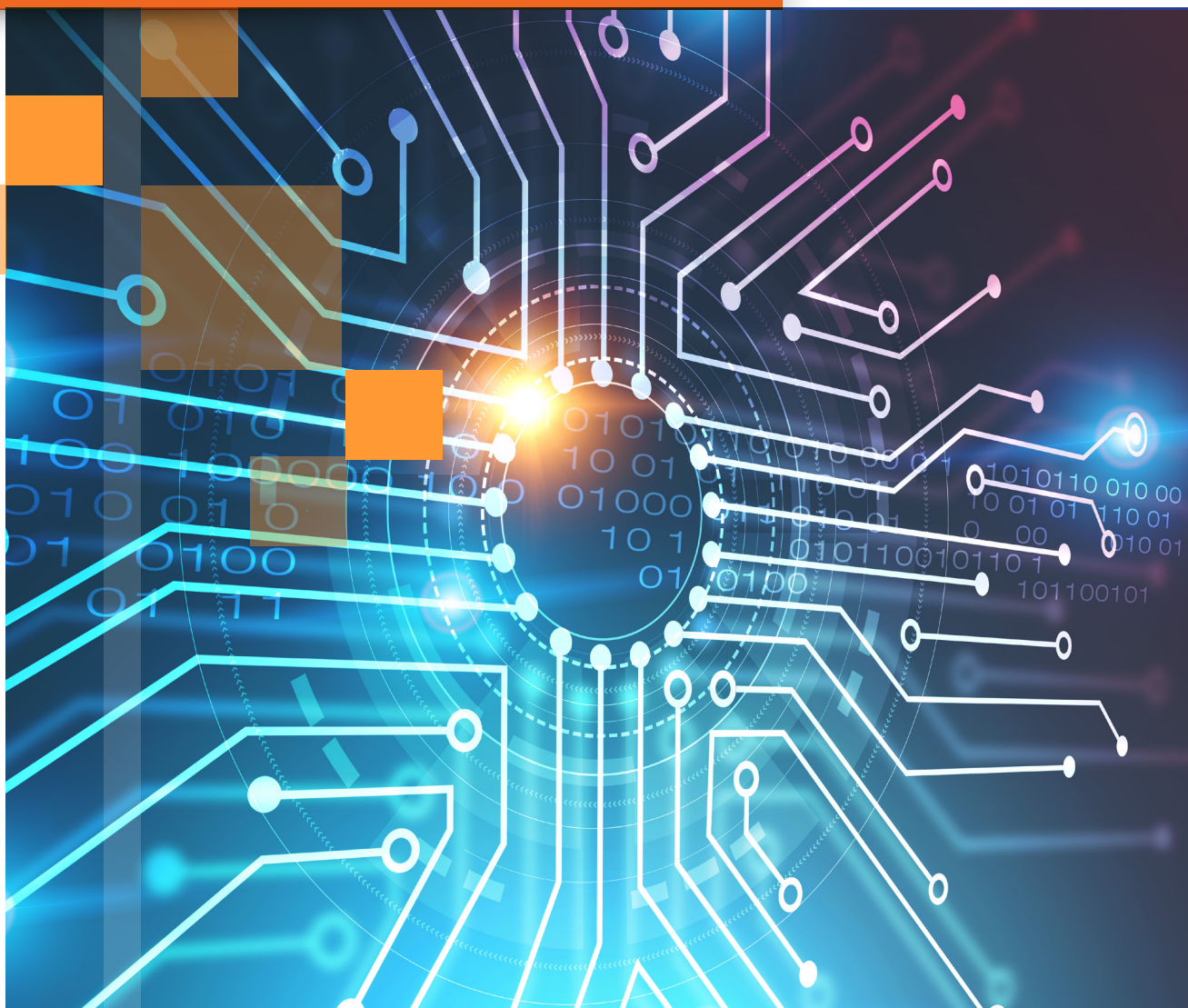
KnowBe4
Human error. Conquered.

Leitfaden für Einkäufer

Plattform für Security Awareness Trainings und Phishing-Simulationen



Leitfaden für Einkäufer:
Plattform für Security Awareness Trainings und Phishing-Simulationen

Inhaltsverzeichnis

KnowBe4 ist die weltweit größte integrierte Plattform für Security Awareness Trainings und Phishing-Simulationen. In diesem Leitfaden erfahren Sie mehr über folgende Themen:

- Die erheblichen Vorteile von Security Awareness Training
- Was die KnowBe4-Plattform bietet
- Worauf Sie bei der Auswahl eines Security-Awareness-Training-Anbieters achten sollten

Das allgegenwärtige Problem Social Engineering

Der Schwachpunkt bei der IT-Sicherheit sind Ihre Mitarbeitenden. Social Engineering ist in allen Organisationen die größte Sicherheitsbedrohung. Hinzu kommt, dass die Anzahl komplexer Cyberangriffe in alarmierendem Maße wächst. Cyberkriminelle nehmen einfache Ziele ins Visier: Mitarbeitende. Zahlreiche Reports und Whitepaper belegen die massive Zunahme der Cyberangriffe auf Organisationen in den vergangenen fünf Jahren.

Die Bedrohungsakteure setzen bei Ihren Mitarbeitenden an, deshalb ist Security Awareness Training unverzichtbar. Security Awareness Training besteht aus Kursen, die Mitarbeitenden einer Organisation die notwendigen Informationen vermitteln, mit denen sie sich und ihre Organisationen vor Verlusten und Schäden schützen können.

Ziel des Security Awareness Trainings ist es, Mitarbeitende mit dem Know-how zur Abwehr der Bedrohungen auszustatten. Sie dürfen nicht voraussetzen, dass Mitarbeitende alle Arten von Bedrohungen und die entsprechenden Sicherheitsmaßnahmen kennen. Mitarbeitende müssen vom Arbeitgeber zu gefährlichen und sicheren Verhaltensweisen geschult und für Hinweise auf Bedrohungen sensibilisiert werden. Zudem müssen sie mit Vorgehensweisen für den Ernstfall vertraut sein.

„Wir haben uns an technische Lösungen gewöhnt, [doch] Social Engineering umgeht alle Technologien, einschließlich Firewalls. Technologie ist wichtig. Wir müssen jedoch auch Menschen und Prozesse im Auge behalten. Social Engineering ist eine Form des Hackings, die auf der Beeinflussung von Menschen beruht.“

– Kevin Mitnick

Der Ansatz von KnowBe4: Phishing, Training, Analyse

KnowBe4 unterstützt Zehntausende Kunden bei der Bewältigung des allgegenwärtigen Problems Social Engineering. Wir verfügen über die weltweit größte Bibliothek mit Security Awareness Training Content wie interaktiven Modulen, Videos, Spielen, Postern sowie Newslettern und haben es uns zur Aufgabe gemacht, Ihren Mitarbeitenden Tag für Tag die richtigen sicherheitsrelevanten Entscheidungen zu ermöglichen.

KnowBe4 verschafft Ihnen einen doppelten Wettbewerbsvorteil. Erstens liefern wir Organisationen mithilfe zahlreicher Tools und Informationsfeeds einen ausführlichen Überblick über ihr aktuelles Risikoprofil. Dieser Schritt wird von Wettbewerbern häufig übersprungen, ist jedoch unverzichtbar für die Auswahl geeigneter Abwehrmaßnahmen und zur effizienten Risikominimierung. Zweitens setzt KnowBe4 auf lokale Bedrohungsdaten, sodass Sie gezielt Gefahren abwehren können, die speziell gegen Ihre Umgebung gerichtet sind und denen Sie andernfalls schutzlos ausgeliefert wären. Die meisten Anbieter von Security Awareness Trainings stützen sich in erster Linie auf allgemeine statistische Daten zu allen Phishing-E-Mail-Methoden und Kunden. Sie kommunizieren globale Trends, als ob diese auch für Sie die größte Bedrohung darstellen würden. KnowBe4 weist auf aktuelle globale Trends hin, bietet IT-Administratoren jedoch gleichzeitig die Möglichkeit zu erkennen, was Phishing-Versuche und erfolgreiche Angriffe in der jeweiligen Region vom weltweiten Gesamtbild unterscheidet und wie entsprechend reagiert werden kann.

Der Ansatz von KnowBe4 ist mehrgleisig. Im ersten Schritt ermitteln wir die spezifische Risikolage Ihrer Organisation. Anschießend bieten wir Ihnen die Möglichkeit, anhand globaler Daten und konkreter Phishing-Versuche, die in Ihrer Organisation erfolgreich waren, erfolgreiche Schutzmaßnahmen vorzubereiten:

Baseline Testing

Mit einem ersten simulierten und kostenfreien Phishing-Angriff ermitteln wir, wie anfällig Ihre Nutzer:innen für Angriffe sind (Phish-prone™ Percentage).

Nutzer:innen schulen

Profitieren Sie von der weltweit größten Bibliothek für Security Awareness Training Content mit interaktiven Modulen, Videos, Spielen, Postern sowie Newslettern und automatisierten Trainingskampagnen mit Erinnerungs-E-Mails.

Nutzer:innen testen

Nutzen Sie branchenführende, voll automatisierte simulierte Phishing-Kampagnen. Tausende Vorlagen mit unbegrenzter Nutzung sowie ständig aktualisierte Community-Phishing-Vorlagen.

Ergebnisse analysieren

Präsentieren Sie dem Management anhand detaillierter Reports mit Statistiken und Diagrammen zu Security Awareness Training und Phishing Ihre Erfolge und verbesserungsfähige Bereiche.

Im weiteren Verlauf des vorliegenden Leitfadens lernen Sie unser Angebot an Training Content und die vielfältigen Funktionen unserer Plattform für Training und Phishing-Simulationen kennen.

Trainingsbibliothek und Content mit Phishing-Simulationen von KnowBe4

Trainingsbibliothek

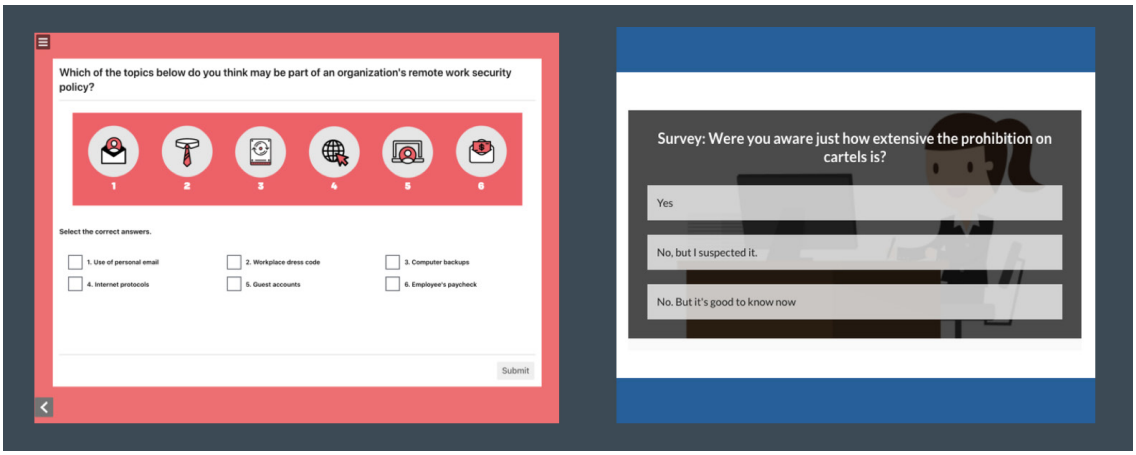
KnowBe4 bietet die weltweit größte Bibliothek mit stets aktuellem Security Awareness Training Content wie Assessments, interaktiven Trainingsmodulen, Videos, Spielen, Postern und Newslettern.

Über den ModStore können KnowBe4 Kunden einfach auf Training Content zugreifen. Als Kunde finden Sie im ModStore Inhalte, können diese durchsuchen und in einer Vorschau anzeigen. Abhängig von Ihrer Abonnementstufe können Sie auch ausgewählten Training Content zur Bibliothek in Ihrem KnowBe4-Konto hinzuzufügen.

Unsere Partnerschaften mit E-Learning- und Security-Awareness-Content-Anbietern auf der ganzen Welt machen das Angebot einzigartig und gewährleisten, dass die Trainingskampagnen für Ihre Nutzer:innen stets aktuell, relevant und ansprechend sind. Der ModStore enthält eine umfassende Auswahl an Trainingsformaten sowie Content zu zahlreichen unterschiedlichen Themen.

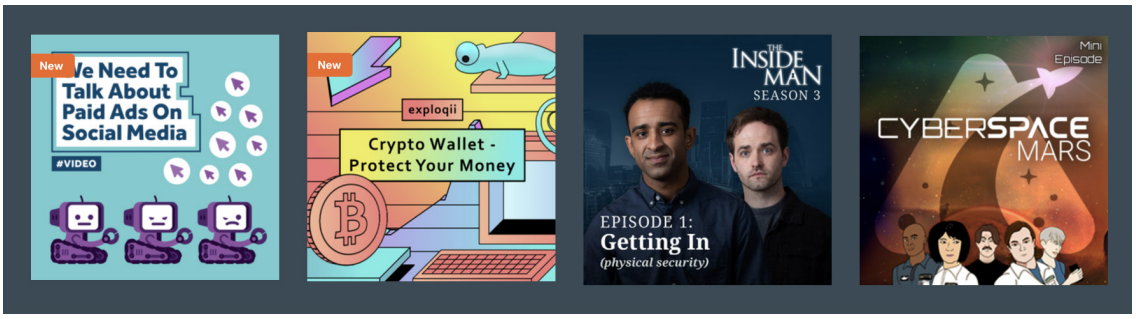
Trainingsmodule

Trainingsmodule sind interaktive Module, die ein breites Spektrum an Themen abdecken. Die Module sind SCORM-kompatibel und können zur Verwendung in Ihrem eigenen LMS heruntergeladen werden. Hunderte Trainingsmodule lassen sich mit einem eigenen Branding versehen.



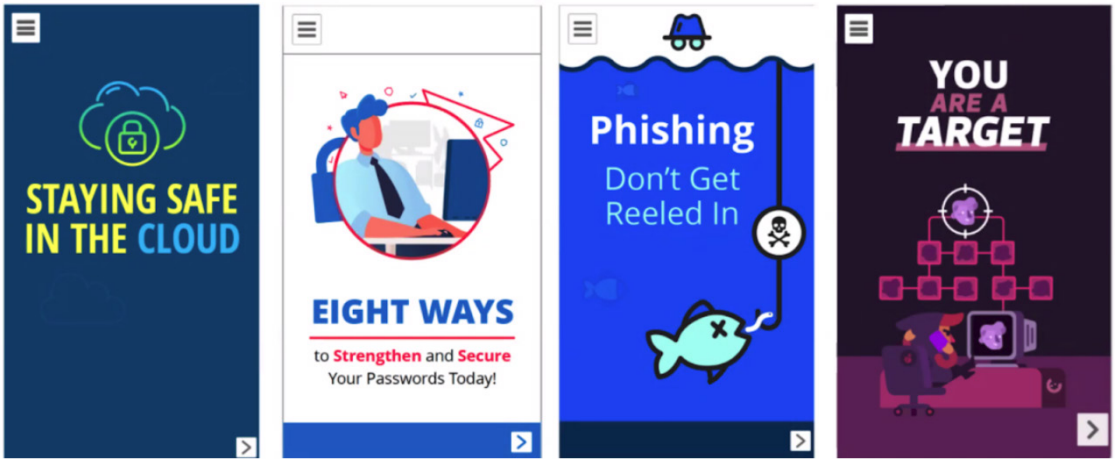
Videomodule

Bei den Videos handelt es sich um MP4-Dateien, die im Browser angezeigt oder zur Verwendung in Ihrem eigenen LMS heruntergeladen werden können.



