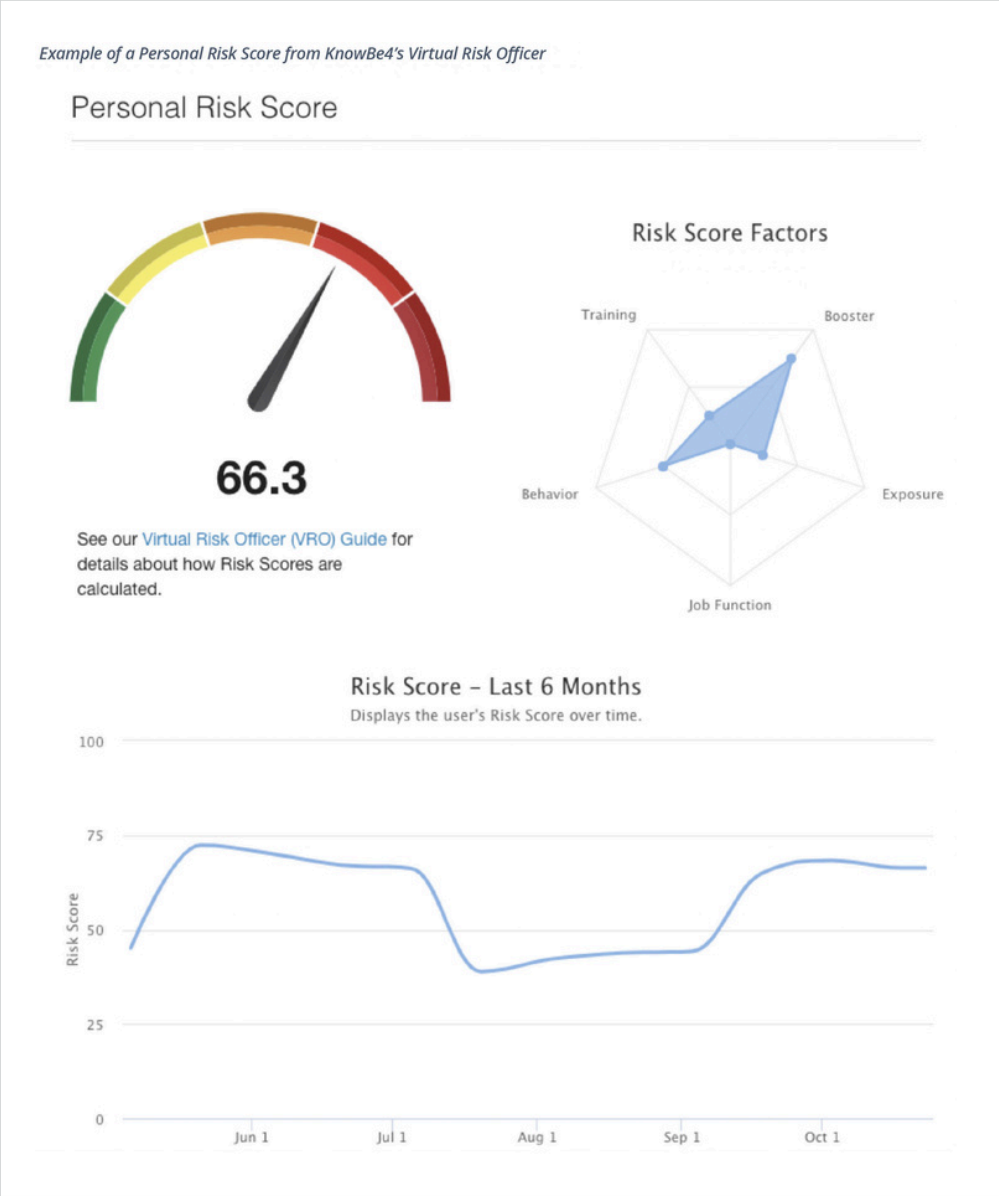
Os Relatórios avançados fornecem métricas práticas e insights sobre a eficácia do seu treinamento de conscientização em segurança. Use os Relatórios avançados para criar diversos tipos de relatórios destinados a atender às necessidades da sua organização. Esse recurso traz uma coletânea com mais de 60 relatórios incorporados, com insights que oferecem uma visão holística de toda a organização ao longo do tempo. Isso expande consideravelmente o número de relatórios detalhados instantâneos sobre vários indicadores-chave de treinamento de conscientização.

Além disso, com os **Relatórios executivos**, você pode criar e fornecer relatórios executivos personalizados que oferecem insights para ajudar a tomar decisões baseadas em dados sobre o seu programa.