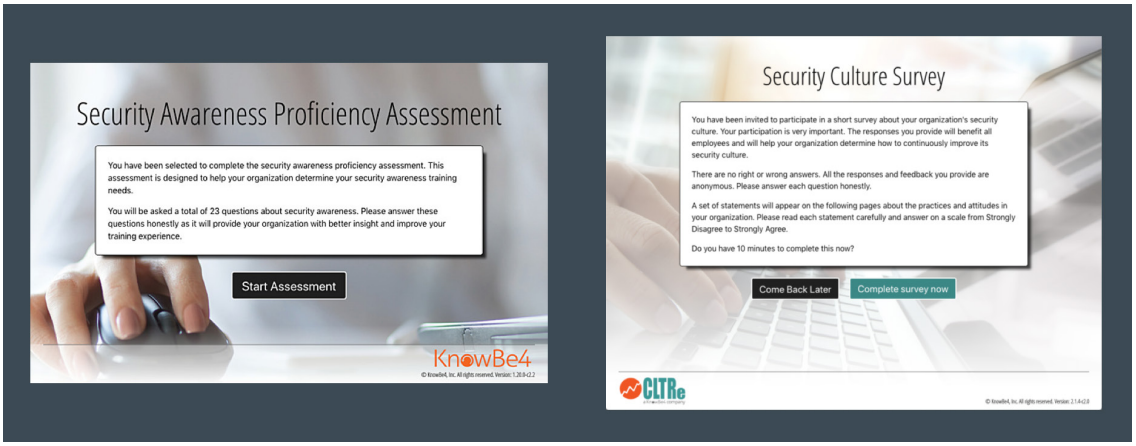
Für Mobilgeräte optimierte Module

Für Mobilgeräte optimierte Module wurden speziell an die Nutzung auf Mobilgeräten angepasst. Diese Module dauern nicht länger als fünf Minuten und sind so konzipiert, dass Nutzer:innen sie auch unterwegs oder in Regionen mit geringer Bandbreite absolvieren können. Für Mobilgeräte optimierte Module können mit einem eigenen Branding versehen werden und sind SCORM-kompatibel, sodass sie zur Verwendung in Ihrem eigenen LMS heruntergeladen werden können.



Assessments

Assessments bieten eine Übersicht über Stärken und Schwächen Ihrer Organisation. Anhand der Assessment-Ergebnisse können Sie einen gezielten Security-Awareness-Training-Plan erstellen.

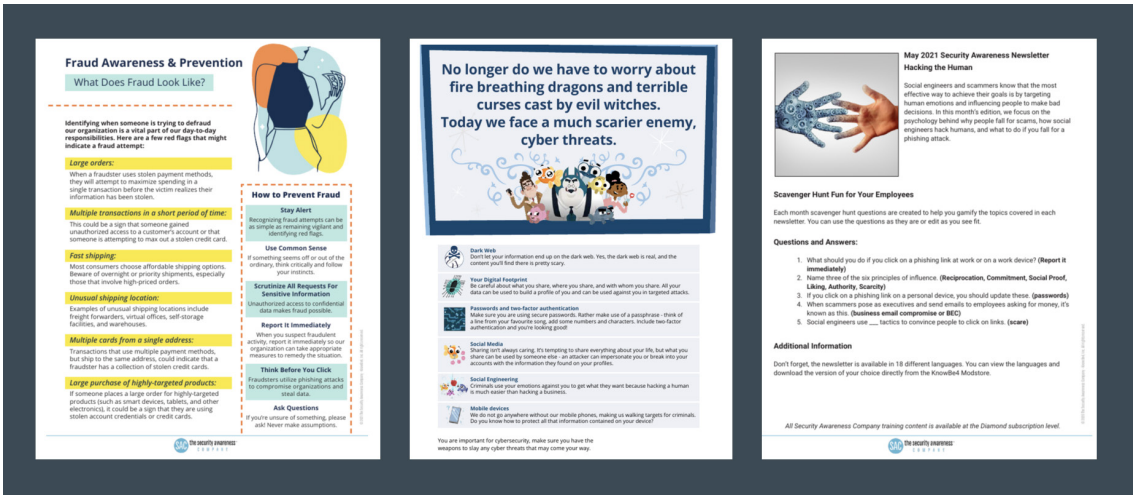


Spiele

Spiele vermitteln Lerninhalte und festigen Kompetenzen in einem ansprechenden Format. Die Spiele sind SCORM-kompatibel und können zur Verwendung in Ihrem eigenen LMS heruntergeladen werden.

Newsletter und Sicherheitsdokumente

Bei den Newslettern und Sicherheitsdokumenten handelt es sich um PDF-Dateien, die Sie ausdrucken oder Nutzer:innen in digitaler Form bereitstellen können. Diese Dokumente decken ein breites Spektrum an Cybersicherheitsthemen ab und helfen dabei, die im Training erworbenen Kompetenzen Ihrer Nutzer:innen zu festigen.



Poster und Designs

Bei Postern und Designs handelt es sich um Bilder und PDF-Dateien in hoher Qualität, die Sie ausdrucken oder Nutzer:innen in digitaler Form bereitstellen können. Wir empfehlen Ihnen, die Poster an Ihrem Standort aufzuhängen oder sie an Mitarbeitende im Homeoffice zu verteilen. Damit erhalten diese eine Gedächtnisstütze zu den sicherheitsrelevanten Aspekten, die sie bei ihrer täglichen Arbeit im Auge behalten müssen.

Trainingszugriffsstufen

Wir bieten drei Trainingszugriffsstufen an: I, II und III (abhängig von Ihrer Abonnementstufe). Der Security Awareness Training Content ist sorgfältig abgestimmt, sodass die Stufen aufeinander aufbauen. Die einzelnen Abonnements bieten unterschiedliche Stufen mit unterschiedlichen Sprachen und für Mobilgeräte optimiertem Content. Registrieren Sie sich für die KnowBe4 ModStore Training Preview, um sich mit unserer gesamten, laufend aktualisierten Bibliothek vertraut zu machen.

Trainingszugriffsstufe I (Silver)

Die Trainingszugriffsstufe I vermittelt die Grundlagen für den Aufbau eines Security-Awareness-Training-Programms. Diese Stufe eignet sich optimal für Organisationen, die noch kein Security Awareness Training durchgeführt haben und ein zumindest jährliches Trainingsprogramm ins Leben rufen möchten. Sie erhalten Trainings- und Videomodule, Assessments und Trainingsmaterialien wie Sicherheitsdokumente und Poster. Kunden beginnen häufig mit Stufe I, um ihren Nutzer:innen Security Awareness-Grundlagen zu vermitteln, einschließlich der Gefahr durch Social Engineering. Anschließend wechseln sie dann zur nächsten Stufe der Trainingsinhalte, die einen tieferen Einblick in andere Cybersicherheitsthemen bietet. Wenn ein jährliches Training nicht mehr ausreicht und Sie bereit sind, und Sie häufigere Trainingskampagnen durchführen möchten, können Sie mit den Trainingszugriffsstufen II und III ein umfassenderes und ausgereifteres Security-Awareness-Training-Programm entwickeln.

Trainingszugriffsstufe II (Gold und Platinum)

Die Bibliothek der Trainingszugriffsstufe II baut auf Stufe I auf und bietet eine größere Vielfalt an Training Content, Formaten und Themen. Von Animationen über Live-Action bis hin zu selbstbestimmtem Lernen – Stufe II eröffnet Ihnen die Möglichkeit, gezieltere Trainings anzubieten, passend zu den Rollen Ihrer Nutzer:innen, der jeweiligen Region und der Branche Ihrer Organisation. Die Auswahl an kurzen Trainingsmodulen, die höchstens fünf Minuten dauern, ermöglicht die problemlose Durchführung häufigerer Trainingskampagnen, sodass Ihre Nutzer:innen wachsam bleiben. Häufigeres Training in kürzeren Abständen kann zu einer Verhaltensänderung beitragen und Security Awareness als Verhaltensgrundlage etablieren.

Trainingszugriffsstufe III (Diamond)

Trainingszugriffsstufe III umfasst alle Trainingsinhalte der Stufen I und II sowie den Zugriff auf die umfangreichste Bibliothek mit Security Awareness Training Content, sodass Ihre Organisation ein fortlaufendes ausgereiftes Awareness-Programm anbieten kann. Stufe III umfasst mehrere preisgekrönte Videoserien in Streaming-Qualität. Die Inhalte der einzelnen Folgen beziehen sich auf die wichtigsten Best Practices zum Thema Cybersicherheit und vermitteln auf ansprechende Weise anhand praxisrelevanter Beispiele, wie die richtigen Sicherheitsentscheidungen getroffen werden. Mit einer breiten Palette an Themen, Formaten, Längen und Stilen von unterschiedlichen Content-Publishern haben Sie mehr Optionen, mit Content auf die spezifischen Bedürfnisse Ihrer Nutzer:innen einzugehen und den Content auf Ihre Organisationskultur abzustimmen. Stufe III bietet Ihnen die Möglichkeit, mit unterschiedlichen Stilen und Formaten für verschiedene Zielgruppen zu experimentieren, um das Engagement der Nutzer:innen zu maximieren. Diese Stufe bietet zusätzlich die Flexibilität, Content selbst passend zu den verschiedenen Abteilungen und regionalen Standorten Ihres Unternehmens zusammenzustellen. Sie können kürzere und häufigere Trainingskampagnen erstellen, sodass sich das Awareness-Programm einfach über das ganze Jahr verteilen lässt. Regelmäßige Kampagnen mit unterschiedlichem Content zu Best Practices im Bereich Sicherheit gewährleisten, dass die Teilnehmer wachsam bleiben. Dieser Mix mit neuem Content sorgt dafür, dass die Teilnehmer die richtigen Handlungsweisen verinnerlichen, ohne immer wieder dasselbe Training absolvieren zu müssen.

Training-Publisher

Informieren Sie sich über die unten aufgeführten Publisher und stellen Sie den optimalen Mix für Ihr eigenes ausgereiftes und vielseitiges Security-Awareness-Training-Programm zusammen.

KnowBe4

Der von KnowBe4 und dem weltberühmten Hacker Kevin Mitnick entwickelte Security Awareness Training Content zeigt anhand praxisrelevanter Beispiele, wie Cyberkriminelle vorgehen. Der Training Content von KnowBe4 gewährleistet durch die perfekte Mischung aus Grafiken und Text die Motivation der Lernenden und die Aufnahme der Informationen. Die Trainingsmodule und -videos zeichnen sich durch praktische Tipps und Hinweise, einprägsame Charaktere und eindrucksvolle Handlungsstränge aus.

Security Awareness Company (SAC)

SAC bietet abwechslungsreiches, grundlegendes und informatives Training. Fokus der Inhalte sind Verständlichkeit, Merkbarkeit und Verhaltensänderung. Das ausgewogene Kursangebot umfasst außerdem Wissenstests, Kursinteraktionen, Quizspiele, Spiele, Dokumente und monatliche Newsletter.

Popcorn Training

Wir alle mögen gute Geschichten. Dieses Training weckt Emotionen, regt die Fantasie an und motiviert die Lernenden zum Handeln. Bunte Animationen, Live-Action-Videoclips und Quizfragen helfen, das Gelernte zu festigen. Zusätzlich erhalten Sie Sicherheitsdokumente und Poster mit den Kernbotschaften.

Exploqii

Einfaches Security Awareness Training. Kurze, knappe Trainingsvideos mit lebendigen, farbenfrohen Animationen. Der Content ist leicht verständlich und ebenso leicht zu merken.

Twist & Shout

Humorvolles Edutainment, das auch in Ihrem Unternehmen ein Hit wird. Diese Videos orientieren sich an TV-Serien und stellen so einen persönlichen Bezug her. Das Training ist nachvollziehbar, realitätsnah und unterhaltsam.

El Pescador

Farbenfrohe Animationen für lebendiges Training. Die Abenteuer des unvergesslichen Kapitäns El Pescador vermitteln Lernenden in einer Vielzahl von Trainingsmodulen, Videos, Postern und Dokumenten wichtige Security-Awareness-Themen.

CLTRe

Die Umfrage zur Sicherheitskultur von CLTRe ist eine wirksame und einfache Methode, den aktuellen Stand Ihrer Sicherheitskultur einzuschätzen und deren Veränderung im Laufe der Zeit zu verfolgen. Die Umfrage zur Sicherheitskultur basiert auf bewährten sozialwissenschaftlichen Methoden und Prinzipien. Sie liefert damit zuverlässige, evidenzbasierte Ergebnisse, die es Organisationen ermöglichen, ihre Sicherheitskultur einzuschätzen, auszubauen und zu optimieren.

Saya University

Die Microlearning-Module der Saya University sind speziell auf die Gegebenheiten und die Bedrohungslage in Japan abgestimmt, damit sich Mitarbeitende vor allgemeinen Bedrohungen der Cybersicherheit schützen können.

MediaPRO

Interaktive Module und Kurzvideos vermitteln Themen wie Datenschutz, Corporate Compliance und Prävention von sexueller Belästigung spannend und einprägsam.

Compliance Plus Training

(Erhältlich als Add-on auf allen Abonnementstufen)

Das Compliance Plus Training von KnowBe4 ist interaktiv, relevant und motivierend – mit wirklichkeitsnahen, simulierten Szenarien. Ihre Nutzer:innen erfahren, wie sie auch komplexe Herausforderungen bewältigen. Der Content umfasst schwierige Themen wie sexuelle Belästigung, Vielfalt und Inklusion, Diskriminierung und Unternehmensethik. In der Compliance-Plus-Bibliothek finden Sie verschiedene Arten von Medienformaten und Materialien für Ihr Compliance-Trainingsprogramm.

Content mit Phishing-Simulationen

In unserer umfangreichen Vorlagenbibliothek finden Sie vorgefertigte Phishing-Simulationen, die in weniger als 30 Minuten über die KnowBe4-Plattform einsatzbereit sind.

E-Mail-Vorlagen

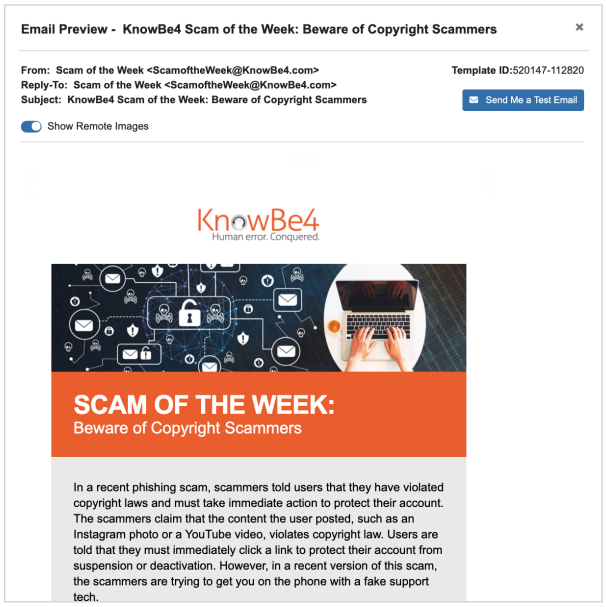
Unsere Bibliothek mit mehrsprachigen Vorlagen umfasst über 30 E-Mail-Kategorien, darunter: Banken und Finanzen, Social Media, IT, Behörden, Online-Services, aktuelle Phishing-Scams, Gesundheitswesen und viele mehr. Außerdem erhalten Sie Zugriff auf einen Community-Bereich, in dem Sie Vorlagen mit Tausenden anderer KnowBe4-Kunden austauschen können.

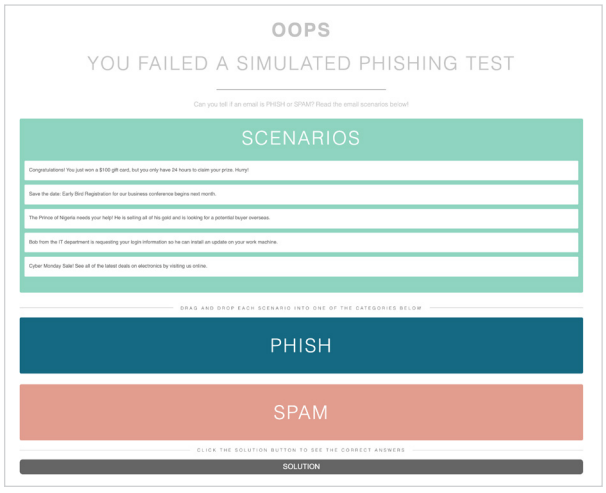
Landingpage-Vorlagen

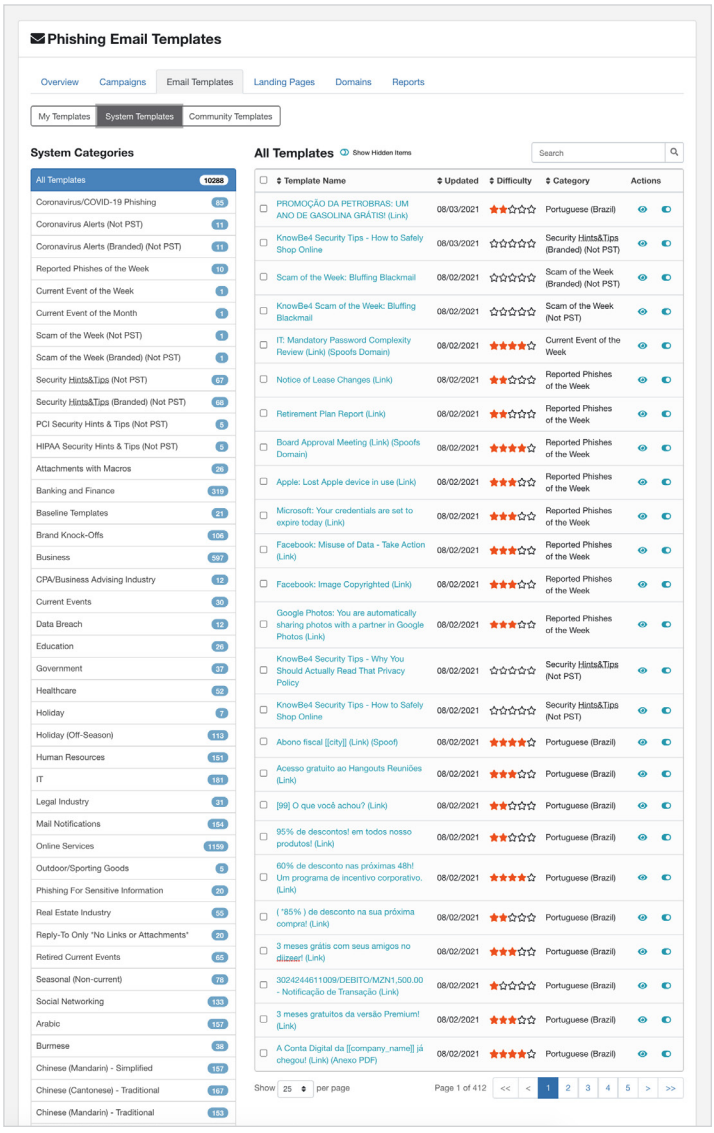
Jede Phishing-E-Mail-Vorlage kann auf eine zugehörige Landingpage verweisen, die eine Aufklärung über Points of Failure ermöglicht oder speziell auf das Phishing sensibler Informationen ausgelegt ist. Sie können aus über 200 Landingpages wählen und damit die Reaktion Ihrer Nutzer:innen auf einen Phishing-Test beeinflussen. Ihnen stehen drei Optionen zur Wahl, welche Landingpage Ihren Nutzer:innen angezeigt wird, wenn sie Phishing-Tests nicht bestehen. Sie können 1) eine Standard-Landingpage gestalten, 2) eine kampagnenspezifische Landingpage wählen oder 3) eine vorlagenspezifische Landingpage festlegen. Zudem profitieren Sie von Unterstützung für mobilgeräteoptimierte Seiten.

Newsletter

Unter den Kategorien der Phishing-Vorlagen von KnowBe4 finden Sie auch die Newsletter „Scam der Woche“ und „Security Tipps & Tricks“. Mit diesen können Sie Ihre Nutzer:innen über die neuesten Phishing-Scams informieren und grundlegende Sicherheitstipps wiederholen. Nutzen Sie diese Newsletter im Rahmen einer wöchentlichen, zweiwöchentlichen oder monatlichen Kampagne, wenn Sie eine Phishing-Kampagne in der KnowBe4-Konsole einrichten.







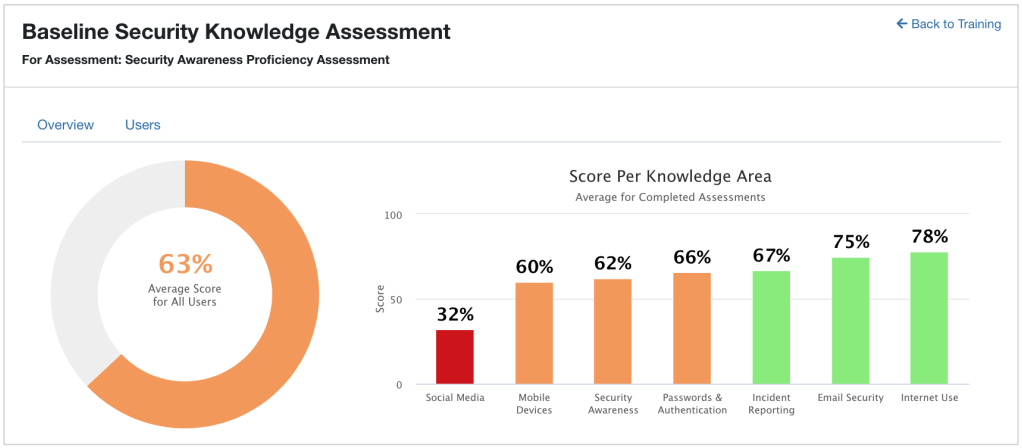
Assessments

Finden Sie heraus, wo Ihre Nutzer:innen in Bezug auf Sicherheitswissen und Sicherheitskultur stehen. Damit können Sie grundlegende Sicherheitsmetriken festlegen, die sich im Laufe der Zeit verbessern lassen.

Die Assessments von KnowBe4 sind in die KnowBe4-Plattform integriert. Ihnen entstehen keine zusätzlichen Kosten. Mit den Assessments bringen Sie in Erfahrung, welche Nutzer:innen die sichersten Verhaltensweisen in Risikosituationen kennen und wissen, wie sie diese anwenden. Mit diesem Wissen schaffen Sie ein Fundament für die gewünschte Sicherheitskultur in Ihrer Organisation und können den Erfolg Ihrer Trainingsmaßnahmen verfolgen.

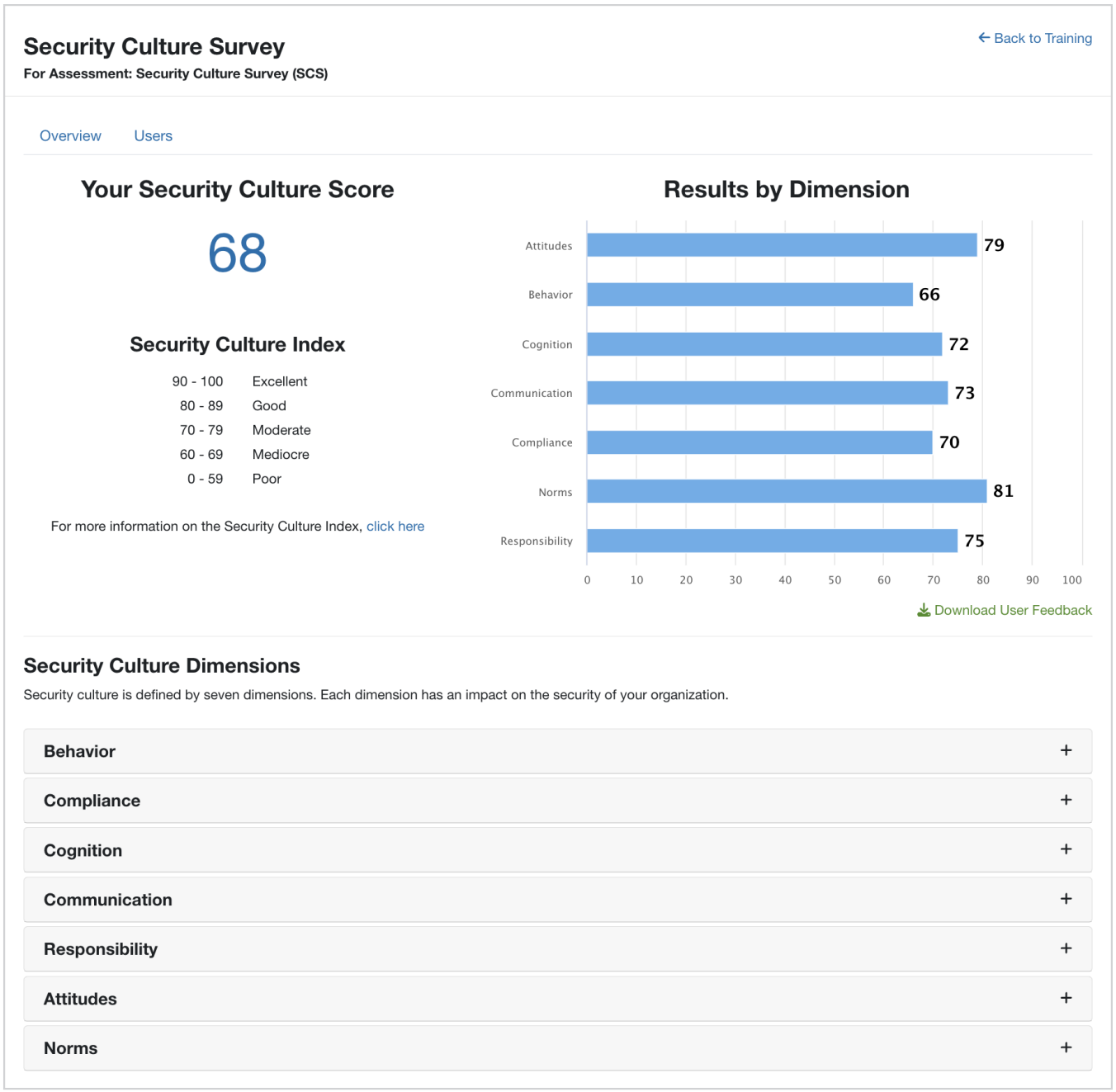
Security Awareness Proficiency Assessment (SAPA)

SAPA ist ein kompetenzbasiertes Assessment, das Wissenslücken bei einzelnen Nutzer:innen sowie empfohlene Verbesserungen aufzeigt, sodass Ihre Organisation den Bedarf an Security Awareness Training ermitteln kann.



Umfrage zur Sicherheitskultur (SCS)

Die Umfrage zur Sicherheitskultur erfasst die Einstellung Ihrer Nutzer:innen zum Thema Sicherheit in der Organisation, d. h. die psychologischen und sozialen Aspekte, die das soziale Verhalten bestimmen. Die SCS zeigt Ihnen, wie effektiv Ihr Programm zur Entwicklung der Sicherheitskultur ist und wie sich Ihre Sicherheitskultur im Laufe der Zeit verbessert.



Sowohl das SAPA als auch die SCS sind wissenschaftlich fundiert und ermöglichen die Ermittlung der Kenntnisse und Kompetenzen Ihrer Nutzer:innen rund um das Thema Sicherheit sowie die Begutachtung der allgemeinen Sicherheitskultur in der Organisation.

Mehrere Sprachen

Lokalisierte Oberfläche und vollständig übersetzte Inhalte für Phishing- und Trainingskampagnen in 35 Sprachen. Administratorkonsole in 10 Sprachen.

KnowBe4-Konsole

Die KnowBe4-Plattform ist benutzerfreundlich, intuitiv und leistungsstark. Sie wurde speziell für vielbeschäftigte IT-Mitarbeitende entwickelt, die auch zahlreiche andere Bereiche im Blick behalten müssen. Kunden jeder Größe können die KnowBe4-Plattform mindestens doppelt so schnell wie Konkurrenzprodukte einführen.

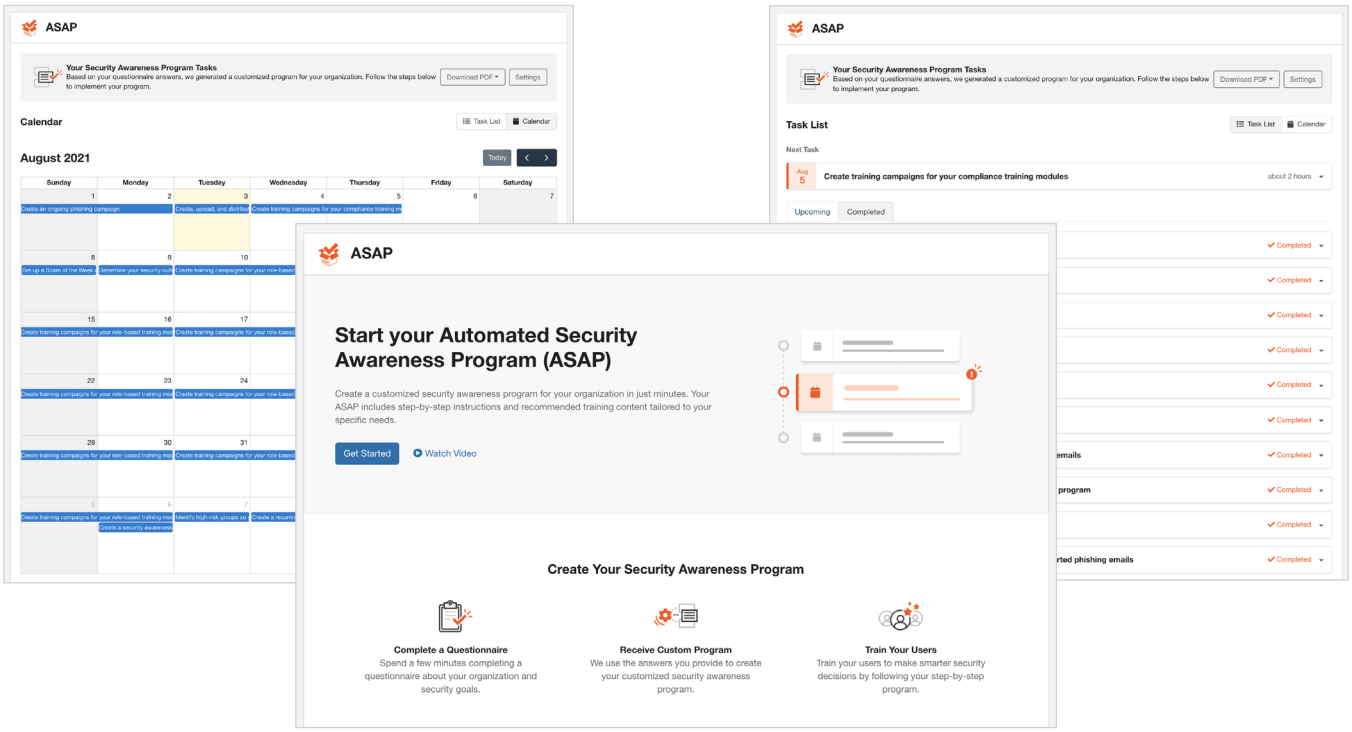
Im folgenden erfahren Sie mehr über die Funktionen der KnowBe4-Plattform.