Virtual Risk Officer

A função Virtual Risk Officer (VRO) ajuda você a identificar riscos no nível do usuário, do grupo e da organização, além de permitir tomar decisões controladas por dados quando se trata do seu plano de conscientização em segurança. Com o VRO, é possível monitorar a situação dos seus funcionários e da organização ao longo do tempo em termos de risco do usuário.



APIs flexíveis

Disponíveis nos níveis de assinatura Platina e superior, a KnowBe4 oferece duas APIs robustas como opções adicionais para análise e relatórios de atividades dos usuários.

- Com as APIs de relatórios, você pode extrair dados do console da KnowBe4 para fins de geração de relatórios. As APIs permitem realizar solicitações de dados de phishing, treinamento, usuários e grupos.
- Com a API de eventos do usuário, você pode integrar facilmente dados de eventos relacionados a segurança ou atividades de treinamento de seus usuários ocorridas em outras plataformas de terceiros e inseri-los no console da KnowBe4. Adicione esses eventos aos calendários dos usuários e os utilize para elevar os níveis de risco dos usuários, o que ajudará você a adaptar conteúdo específico a campanhas adicionais de phishing ou de treinamento.

PasswordIQ

Disponível no nível de assinatura Diamante, o PasswordIQ monitora continuamente a sua organização em busca de vulnerabilidades de senha detectadas no Active Directory. Ele verifica se os seus usuários estão usando senhas compartilhadas, fracas ou que apareceram em violações de dados divulgadas publicamente, para que você possa estabelecer uma linha de base dos problemas com senhas e gerenciar melhor o problema contínuo do risco de senhas entre seus usuários.

Níveis de assinatura

Nível Prata: o Nível de acesso a treinamentos I inclui o Treinamento de conscientização em segurança de Kevin Mitnick no módulo completo de 45 minutos e na versão executiva de 15 minutos. Além disso, ele inclui testes ilimitados de simulação de phishing, avaliações, o aplicativo KnowBe4 Learner, treinamento recomendado pela IA e relatórios de integridade corporativa enquanto durar a sua assinatura.

Nível Ouro: inclui todos os recursos do nível Prata mais conteúdo do Nível de acesso a treinamentos II, que também traz os módulos de treinamento da KnowBe4. O nível Ouro inclui também relatórios mensais do Email Exposure Check (EEC).

Nível Platina: inclui todos os recursos dos níveis Prata e Ouro. O nível Platina traz também nossos recursos de Phishing avançado, Grupos inteligentes, APIs de relatórios, API de eventos do usuário, Funções de segurança e Indicadores de engenharia social em páginas de destino.

Nível Diamante: inclui todos os recursos dos níveis Prata, Ouro e Platina, mais o Nível de acesso a treinamentos III, e oferece acesso total à nossa biblioteca de conteúdo com mais de 1.300 itens, incluindo módulos interativos, vídeos, jogos, pôsteres e boletins informativos relacionados ao treinamento de conscientização em segurança. Além disso, você poderá aproveitar nosso recurso de phishing controlado por IA para personalizar testes de phishing por usuário, habilitar o aprendizado opcional recomendado por IA para os seus usuários e usar o PasswordIQ para monitorar continuamente sua organização quanto a vulnerabilidades de senha detectadas no Active Directory.

Compliance Plus: disponível como add-on opcional em todos os níveis de assinatura. Interativo, relevante e envolvente, o treinamento Compliance Plus utiliza simulação de cenários reais para ajudar seus usuários a aprender como reagir diante de uma condição desafiadora. O conteúdo aborda temas difíceis, como assédio sexual, diversidade e inclusão, discriminação e ética profissional. A biblioteca do Compliance Plus inclui diversos tipos de formatos de mídia e materiais de reforço para dar suporte ao seu programa de treinamento de conformidade.

PhishER Plus: disponível como produto autônomo ou add-on opcional em todos os níveis de assinatura. O PhishER Plus é uma plataforma de SOAR leve que analisa e prioriza automaticamente as mensagens de e-mail denunciadas para identificar e colocar em quarentena os e-mails mal-intencionados em toda a organização. Além disso, ele transforma os e-mails de phishing mal-intencionados em oportunidades de treinamento, transformando-os em campanhas de phishing simulado. Com recursos adicionais de lista de bloqueio validada por IA e obtida por crowdsourcing e do PhishRIP Global para bloquear e remover proativamente ataques de phishing ativos que tenham burlado os filtros de e-mail ANTES que o usuário fosse exposto a eles, o PhishER Plus economiza consideravelmente o orçamento e o tempo do pessoal de Segurança das informações porque reduz os esforços de correção da equipe da central de operações de segurança.