Automated Security Awareness Program (ASAP)

Viele IT-Mitarbeitende sind unsicher, wo Sie bei der Entwicklung eines geeigneten Programms für Security Awareness Training und Sicherheitskultur in der Organisation ansetzen sollen.

Hier kommt unser Automated Security Awareness Program Builder (ASAP) ins Spiel. ASAP ist ein konsoleninternes Tool, mit dem Sie ein auf Ihre Organisation zugeschnittenes Security Awareness Program zusammenstellen können. ASAP zeigt Ihnen die Schritte, mit denen Sie in wenigen Minuten ein umfassendes Trainingsprogramm erstellen.

Durch die Beantwortung von sieben Fragen zu Ihren Zielen und Ihrer Organisation schlägt das ASAP-Tool automatisch ein Programm und einen entsprechenden Zeitplan vor. Die Programmaufgaben basieren auf Best Practices zur Erreichung Ihrer Security-Awareness-Ziele.



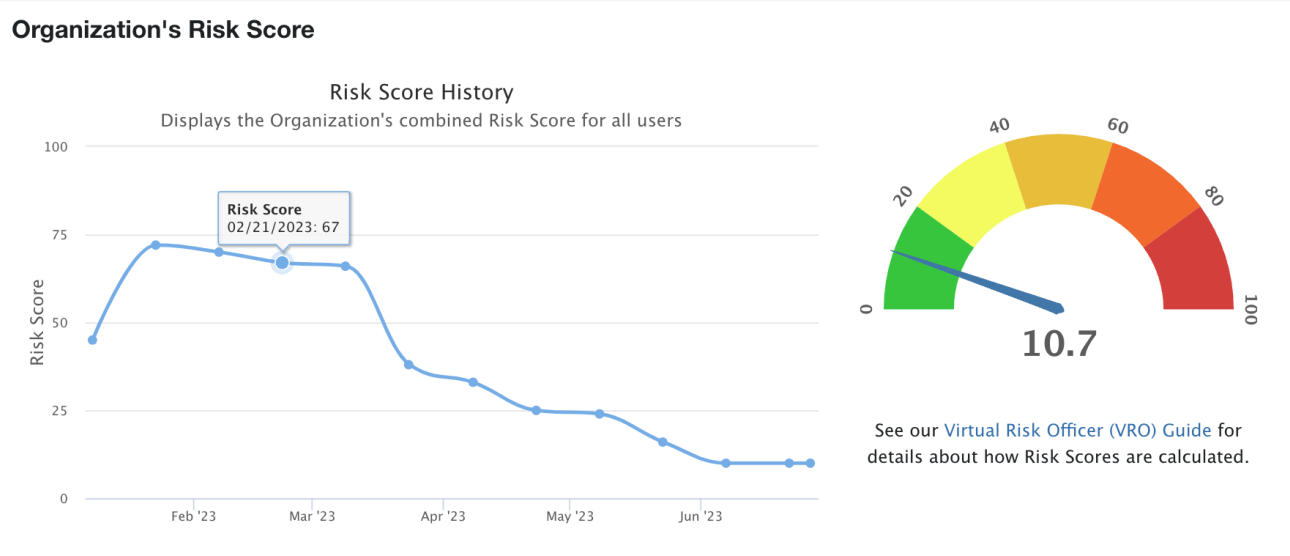
Das Programm enthält praktische Aufgaben, hilfreiche Tipps, Vorschläge für Training Content sowie einen Kalender für die Aufgabenplanung. Ihr kundenspezifisches Programm kann dann vollständig über die KnowBe4-Konsole durchgeführt werden. Sie haben auch die Möglichkeit, das fertige Programm ausführlich oder als Zusammenfassung für Führungskräfte im PDF-Format zu exportieren, um Compliance- und/oder Reporting-Anforderungen zu erfüllen.

Konsolen-Dashboard

Auf dem Phishing- und Trainingsdashboard sehen Sie den Risk Score der Organisation und Ihrer Endnutzer:innen auf einen Blick und im Vergleich zu anderen Organisationen Ihrer Branche.

Risk Score der Organisation anzeigen

Zeigen Sie den Gesamt-Risk-Score der Organisation an, der auf Basis der Risk Scores der einzelnen Mitarbeitenden berechnet wird.



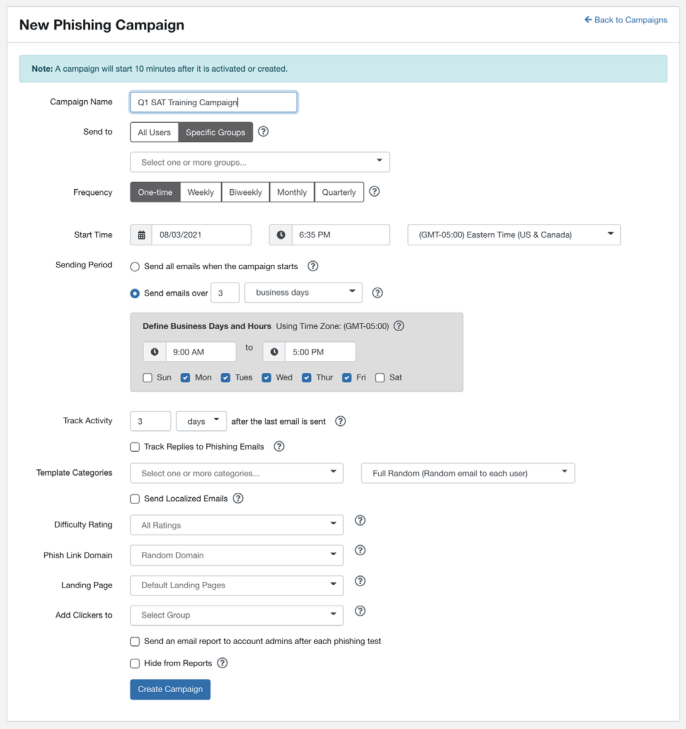
Ergebnisse zum Phish-prone Percentage

Unsere Plattform bietet verschiedene Möglichkeiten, anhand von Phishing- und Assessment-Ergebnissen den Fortschritt von Endnutzer:innen mit dem in ähnlichen Branchen zu vergleichen. Mit dieser Dashboard-Funktion können Sie den Phish-prone Percentage Ihrer Organisation (bzw. die Wahrscheinlichkeit, dass Nutzer:innen auf eine Phishing-E-Mail klicken) im Vergleich zu anderen Organisationen Ihrer Branche ermitteln.

Plattform für Phishing-Simulationen

KnowBe4 bietet einen neuen Ansatz für das Training von Nutzer:innen in Bezug auf Phishing-Bedrohungen. Sie können Phishing-Kampagnen erstellen, in deren Rahmen Ihre Nutzer:innen E-Mails mit simulierten Phishing-Angriffen erhalten. Es werden tatsächliche Phishing-Angriffe simuliert. Dadurch lernen Nutzer:innen, wachsam zu bleiben.

KnowBe4-Kunden können während der Abonnementlaufzeit eine unbegrenzte Anzahl von simulierten Phishing Security Tests (PSTs) durchführen. Im weiteren Verlauf erfahren Sie mehr über die beliebtesten Funktionen unserer Phishing-Plattform.

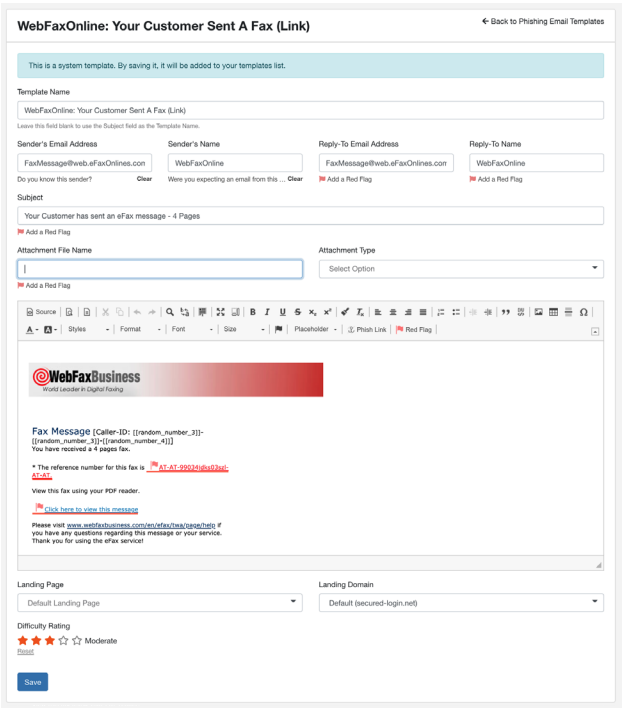


Phishing-Kampagnen

Mit der KnowBe4-Plattform können Sie ermitteln, für welche Arten von Angriffen Ihre Nutzer:innen anfällig sind, sowie die Nutzer:innen schulen, auf Warnsignale zu achten. Außerdem lässt sich der Phish-prone Percentage Ihrer Organisation berechnen. Erstellen Sie zum Testen Ihrer Nutzer:innen zunächst Phishing-Kampagnen. Durch diese erfahren Sie, welche Trainings Ihre Nutzer:innen benötigen. Sie können dann ein entsprechendes Trainingsprogramm zusammenstellen.

Phishing-Tests planen

Sie können Phishing-Tests mithilfe unserer umfangreichen Bibliothek planen, die über 25.000 Vorlagen in mehr als 40 Sprachen umfasst, oder Community-Vorlagen wählen, die von Administrator:innen für Administrator:innen erstellt und geteilt wurden. Wählen Sie zwischen einmaligen, wöchentlichen, zweiwöchentlichen oder monatlichen simulierten Phishing-Angriffen. Sie sehen sofort, welche Mitarbeitenden auf diese Social-Engineering-Angriffe hereinfallen. Und mit der einzigartigen „Anti-Prairie Dog"-Funktion von KnowBe4 können Sie während einer Phishing-Kampagne zufällig ausgewählte Phishing-Vorlagen zu ebenfalls zufällig ausgewählten Zeitpunkten versenden. Damit imitieren Sie echte Phishing-Angriffe und verhindern, dass sich die Nutzer:innen gegenseitig über laufende Phishing-Tests informieren.



Phishing-Vorlagen anpassen

Sie können sämtliche Systemvorlagen anpassen und auch Anhänge und Makros mit simulierten Inhalten einfügen. Sie haben die Möglichkeit, eigene Phishing-E-Mail-Vorlagen von Grund auf neu zu erstellen oder vorhandenen Vorlagen anzupassen und an Ihre Nutzer:innen zu senden. Sie können sogar noch einen Schritt weiter gehen und Szenarien mithilfe öffentlich zugänglicher und/oder vertraulicher Informationen gestalten sowie gezielte Spear-Phishing-Kampagnen mit Feldern für personalisierte Daten erstellen.

Phishing-E-Mails lassen sich auf unserer Plattform mit Logos versehen und wirken damit authentisch. Die eingebetteten Links verweisen auf die ursprüngliche URL-Adresse des Logos. Damit wird das Bild ausschließlich beim Eigentümer des Logos gehostet. Folglich gibt es keine Probleme mit den Urheberrechten.

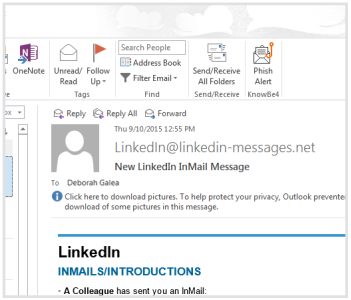
Phish Alert Button

Der KnowBe4 Phish Alert Button erlaubt es Nutzer:innen, E-Mails zur Analyse direkt an das IT-Security-Team weiterzuleiten. Gleichzeitig wird die E-Mail aus dem Postfach gelöscht. Und das alles mit nur einem Klick! Beim Phish Alert Button (PAB) für Microsoft 365 können Sie Ihrer PAB-Instanz Sprachen hinzufügen, sodass die im System der Nutzer:innen festgelegte Sprache verwendet wird.

- Wenn Nutzer:innen in einem simulierten Phishing Security Test auf den Phish Alert Button klicken, wird diese korrekte Reaktion gemeldet.
- Wenn Nutzer:innen den Phish Alert Button für eine nicht simulierte Phishing-E-Mail verwenden, wird die E-Mail direkt an Ihr Incident-Response-Team weitergeleitet.
- Schaltflächentext und Benutzerdialogfelder sind vollständig anpassbar.
- Unterstützte Clients: Outlook 2016, 2019, 2021 sowie Outlook für Microsoft 365, Exchange 2016, 2019 und 2021, Outlook im Web (Outlook.com), die Outlook Mobile App (iOS und Android), Chrome 80 und höher (Linux, OS X und Windows), Gmail-Konten mit Google Workspace-Anbindung; Gmail-Add-on mit Gmail im Browser und mobilen Clients kompatibel.

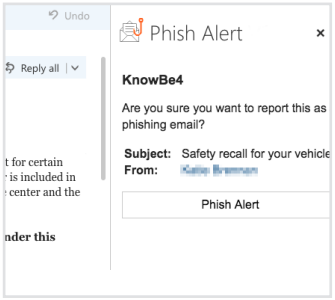
Outlook-Symbolleiste

Fügt einen Phish Alert Button für Ihre Nutzer:innen hinzu



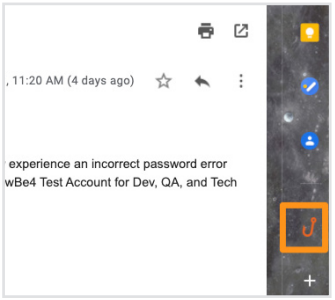
Microsoft 365-Add-in-Bereich

Fügt einen Phish Alert Button für Ihre Nutzer:innen hinzu



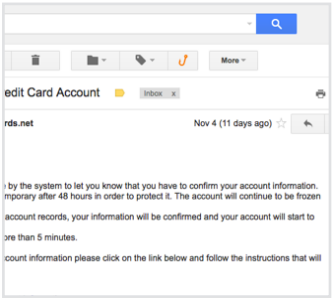
Gmail-Add-on

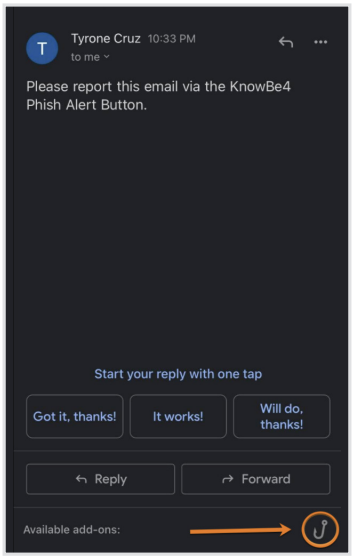
Fügt einen Phish Alert Button für Ihre Nutzer:innen hinzu



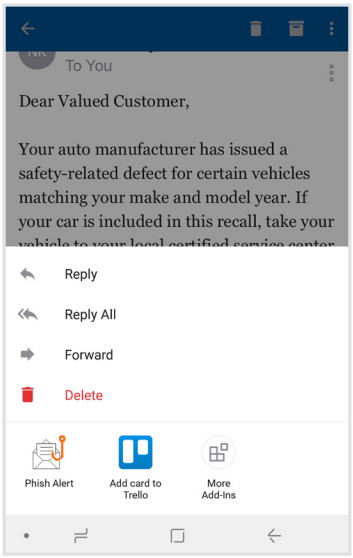
Gmail-Erweiterung

Fügt einen Phish Alert Button für Ihre Nutzer:innen hinzu

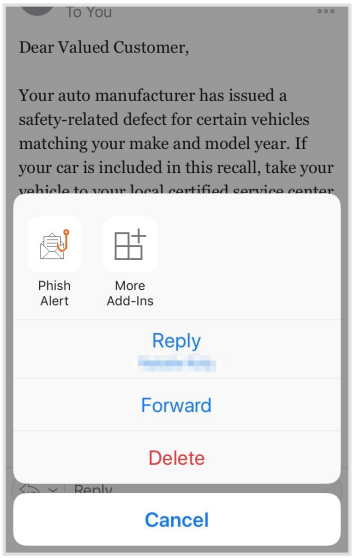




Gmail Mobile (Android)



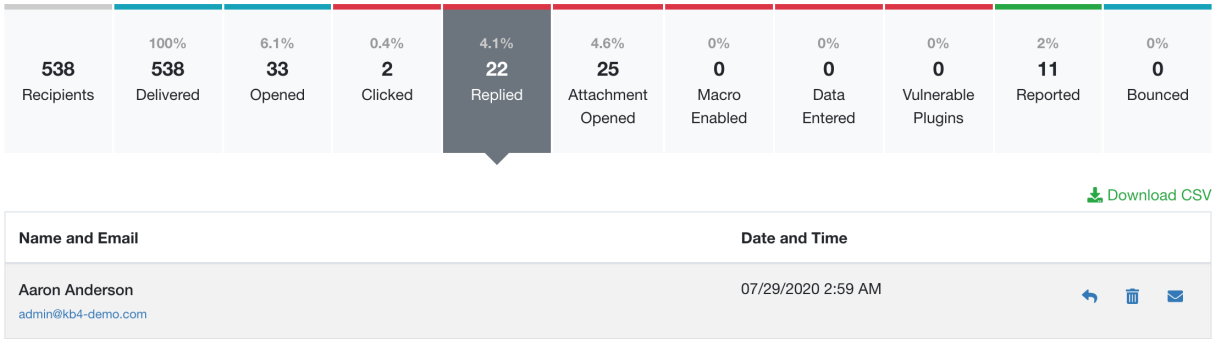
Outlook Mobile (Android)



Outlook Mobile (iOS)

Phishing Reply Tracking

Mit dem Phishing Reply Tracking von KnowBe4 können Sie verfolgen, ob Nutzer:innen auf E-Mails mit simulierten Phishing-Versuchen antworten und die Informationen in der Antwort zur Überprüfung in der KnowBe4-Konsole erfassen. Unter der Kategorie „Reply-To Online“ finden Sie spezielle, vom System generierte Phishing-Vorlagen, mit denen Sie prüfen können, ob Nutzer:innen Kontakt mit Angreifern aufnehmen. Das Phishing Reply Tracking funktioniert jedoch auch mit allen anderen unserer Phishing-Vorlagen.



Das Phishing Reply Tracking ist benutzerfreundlich und über die Option „Antworten auf Phishing-E-Mails tracken“ standardmäßig für neue Phishing-Kampagnen aktiviert.

Kundenspezifische Phish-Domains

Phish-Domain ist unsere Bezeichnung für die URL, die in der unteren linken Bildschirmecke angezeigt wird, wenn Sie den Mauszeiger über einen Link in einer verdächtigen E-Mail bewegen. Sie können aus einer Vielzahl verschiedener Phish-Domains wählen, damit die angezeigte URL stetig wechselt und Ihre Endnutzer:innen gefordert bleiben.
Mit dem unbegrenzten Domain-Spoofing können Sie bei Kampagnen mit simulierten Phishing-Versuchen beliebige E-Mail-Adressen spoofen.

Erweiterte Phishing-Funktionen

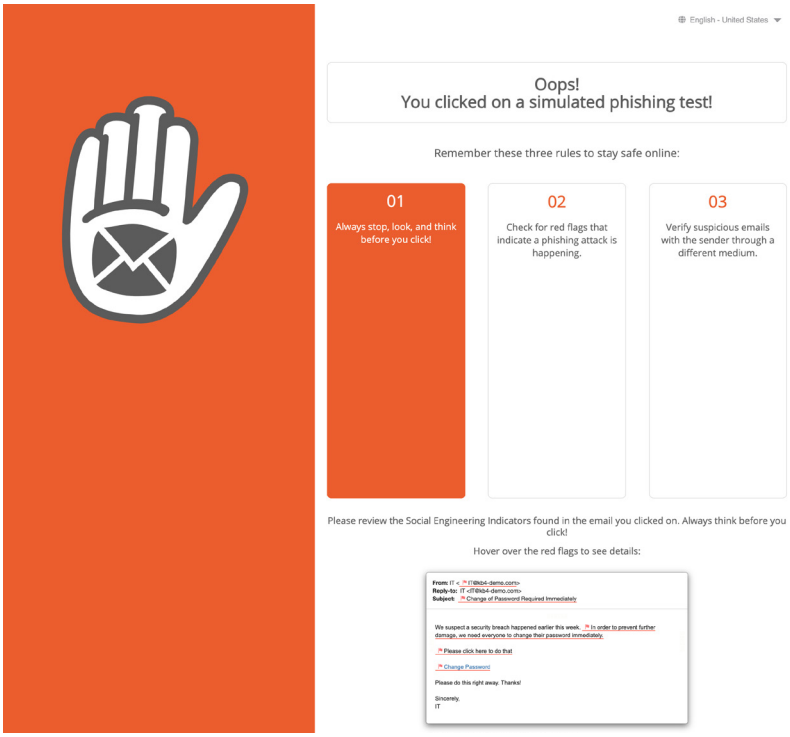
Ausgewählte Abonnementstufen bieten zusätzliche Möglichkeiten, unsere Phishing-Plattform optimal einzusetzen. Im weiteren Verlauf erfahren Sie mehr über diese Funktionen.

Social Engineering Indikatoren

Bei unseren Social Engineering Indikatoren (SEI) handelt es sich um eine patentierte Technologie, mit der jede simulierte Phishing-E-Mail zu einem Tool der IT-Abteilung für das Training von Mitarbeitenden wird.

Wenn ein:e Nutzer:in auf eine simulierte Phishing-E-Mail von KnowBe4 klickt, wird er bzw. sie auf eine Landingpage weitergeleitet, die eine dynamische Kopie dieser Phishing-E-Mail mit Hinweisen auf alle Warnsignale enthält. Sie können auch sämtliche simulierten Phishing-E-Mails anpassen und eigene Warnsignale erstellen.

So lernen Nutzer:innen, Fallstricke unmittelbar zu erkennen, oder sie merken sich die übersehenen Warnsignale für die Zukunft.



USB Drive Test

Über die KnowBe4-Konsole können ganz einfach einen eigenen USB Drive Test und speziell präparierte Microsoft Office-Dateien herunterladen. Sie können diese Dateien ggf. umbenennen und Mitarbeitende so verleiten, die Dateien zu öffnen. Speichern Sie die Dateien anschließend auf einem beliebigen USB-Stick, den Sie dann an einem stark frequentierten Ort im Unternehmen ablegen können. Wenn ein Mitarbeitender den USB-Stick an seinen Computer anschließt und die Datei öffnet, meldet das System den Fehler sowie Informationen wie die Zugriffszeit und IP-Adresse. Aktiviert ein:e Nutzer:in auch die Makros in der Datei, werden zusätzliche Daten wie Benutzername und Computername erfasst und in der Konsole verfügbar gemacht.

QR-Code-Phishing

Sie können Nutzer:innen nicht nur anhand von Phishing-Links oder E-Mail-Anhängen testen, sondern auch mithilfe von QR-Codes. QR-Codes (QR steht für Quick Response) sind kompakte Barcodes, die gescannt werden können und Daten enthalten. Nutzer:innen, die einen schädlichen Barcode scannen, können beispielsweise auf eine gefährliche Website weitergeleitet werden. Außerdem können in QR-Codes schädliche Links versteckt sein, die die Sicherheitsfilter Ihrer Organisation umgehen.

In Kampagnen mit QR-Code-Postern können Sie testen, wie Ihre Nutzer:innen reagieren, wenn sie auf einen zu diesem Zweck platzieren QR-Code stoßen. Wenn Nutzer:innen beispielsweise an einem vertrauten Ort ein Poster mit QR-Code sehen, scannen sie diesen möglicherweise und öffnen den Link – ohne vorherige Prüfung. QR-Code Phishing Security Tests können dazu beitragen, Ihre Nutzer:innen auf tatsächliche Phishing-Angriffe mit QR-Codes vorzubereiten.

KI-gestütztes Phishing

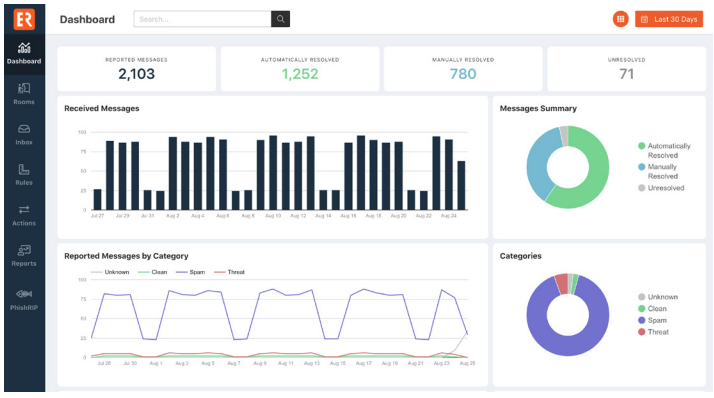
KI-gestütztes Phishing wählt automatisch die beste Phishing-Vorlage für jeden Ihrer Nutzer aus, basierend auf dessen individuellem Trainings- und Phishing-Verlauf. Mit den Daten von AIDA (Artificial Intelligence Driven Agent), einer Engine für Empfehlungen von KnowBe4, können einzigartige Vorlagen für Phishing Security Tests automatisch und dynamisch für Ihre Nutzer:innen ausgewählt werden.

Es ist wie ein eigener KI-Phishing-Assistent, der automatisch den für jede:n Nutzer:in in diesem Moment besten Phishing-Test auswählt. Beim KI-gestützten Phishing erstellen Sie im Grunde für jeden Ihrer Nutzer:innen eine eigene Phishing-Kampagne. So können Sie sicherstellen, dass jede:r Nutzer:in simulierte Phishing-Tests erhält, die auf sein bzw. ihr individuelles Niveau zugeschnitten sind. Bieten Sie Ihren Nutzer:innen ein personalisiertes Training, das ihrem aktuellen Wissensstand entspricht.

Callback-Phishing

Als Administrator oder Administratorin können Sie mit der Callback-Phishing-Funktion in Ihrer KnowBe4-Konsole eine simulierte Callback-Phishing-Kampagne durchführen, um herauszufinden, ob Ihre Mitarbeitenden auf diese Art von Trick hereinfallen würden. Die Mitarbeitenden erhalten eine E-Mail mit einer Telefonnummer und einem Code. Rufen sie diese Nummer an, werden die Mitarbeitenden aufgefordert, den Code anzugeben. Der springende Punkt: Die Eingabe des Codes ist nur der erste Fehler. Zusätzlich wird geprüft, ob auch noch personenbezogene oder sensible Daten eingegeben werden.

PhishER Plus



PhishER Plus ist als Add-on zu jeder Abonnementstufe erhältlich. Es handelt sich um eine einfache und benutzerfreundliche webbasierte Plattform, die Ihrem InfoSec- und Security Operations-Team hilft, das Spamaufkommen zu überblicken und auf die gefährlichsten Bedrohungen zu reagieren. PhishER Plus wurde entwickelt, um die E-Mail-Sicherheit Ihrer Organisation zu stärken. Es bildet eine zusätzliche letzte Sicherheitsebene, sofern Ihre vorhandenen SEG- und anderen Cybersicherheitstool versagen. PhishER Plus ermöglicht einen wichtigen Arbeitsablauf, mit dem Ihre IR-Teams (Incident Response) gemeinsam die Risiken von Phishing-Angriffen mindern können. Das Tool eignet sich für Organisationen, die nach einer präzisen und schnellen Lösung zum automatischen Priorisieren und Verwalten potenziell schädlicher Nachrichten suchen. Wenn Sie KnowBe4 und PhishER Plus gemeinsam in Ihren E-Mail-Sicherheitsworkstream integrieren, entlasten Sie nicht nur Infosec- und IR-Teams und identifizieren echte Bedrohungen, sondern erhöhen auch deutlich die Effektivität Ihres Security-Awareness-Training-Programms.