SecurityCoach: disponível como um add-on opcional para os clientes da KnowBe4 que têm uma assinatura de treinamento de conscientização em segurança de nível Platina ou Diamante. O SecurityCoach é o primeiro produto de coaching de segurança em tempo real criado para ajudar as equipes de TI e operações de segurança a proteger ainda mais a maior superfície de ataque da sua organização: os funcionários. Ao introduzir uma nova categoria de tecnologia de Detecção e Resposta Humana (Human Detection and Response, HDR), o SecurityCoach ajuda a fortalecer a cultura de segurança, permitindo um coaching em tempo real para os usuários como resposta ao comportamento de risco deles.

“A engenharia social é o elo mais fraco da segurança das informações.”

– Kevin Mitnick, “O hacker mais famoso do mundo”, Consultor de Segurança de TI

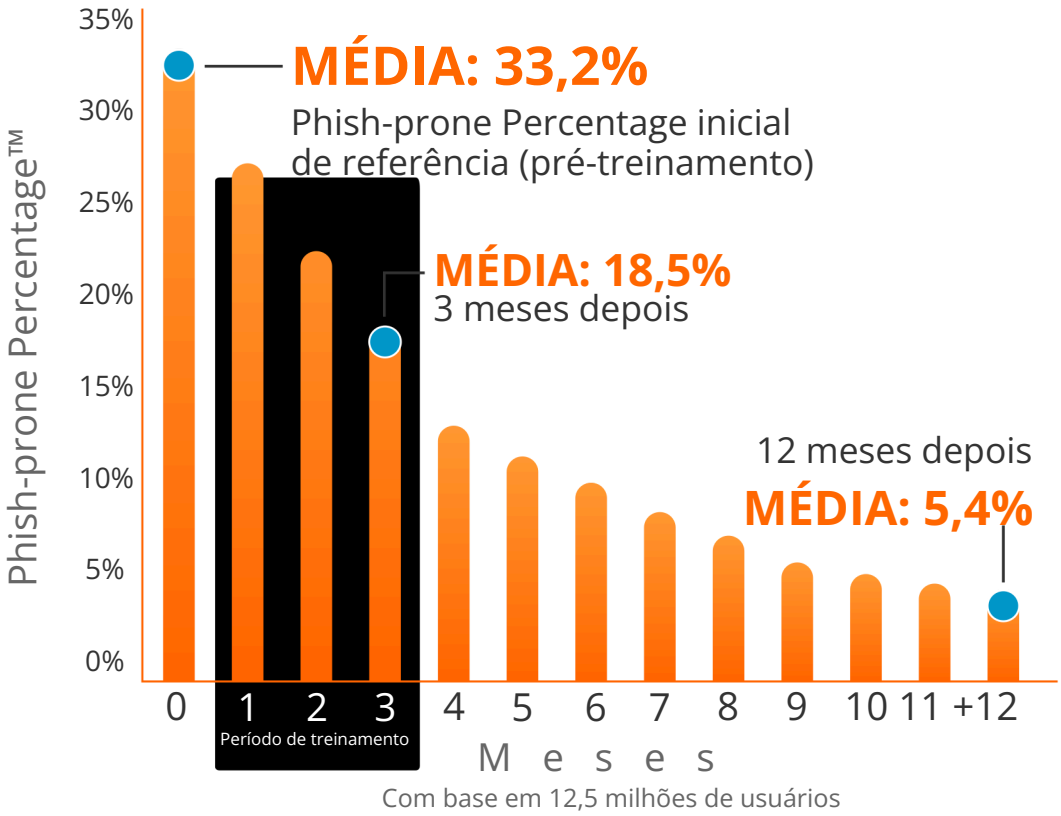
Evidência plausível de que o sistema da KnowBe4 funciona

Ao investir em treinamento de conscientização em segurança e testes de phishing, você colherá valor e retorno sobre o investimento — com rapidez.

Os resultados do relatório da KnowBe4 de benchmark de phishing por setor de 2022 mostram claramente o antes e o depois das Phish-prone Percentages das organizações após, no mínimo, 12 meses de testes regulares e treinamento de conscientização em segurança.

A Phish-prone Percentage geral e inicial do setor como um todo revelou um preocupante valor de 33,2%.

Felizmente, os dados mostraram que esse número pode ser reduzido pela metade, para 18,5%, dentro de 90 dias da implementação do nosso inovador treinamento de conscientização em segurança. Os resultados após um ano mostram que cumprir essas práticas pode reduzir a Phish-prone Percentage final para 5,4% em média.



Com base em 12,5 milhões de usuários

Fonte: 2023 KnowBe4 Phishing by Industry Benchmarking Report (Relatório de benchmark de phishing por setor de 2023 da KnowBe4)

Observação: a Phish-prone Percentage inicial é calculada com base em todos os usuários avaliados. Eles não receberam nenhum treinamento no console da KnowBe4 antes da avaliação. Os outros intervalos refletem as Phish-prone Percentages dos usuários que receberam treinamento no console da KnowBe4.