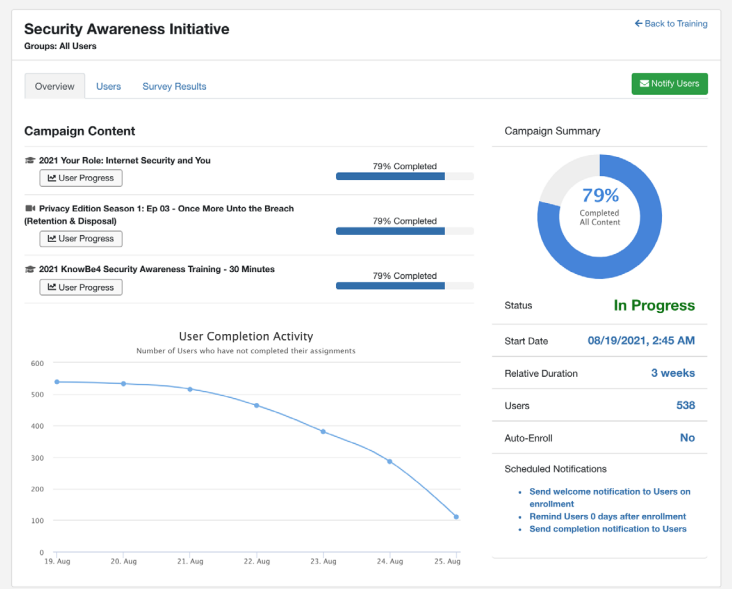
Die wichtigsten Vorteile von PhishER Plus:

- Freisetzung von Ressourcen für die Reaktion auf Zwischenfälle sowie Ermittlung und Bearbeitung des 90%igen Anteils an Nachrichten, bei denen es sich um Spam bzw. legitime E-Mails handelt.
- Anzeigen von Nachrichtenclustern oder -gruppen mit ähnlichem Muster zur Erkennung von großflächigen Phishing-Angriffen auf Ihre Organisation
- Mithilfe von Einträgen in der globalen Blockliste von validierten Bedrohungen – gemeldet von mehr als 10 Millionen geschulten Nutzern und Nutzerinnen – werden übereinstimmende neue eingehende Nachrichten automatisch blockiert, bevor sie in den Posteingängen Ihrer Nutzer und Nutzerinnen landen. Dieser fortlaufend aktualisierte Bedrohungsfeed wird von KnowBe4 verwaltet und mit Ihrem Microsoft 365-E-Mail-Server synchronisiert.
- Bei PhishMLTM handelt es sich um ein Machine-Learning-Modul der PhishER Plus-Plattform, das sämtliche Nachrichten analysiert, die auf der PhishER Plus-Plattform eingehen, und Informationen liefert, die die Priorisierung vereinfachen, beschleunigen und präzisieren.
- Die globale PhishRIP-Funktion ist eine Quarantänefunktion für E-Mails mit Unterstützung für Microsoft 365 und Google Workspace, dank der Ihr IR-Team schnell reagieren und Maßnahmen ergreifen kann. Nachrichten, die mit einer von anderen PhishER Plus-Kunden und -Kundinnen erkannten Phishing-Bedrohung übereinstimmen und aus den Posteingängen dieser Organisation entfernt wurden, werden im Anschluss vom Threat Research Lab von KnowBe4 überprüft.
- PhishFlipTM ist eine Funktion von PhishER Plus, bei der von Nutzer:innen gemeldete tatsächliche Phishing-Angriffe im Rahmen sicherer Kampagnen mit simulierten Phishing-Angriffen eingesetzt werden.

Trainingsplattform

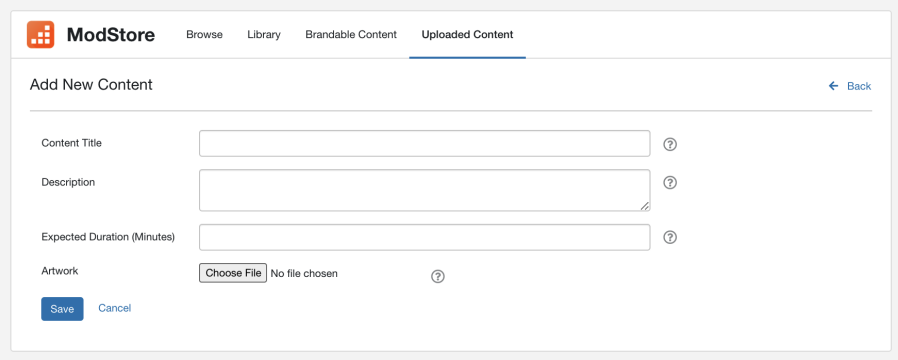
Trainingskampagnen

In der KnowBe4-Konsole lassen sich schnell kontinuierliche oder befristete Kampagnen erstellen, Trainingsmodule nach Nutzergruppen auswählen, neue Nutzer:innen automatisch anmelden und Erinnerungs-E-Mails an Nutzer:innen, die ein Training nicht abgeschlossen haben, automatisieren. Es stehen anpassbare Vorlagen für Trainingsbenachrichtigungen zur Verfügung und Sie können Richtlinien für die Nutzerbestätigung vorbereiten sowie Trainingsreports anzeigen. Mithilfe von Trainingskampagnen können Sie den Training Content für Ihre Nutzer:innen im Nutzerbereich anpassen und verwalten.



Optionen des Learning-Management-Systems

Laden Sie mit dem zuverlässigen Learning-Management-System von KnowBe4 Ihren SCORM-kompatiblen Training und Video Content in allen verfügbaren Sprachen einfach in den KnowBe4 ModStore und koordinieren Sie Ihren gesamten Training Content an einem einzigen Ort – ohne zusätzliche Kosten.

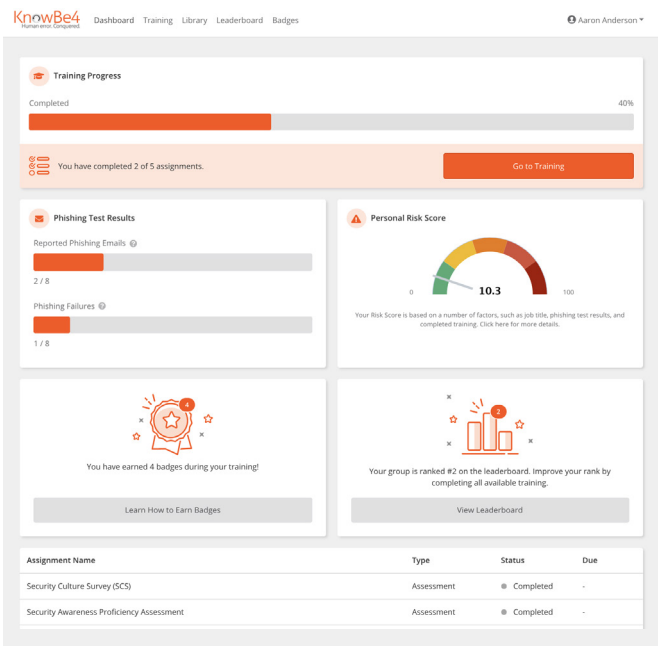


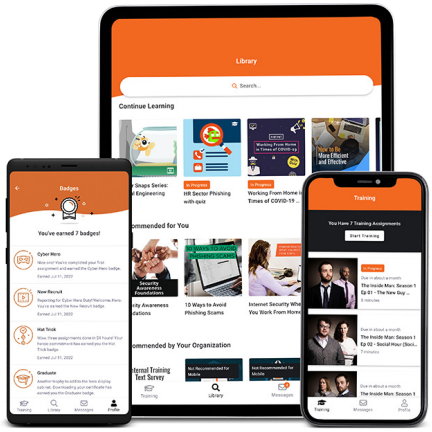
Nutzerbereich

Der Nutzerbereich von KnowBe4 ermöglicht die Anpassung des Security-Awareness-Training-Plans und bietet ansprechende Gamification-Optionen.

Nutzer:innen können ihre Leistungen anhand von Bestenlisten vergleichen und Abzeichen verdienen – während sie zugleich lernen, wie sie die Organisation vor Cyberangriffen schützen. Eine informative, optionale Einführung macht Ihre Nutzer:innen mit der neuen Lernumgebung vertraut.

Der Nutzerbereich enthält auch das Nutzer-Dashboard. Hier finden Nutzer:innen eine Übersicht über absolvierte Trainings, einschließlich des Trainingsstatus und der Fälligkeitstermine. Optional können Sie die Phishing-Testergebnisse, den persönlichen Risk Score und Gamification-Statistiken Ihrer Nutzer:innen anzeigen.





KnowBe4 Learner App

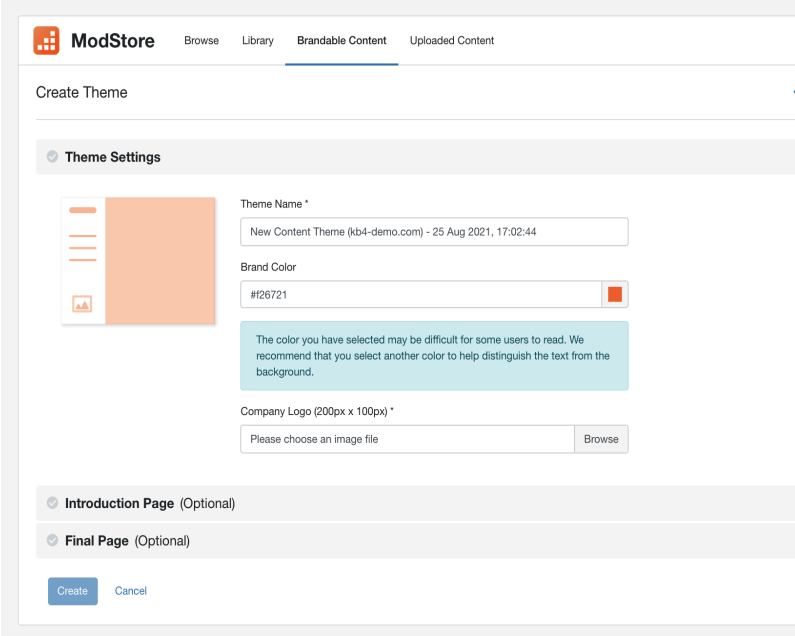
Mit der KnowBe4 Learner App können Nutzer:innen die ihnen zugewiesenen Trainingsinhalte bequem über ein Tablet, ein Smartphone oder andere Mobilgeräte absolvieren. Verstärken Sie den Schutz Ihrer größten Angriffsfläche. Denken Sie auch an Mitarbeitende, die während der Arbeit in der Regel keinen Desktop-PC oder Laptop verwenden. Wir haben eine App entwickelt, die sich gleichermaßen an Nutzer:innen und Administrator:innen richtet.

Die KnowBe4 Learner App ist ohne Zusatzkosten in Ihrem Abonnement enthalten und bietet Ihren Nutzer:innen die Möglichkeit, flexibel und rund um die Uhr zu lernen. Die App ist für iOS- und Android-Geräte verfügbar. Sie können Push-Benachrichtigungen für eigene Ankündigungen, Updates bei zugewiesenem Training sowie KnowBe4-Newsletter aktivieren.

Anpassbare Module

Mit der Funktion „Anpassbare Module“ können Sie ein individuelles Design erstellen und auf aktive Trainingskampagnen mit geeigneten Inhalten anwenden. Auf der Registerkarte „Anpassbare Module“ können Sie die Farbe Ihres Brandings festlegen, ein Unternehmenslogo hochladen sowie eine Einführungs- und eine Abschlussseite hinzufügen. Diese optionalen Seiten enthalten Ihr Unternehmenslogo, benutzerdefinierten Text und ein Bild Ihrer Wahl.

So bieten Sie Mitarbeitenden ein vertrautes Erscheinungsbild. Sie haben auch die Möglichkeit, die Zertifikate mit dem Branding Ihrer Organisation in die KnowBe4-Plattform hochzuladen. Mit den unternehmensspezifischen Abschlusszertifikaten können Sie Nutzer:innen zum Ende der einzelnen Trainingsmodule auszeichnen.



Content Manager

Mit dem Content Manager lassen sich Training-Content-Präferenzen ganz einfach festlegen. Sie können die zum Bestehen erforderliche Punktzahl anpassen, individuelle Designs nutzen, Befreiungsprüfungen zulassen und das Überspringen von Content unterbinden. Und das Beste: Der Content Manager steht bei allen Abonnementstufen zur Verfügung.

KI-Trainingsempfehlungen

Der KnowBe4 ModStore bietet mithilfe von Machine Learning fundierte Trainingsvorschläge, die anhand von Performance-Metriken Ihrer Nutzer:innen aus Phishing Security Test-Kampagnen erfolgen. Der ModStore ist auf den allgemeinen Phish-prone Percentage der Organisation abgestimmt und schlägt Trainingsmodule vor, mit denen Sie die Klickraten Ihrer Nutzer:innen im Laufe der Zeit senken können.

Optionale Lerninhalte für Nutzer:innen

Optionale Lerninhalte lassen sich für Ihre Nutzer:innen aus zusätzlichem Training Content im KnowBe4 ModStore zusammenstellen. Erstellen Sie einfach spezifische Trainingskampagnen mit optionalem Training Content, die Sie Ihren Nutzer:innen im Rahmen eines Self-Service-Modells zu Verfügung stellen möchten. Unseren Diamond-Kunden steht die fortschrittliche Option „Empfohlene optionale KI-Lerninhalte“ zur Verfügung. Nutzer:innen kann mithilfe dieser Option auf Grundlage bereits abgeschlossener Kurse zusätzlicher Training Content empfohlen und bereitgestellt werden, ohne dass eine separate Trainingskampagne eingerichtet werden muss.

SecurityCoach

SecurityCoach ist das erste Echtzeit-Sicherheitscoaching, das IT- und SOC-Teams dabei unterstützt, die größte Angriffsfläche Ihrer Organisation zu schützen – Ihre Mitarbeitenden. Mithilfe der neuen Technologie Human Detection and Response (HDR) stärkt SecurityCoach Ihre Sicherheitskultur, indem Ihre Nutzer:innen bei riskantem Verhalten ein Echtzeit-Coaching erhalten.

SecurityCoach lässt sich in die New-School Security Awareness Training Platform von KnowBe4 und in Ihren Security Stack integrieren, um Nutzer:innen unmittelbares Feedback als Reaktion auf riskantes Verhalten bereitzustellen. SecurityCoach steht Platinum- oder Diamond-Abonnenten als optionales Add-on zur Verfügung. SecurityCoach verwendet Standard-APIs, um die in Ihrer Organisation vorhandenen Sicherheitsprodukte schnell und einfach in Ihre KnowBe4-Konsole zu integrieren. Ihr Security Stack generiert Warnungen, die dann von SecurityCoach analysiert werden, um jene Ereignisse zu identifizieren, die auf das riskante sicherheitsrelevante Verhalten Ihrer Nutzer:innen zurückgehen.

Wesentliche Vorteile von SecurityCoach:

- Besseres Verständnis und Festigung der Kenntnisse der Nutzer:innen in Bezug auf Security Awareness Training und der geltenden Sicherheitsrichtlinien durch Echtzeit-Coaching zum tatsächlichen Verhalten
- Nutzung des vorhandenen Security Stack für das Echtzeit-Coaching von Nutzer:innen mit Risiko und optimale Nutzung getätigter Investitionen
- Benutzerdefinierte Kampagnen für Nutzer:innen mit hohem Risiko, die ein lohnendes Ziel für Cyberkriminelle darstellen oder die sich wiederholt riskant verhalten
- Daten und Reports über Verbesserungen im Sicherheitsverhalten in Ihrer gesamten Organisation, mit denen sich eine fortgesetzte Investition rechtfertigen lässt
- Nachweisbare Verringerung des Risikos durch den Aufbau einer ausgereiften Sicherheitskultur in kurzer Zeit
- Weniger Belastung für Ihr SOC und höhere Effizienz, da weniger Warnmeldungen aufgrund von wiederholt riskantem Verhalten eingehen

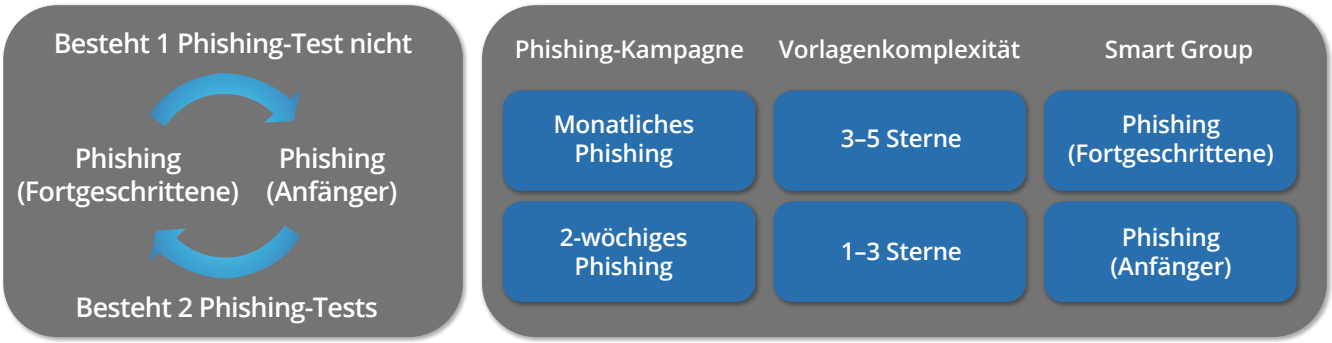
Benutzermanagement

Nutzerbereitstellung über Active Directory- oder SCIM-Integration

KnowBe4 erleichtert das Benutzermanagement mithilfe der Active Directory-Integration (ADI) oder SCIM-Integration für Identitätsanbieter wie Microsoft Entra ID, Okta oder OneLogin. Active Directory- und SCIM-Integration ermöglichen den Upload und die Synchronisierung der Daten von Nutzer:innen Ihrer KnowBe4-Konsole. Sie sparen Zeit, da Änderungen an den Daten von Nutzer:innen nicht mehr manuell vorgenommen werden müssen.

Smart Groups

Mit Smart Groups automatisieren Sie Phishing, Training und Reports. Sorgen Sie dafür, dass Ihre Mitarbeitenden automatisch die richtigen Entscheidungen treffen, wenn es um IT-Sicherheit geht. Unsere für Platinum- und Diamond-Kunden verfügbare Funktion „Smart Groups“ ermöglicht dynamische Phishing-Kampagnen, indem Sie Gruppen auf Basis selbstgewählter Kriterien erstellen. Nutzer:innen werden anhand dieser Kriterien dynamisch zu Smart Groups hinzugefügt bzw. aus ihnen entfernt. Bei als dynamisch bezeichneten Kampagnen basiert die Häufigkeit, mit der Nutzer:innen getestet werden, auf deren bei Phishing-Kampagnen erzielten Ergebnissen. Die Funktion eignet sich bestens für Phishing-Tests, Trainingskampagnen und die Generierung einzigartiger Reports. Mit der leistungsstarken Funktion „Smart Groups“ lassen sich Verhalten und Nutzerattribute aller Mitarbeitenden für die individuelle Gestaltung von Phishing-Kampagnen, Trainingsaufgaben, Wiederholungen und Reports verwenden.



Sie können Phishing- und Trainingskampagnen erstellen, die nach der Konfiguration vollständig automatisiert durchgeführt werden. Mitarbeitenden, die auf Phishing-Versuche hereinfallen, lässt sich so beispielsweise unmittelbar ein zusätzliches Training zuweisen, neue Mitarbeitende können automatisch zu einem Onboarding-Training eingeladen werden u. v. m. Sie haben bei jeder Smart Group die Wahl zwischen fünf Hauptkriterien und können dann Trigger, Bedingungen und Aktionen hinzufügen, damit die richtigen Mitarbeitende zur richtigen Zeit die richtigen Phishing-E-Mails oder Trainings erhalten.

Das Beste daran ist, dass Sie Reports auf Basis der verfügbaren Kriterien filtern und aufrufen können, die Sie in Ihren „Smart Group“-Regeln verwenden. So können Sie beispielsweise nach bestimmten Kriterien eines Phishing-Ereignisses filtern und einen Report erstellen, aus dem hervorgeht, welche Nutzer:innen sich durch die von Ihnen durchgeführten Phishing-Tests verbessert bzw. nicht verbessert haben, damit Sie dieser Smart Group unterstützende Trainingskampagnen oder fortgeschritten Phishing-Tests zuweisen können.

Sicherheitsrollen

Die KnowBe4-Funktion „Sicherheitsrollen“ dient der präzisen Steuerung des Zugriffs auf die einzelnen Bereiche der KnowBe4-Konsole. Sämtliche Sicherheitsrollen lassen sich uneingeschränkt organisationsspezifisch anpassen.

Die Rollen sind mehr als einfach eine Reihe vordefinierter Berechtigungen. Sie ermöglichen das Erstellen eines Berechtigungsmodells, das Ihren spezifischen Anforderungen entspricht. Im Folgenden finden Sie einige gängige Szenarien, in denen der Konsolenadministrator mithilfe von Sicherheitsrollen den Nutzer:innen Zugriff nur auf die Teile der KnowBe4-Konsole gewähren kann, die für sie erforderlich sind:

- Auditoren, die den Trainingsverlauf überprüfen müssen
- Personalabteilungen, die die Ergebnisse einzelner Nutzer:innen einsehen möchten
- Trainingsgruppen, die Training Content vor der Bereitstellung überprüfen möchten

Reporting

Die Security Awareness Training-Plattform von KnowBe4 bietet eine breite Palette an Reports, die einen Einblick in die Wirksamkeit Ihres Trainingsprogramms zur Security Awareness liefern. Jeder in der Konsole verfügbare Report kann abhängig vom jeweiligen Typ als CSV- oder PDF-Datei heruntergeladen werden. Hier erfahren Sie mehr über die verschiedenen Reportkategorien und -typen.

Reports auf Geschäftsführungs- und Organisationsebene bieten einen Überblick über die Security-Awareness-Performance der gesamten Organisation sowie Insights zu korrelierten Trainings- und Phishing-Simulationsdaten über einen beliebigen Zeitraum. Reports lassen sich für die spätere Verwendung speichern und auch an andere Nutzer:innen senden. Außerdem können Sie Reports in bestimmten Intervallen, z. B. vierteljährlich, erstellen und versenden lassen. Nutzen Sie die Reporting-APIs, um eigene benutzerdefinierte Reports zu erstellen und in andere BI-Systeme zu integrieren. Wenn Sie mehrere KnowBe4-Konten managen, lassen sich mit dem Roll-up-Reporting ganz einfach Reports auswählen und die Ergebnisse über mehrere Konten oder Niederlassungen hinweg vergleichen.

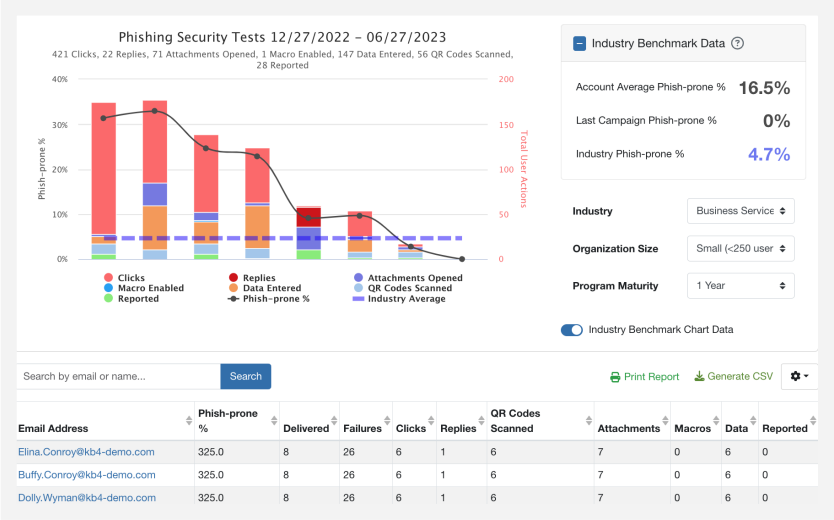
Das **Dashboard** Ihrer Konsole enthält den Risk Score der Organisationen und Phishing-Reports. Diese Reports liefern allgemeine Informationen über den Phish-prone Percentage der Organisation zum Zeitpunkt der Phishing-Kampagne und die Aktionen Ihrer Nutzer:innen während der Kampagnen. Sie können mit der Maus auf Punkte in der Tabelle zeigen, um weitere Details zu bestimmten Phishing-Kampagnen, zur Anzahl der Nutzer:innen, an die die einzelnen Tests gesendet wurden, und zu den Aktionen Ihrer Nutzer:innen zu erhalten.

Im weiteren Verlauf erfahren Sie mehr über die zahlreichen verfügbaren Reporting-Funktionen.

Phishing-Reports

Der Abschnitt „Phishing-Reports“ in der KnowBe4-Konsole enthält Reports, mit denen sich die Nutzeraktionen in mehreren Kampagnen summieren lassen (z. B. wie oft die einzelnen Nutzer:innen auf einen Phishing-Link geklickt haben).

Reports lassen sich nach einem bestimmten Zeitraum, nach bestimmten Kampagnen und nach Kampagnen, die an bestimmte Nutzer:innen gesendet wurden, filtern. Sie können auch Fehler, gemeldete Phishing-E-Mails (E-Mails, die über den Phish Alert Button gemeldet wurden) oder Ergebnisse nach Gruppen vergleichen.



Trainingsreports

Der Abschnitt „Trainingsreports“ der KnowBe4-Konsole enthält Reports zu Nutzer:innen, die sich mindestens einmal angemeldet haben, und solche, die sich nie angemeldet haben. Sie können auch Reports zu spezifischen Kursen in der Konsole erstellen. Diese Reports lassen sich so filtern, dass alle Nutzer:innen oder nur bestimmte Gruppen ausgewertet werden. Außerdem können Sie ein bestimmtes Start- oder Enddatum festlegen und Sie haben die Möglichkeit, archivierte Nutzer:innen einzuschließen.

Diese Reports liefern folgende Informationen über Ihre Nutzer:innen

- Nutzer:innen, die ihre Kurse innerhalb des angegebenen Datumsbereichs begonnen haben
- Nutzer:innen, die innerhalb des angegebenen Datumsbereichs registriert waren, ihre Kurse jedoch nicht begonnen haben
- Nutzer:innen, die ihre Kurse innerhalb des angegebenen Datumsbereichs begonnen, jedoch nicht beendet haben
- Nutzer:innen, die innerhalb des angegebenen Datumsbereichs registriert waren, ihre Kurse jedoch nicht begonnen oder beendet haben
- Nutzer:innen, die ihre Kurse innerhalb des angegebenen Datumsbereichs abgeschlossen haben

- Nutzer:innen, die innerhalb des angegebenen Datumsbereichs registriert waren, die Kenntnisnahme der Kursen beigefügten Richtlinien jedoch nicht bestätigt haben
- Nutzer:innen, die die Kenntnisnahme der Kursen beigefügten Richtlinien innerhalb des angegebenen Datumsbereichs bestätigt haben

Email Exposure Check Pro

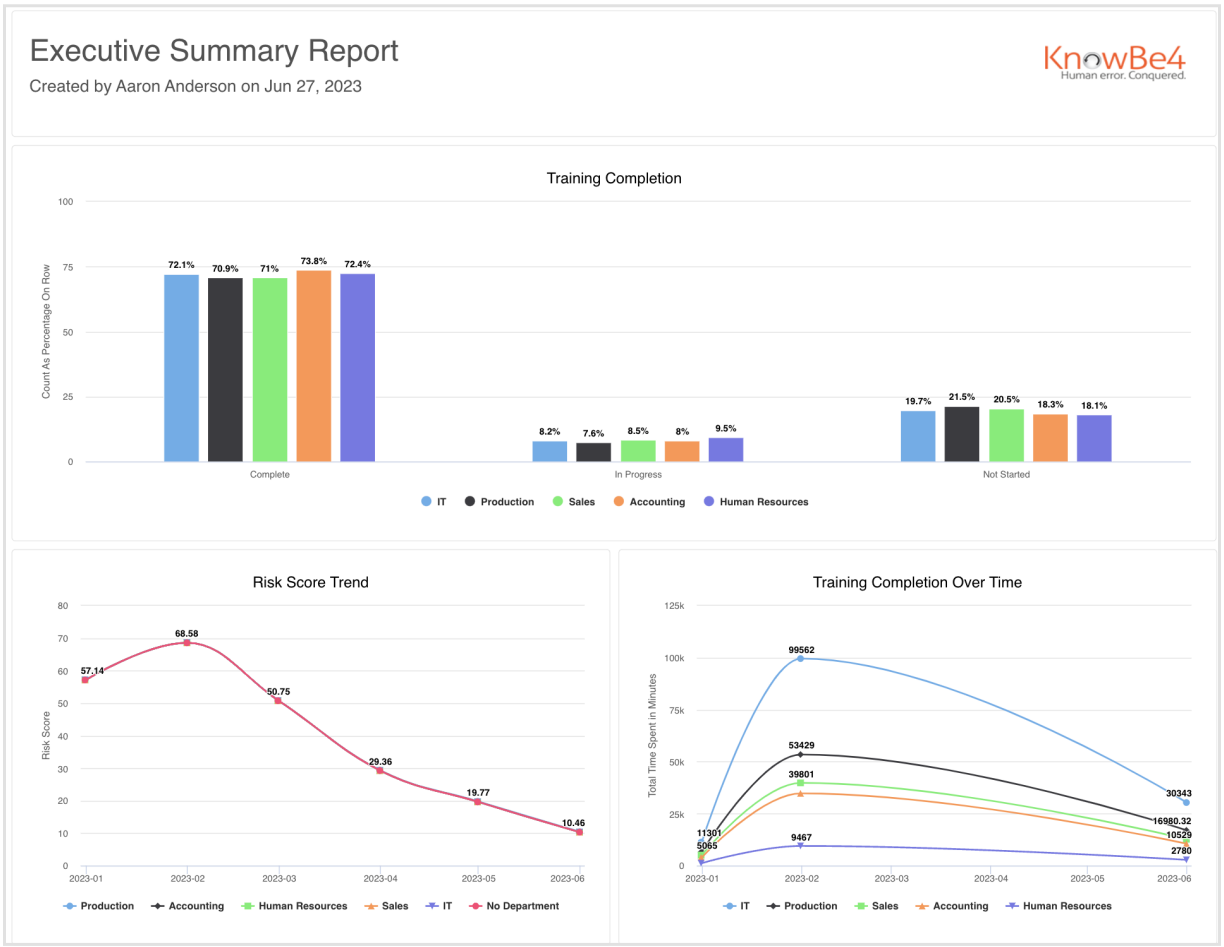
Das in den Abonnementstufen Gold und höher verfügbare Tool Email Exposure Check (EEC) Pro ermittelt gefährdete Nutzer:innen in Ihrer Organisation. Hierzu werden Daten aus Business-Netzwerken in Social Media und jetzt auch Tausende Datenbanken mit Sicherheitsverletzungen ausgewertet.

Nach der Datenauswertung ordnet das EEC Pro-Tool Daten die Nutzer:innen einer Risikoverteilungsgruppe zu. Die Gruppeneinteilung **Sehr hohes Risiko**, **Hohes Risiko** und **Mittleres Risiko** basiert darauf, wie viele Daten zum:zur jeweiligen Nutzer:in ermittelt wurden.

Erweitertes Reporting

Das erweiterte Reporting liefert belastbare Kennzahlen sowie einen Überblick über die Wirksamkeit des Security Awareness Trainings. Mit den erweiterten Reportings können Sie zahlreiche Arten von Reports passend zu den Anforderungen Ihrer Organisation erstellen. Diese Funktion enthält eine Sammlung mit über 60 integrierten Reports, die einen ganzheitlichen Überblick über die Entwicklung in der gesamten Organisation bieten, und ermöglichen das ausführlichere Reporting über eine Vielzahl von Schlüsselindikatoren für Awareness-Trainings.

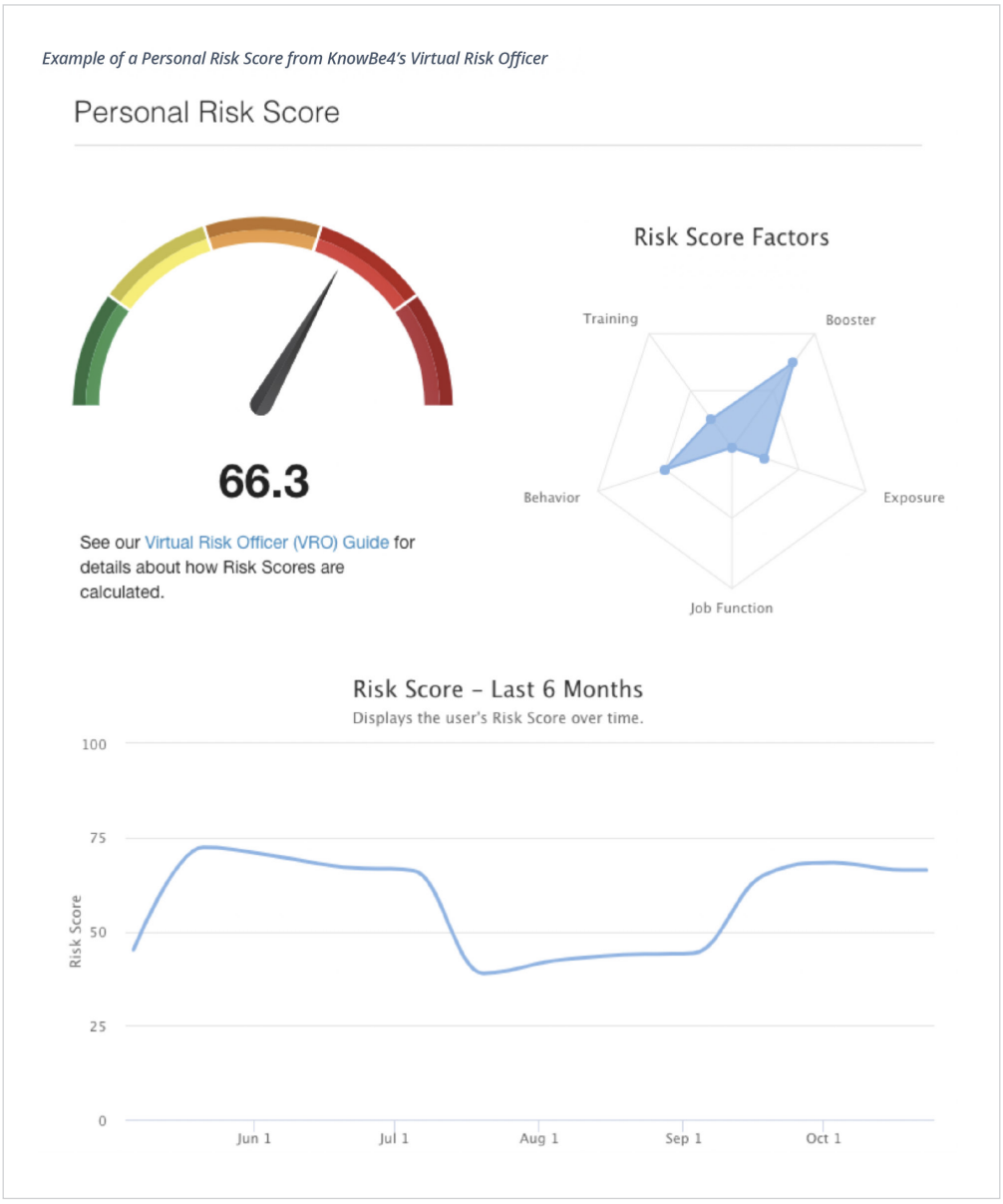
Darüber hinaus können Sie **Reports für Führungskräfte** erstellen. Mithilfe der darin enthaltenen Einblicke können Sie datengestützte Entscheidungen über Ihr Programm treffen.



Virtual Risk Officer

Die Funktion „Virtual Risk Officer“ (VRO) hilft, Risiken für Nutzer:innen, Gruppen oder die gesamte Organisation zu identifizieren und datengestützte strategische Entscheidungen hinsichtlich Ihres Security Awareness Plans zu treffen. Mit VRO können Sie den Nutzerrisikostatus Ihrer Mitarbeitenden und Ihrer Organisation im Laufe der Zeit verfolgen.

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



Flexible APIs

Auf den Abonnementstufen ab Platinum bietet KnowBe4 zwei robuste APIs, die zusätzliche Optionen zur Analyse von Nutzeraktivitäten und das entsprechende Reporting bereitstellen.

- Mithilfe der Reporting-APIs können Sie Daten von Ihrer KnowBe4-Konsole abrufen, um diese in Reports zu verwenden. Die APIs ermöglichen die Abfrage von Phishing-, Trainings-, Nutzer- und Gruppendaten.
- Mit der User Event API lassen sich Daten zu sicherheitsrelevanten Ereignissen oder Trainingsaktivitäten Ihrer Nutzer:innen, die auf Plattformen von Drittanbietern stattfinden, einfach integrieren und in Ihre KnowBe4-Konsole übertragen. Fügen Sie diese Ereignisse zu den Zeitplänen Ihrer Nutzer:innen hinzu und bestimmen Sie deren genauen Risk Score, damit Sie spezifischen Content für zusätzliche Phishing- oder Trainingskampagnen zusammenstellen können.

PasswordIQ

PasswordIQ für die Abonnementstufe Diamond überwacht das Active Directory Ihrer Organisation kontinuierlich auf bekannte Passwortschwachstellen. Verwenden Ihre Nutzer:innen derzeit gemeinsame, schwache oder aufgrund von Datenpannen öffentlich verfügbare Passwörter? In diesem Fall können Sie eine Übersicht der Passwortprobleme zusammenstellen und Passwortrisiken besser im Blick behalten.

Abonnementstufen

Silver-Stufe: Trainingszugriffsstufe I umfasst die Schulung zum Sicherheitsbewusstsein von Kevin Mitnick in der Vollversion (45 Minuten) und die 15-minütige Version für Führungskräfte. Darüber hinaus sind unbegrenzte simulierte Phishing-Tests, Assessments, die KnowBe4 Learner App, KI-Trainingsempfehlungen und Reports für die Dauer Ihres Abonnements enthalten.

Gold-Stufe: Umfasst alle Funktionen der Silver-Stufe sowie Content aus der Trainingszugriffsstufe II, in der auch KnowBe4-Trainingsmodule enthalten sind. Gold umfasst darüber hinaus monatliche Email Exposure Check (EEC)-Reports.

Platinum-Stufe: Umfasst alle Funktionen der Silver- und Gold-Stufe. In der Platinum-Stufe sind darüber hinaus unsere erweiterten Phishing-Funktionen enthalten (Smart Groups, Reporting-APIs, User Event API, Sicherheitsrollen und Social-Engineering-Indikatoren für Landingpages).

Diamond-Stufe: Umfasst alle Funktionen der Silver-, Gold- und Platinum-Stufe sowie Trainingszugriffsstufe III. Sie haben Vollzugriff auf unsere Content-Bibliothek mit mehr als 1.300 Elementen, darunter interaktive Module, Videos, Spiele, Poster und Newsletter zum Thema Security Awareness Training. Mit unserer KI-gestützten Phishing-Funktion können Sie darüber hinaus Phishing-Tests für Nutzer:innen personalisieren, empfohlene optionale KI-Lerninhalte aktivieren und mit PasswordIQ das Active Directory Ihrer Organisation kontinuierlich auf bekannte Passwortschwachstellen im Blick behalten.

Compliance Plus: Erhältlich als optionales Add-on für alle Abonnementstufen. Das Compliance Plus Training ist interaktiv, relevant und motivierend – mit wirklichkeitsnahen, simulierten Szenarien. Ihre Nutzer:innen erfahren, wie sie auch in herausfordernden Situationen richtig handeln. Der Content umfasst schwierige Themen wie sexuelle Belästigung, Vielfalt und Inklusion, Diskriminierung und Unternehmensethik. In der Compliance-Plus-Bibliothek finden Sie verschiedene Arten von Medienformaten und Materialien für Ihr Compliance-Trainingsprogramm.

PhishER Plus: Erhältlich als eigenständiges Produkt oder als optionales Add-on für alle Abonnementstufen. PhishER Plus ist eine schlanke SOAR-Plattform, die gemeldete E-Mail-Nachrichten automatisch analysiert und kategorisiert, um schädliche E-Mails zu identifizieren und unter Quarantäne zu stellen. Darüber hinaus werden gemeldete Phishing-E-Mails in entschärfter Form für Phishing-Simulationen verwendet. Mit der neuen Blockliste – die auf Community-Meldungen basiert und mithilfe von KI validiert wird – und den globalen PhishRIP-Funktionen zum proaktiven Blockieren und Entfernen aktiver Phishing-Angriffe, die E-Mail-Filter umgangen haben, BEVOR Ihre Nutzer:innen damit konfrontiert werden, spart PhishER Plus Zeit und Geld, indem Ihr SOC-Team (Security Operations Center) entlastet wird.

SecurityCoach: SecurityCoach steht Platinum- oder Diamond-Abonnenten als optionales Add-on zur Verfügung. SecurityCoach ist das erste Echtzeit-Sicherheitscoaching, das IT- und SOC-Teams dabei unterstützt, die größte Angriffsfläche Ihrer Organisation zu schützen – Ihre Mitarbeitenden. Mithilfe der neuen Technologie Human Detection and Response (HDR) stärkt SecurityCoach Ihre Sicherheitskultur, indem Ihre Nutzer:innen bei riskantem Verhalten ein Echtzeit-Coaching erhalten.

„Social Engineering ist das schwerwiegendste Problem in Bezug auf Informationssicherheit.“

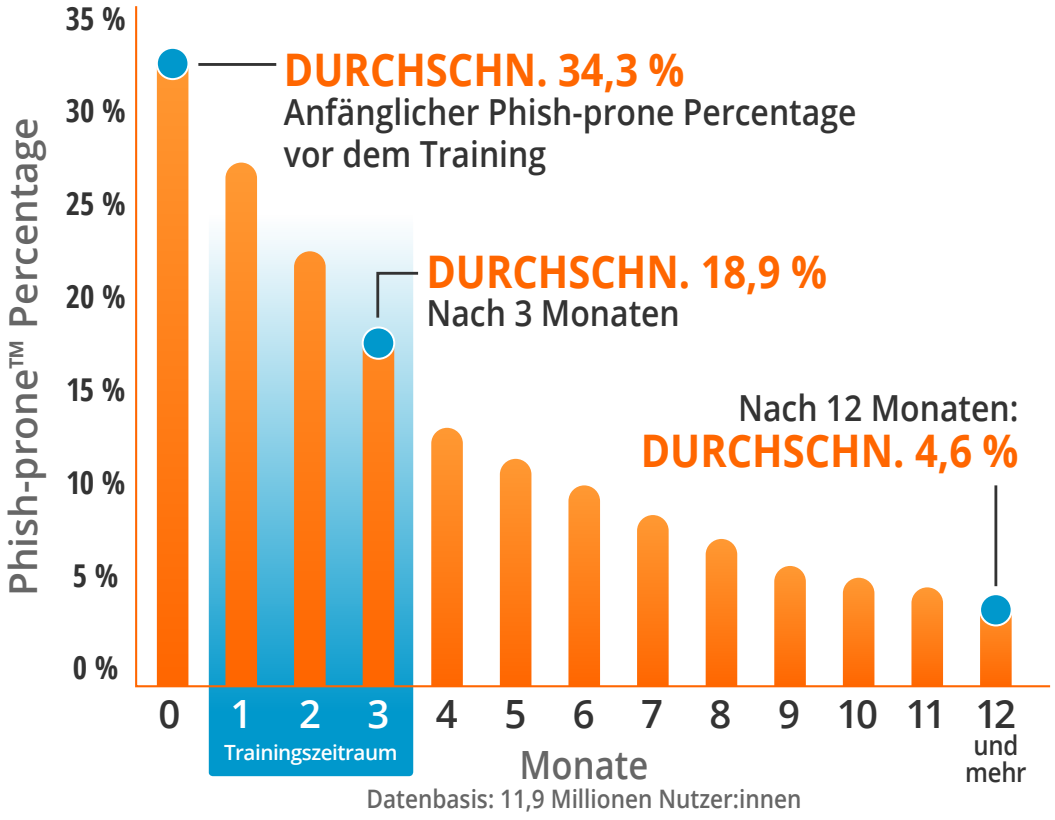
– Kevin Mitnick, IT Security Consultant

Beleg für die Funktion des Systems von KnowBe4

Eine Investition in Security Awareness Training und Phishing Security Tests zahlt sich schnell aus.

Die Ergebnisse des Benchmarking-Reports Phishing-Risiko nach Branchen von KnowBe4 für das Jahr 2024 zeigen den Phish-prone Percentage vor und nach mindestens 12 Monaten fortlaufendem Security Awareness Training.

Branchenübergreifend beträgt der Phish-prone Percentage in Unternehmen beunruhigende 34,3 %. Jedoch kann die Häufigkeit des Fehlverhaltens in nur 90 Tagen um fast die Hälfte – auf nur 18,9 % – reduziert werden. Und zwar durch den Einsatz des „New-School Security Awareness Training“ von KnowBe4. Bei konsequenter Umsetzung dieses Trainings sinkt der Wert für den Phish-prone Percentage nach 365 Tagen auf durchschnittlich nur noch 4,6 %.



Quelle: KnowBe4 – Phishing-Risiko nach Branchen: Benchmarking-Report 2024

Anmerkung: Der anfängliche Phish-prone Percentage wird auf Grundlage aller evaluierten Nutzer:innen berechnet. Diese Nutzer:innen wurden vor der Evaluierung nicht mithilfe der KnowBe4-Konsole geschult. Nachfolgende Zeiträume geben den Phish-prone Percentage für die Untergruppe der Nutzer:innen wieder, die mithilfe der KnowBe4-Konsole geschult wurden.

KnowBe4
Human error. Conquered.

KnowBe4 Germany | Rheinstraße 45/46 | 12161 Berlin – Deutschland | knowbe4.de | +49 30 34 64 64 60 | kontakt@knowbe4.com