KnowBe4

Security Awareness Training & Simulated Phishing Platform

Schützen Sie sich besser gegen **Social Engineering**

KnowBe4 Security Awareness Training

Mitarbeitende sind immer komplexer werdenden Phishing- und Ransomware-Angriffen ausgesetzt. Klassische Security Awareness Trainings bieten einfach nicht mehr genügend Schutz.

Baseline Testing

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

Nutzer und Nutzerinnen schulen

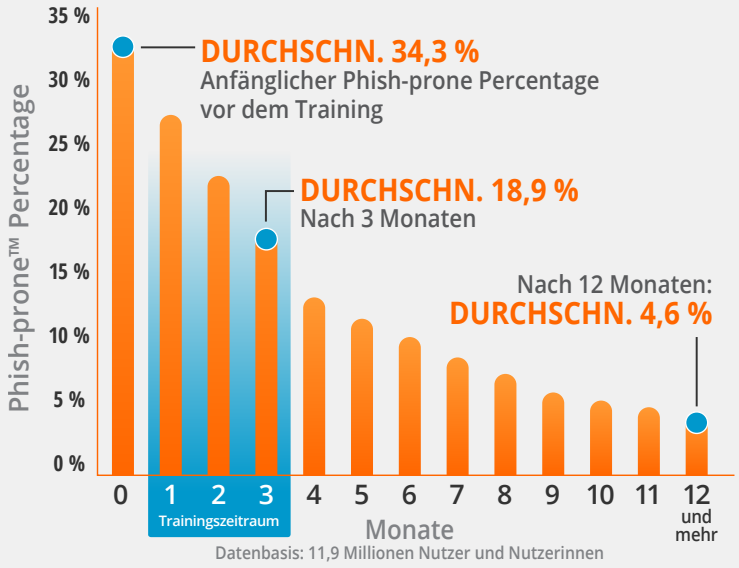
Die weltweit größte Bibliothek für Security Awareness Training Content mit interaktiven Modulen, Videos, Games, Postern, Newslettern und automatisierten Trainingskampagnen mit Erinnerungs-E-Mails.

Nutzer und Nutzerinnen schulen

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

Ergebnisse analysieren

Detaillierte Reports und Statistiken zu Trainingskampagnen und Phishing-Simulationen: solide Entscheidungsgrundlage für das Management – und Nachweis für den Return-on-Invest.



Datenbasis: 11,9 Millionen Nutzer und Nutzerinnen

Nachweislich reduzierte Sicherheitsrisiken

Eine 2024 durchgeführte Analyse – basierend auf den Daten von über 11,9 Mio. Nutzer und Nutzerinnen der KnowBe4-Plattform über die Dauer von 12 Monaten – liefert überraschende Resultate. Branchenübergreifend hat sich der anfängliche Phish-prone Percentage im Vergleich zu 2023 um einen ganzen Prozentpunkt auf 34,3 % erhöht.

Jedoch kann die Häufigkeit des Fehlverhaltens in nur 90 Tagen auf 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 %.

Wie anfällig ist Ihre Organisation im Vergleich? Die Industry-Benchmarking-Funktion ist in Ihrem Abonnement enthalten.

Quelle: KnowBe4 – Phishing-Risiko nach Branchen: Benchmarking-Report 2024
Anmerkung: Der anfängliche Phish-prone Percentage wird auf Grundlage aller evaluierten Nutzer und Nutzerinnen berechnet. Diese Nutzer und Nutzerinnen wurden vor der Evaluierung nicht mithilfe der KnowBe4-Konsole geschult. Nachfolgende Zeiträume geben den Phish-prone Percentage für die Untergruppe der Nutzer und Nutzerinnen wieder, die mithilfe der KnowBe4-Konsole geschult wurden.

KnowBe4 Security Awareness Training Features

Unbegrenzte Nutzung

Unser Angebot umfasst drei Trainingsstufen im KnowBe4-ModStore, die je nach gewählter Abonnementstufe Zugriff auf unsere Content-Bibliothek mit über 1.300 Elementen erlauben. Dazu: unbegrenzter Zugriff auf alle Phishing-Tools bei flexibler Lizenzierung. Und es kommen regelmäßig neue, leistungsstarke Funktionen hinzu.

Lokalisierte Versionen von Administratorkonsole und Nutzerbereich

Sie können eine Standardsprache für folgende drei Bereiche festlegen: Phishing-Sprache, Trainingssprache und Sprache für die Administratorkonsole. Dank dieser Lokalisierungsoptionen können Ihre Administratoren die KnowBe4-Konsole in einer von zehn Sprachen verwalten, während Sie Ihren Nutzern und Nutzerinnen in über 35 Sprachen eine umfassende Trainingserfahrung anbieten können.

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. Verfügbar für alle Abonnementstufen.

Anpassbare Module

Diese Funktion bietet Ihnen die Möglichkeit, individuellen Content am Anfang und am Ende der ausgewählten KnowBe4-Trainingsmodule einzufügen. Stimmen Sie den Content mit Branding-Elementen wie Ihrem Logo, individuellen Grafiken und Unternehmensfarben auf Ihre Nutzer und Nutzerinnen ab.

Eigenen Content hochladen

Sie möchten die Security Awareness Trainings von KnowBe4 durch betriebseigenen Content ergänzen? Laden Sie mit dem zuverlässigen Learning-Management-System von KnowBe4 Ihren SCORM-kompatiblen Training und Video Content einfach in den KnowBe4-ModStore und koordinieren Sie all Ihren Training Content an einem einzigen Ort – ohne zusätzliche Kosten.

Assessments

Wo stehen Ihre Nutzer und Nutzerinnen in Bezug auf Sicherheitswissen und Sicherheitskultur? Erstellen Sie mithilfe unserer Assessment-Tools elementare Messwerte für Ihre Organisation und behalten Sie das Wissen und die Einstellung Ihrer Mitarbeitenden zur internen Sicherheitskultur im Blick.

Individuelle Phishing-Vorlagen und Landingpages

Zusätzlich zu den unzähligen, benutzerfreundlichen Systemvorlagen stehen Ihnen individuelle Angriffsszenarien und gezielte Spear-Phishing-Kampagnen zur Verfügung. Jeder Phishing-E-Mail-Vorlage kann eine eigene Landingpage zugewiesen werden. So können Nutzer und Nutzerinnen direkt im Einzelfall geschult werden.

Phish Alert Button

Der KnowBe4 Phish Alert Button erlaubt es Nutzer und Nutzerinnen, 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!

Social-Engineering-Indikatoren

Mit unseren simulierten Phishing-E-Mails können Sie Mitarbeitende in Bezug auf ihr individuelles Verhalten schulen. Nutzer und Nutzer und Nutzerinnen erhalten direktes, automatisiertes Feedback zu den verborgenen „Red Flags“ der E-Mail.

KI-gestützte Empfehlungen für Phishing- und Training Content

Bieten Sie Ihren Nutzer und Nutzerinnen mithilfe von KI ein personalisiertes Training, das dem aktuellen Wissensstand Ihrer Nutzer und Nutzerinnen entspricht. KI wählt automatisch die beste Phishing-Vorlage für die einzelnen Nutzer und Nutzerinnen aus, basierend auf deren individuellem Trainings- und Phishing-Verlauf. Mit KI-gestützten Trainingsempfehlungen stellt der KnowBe4-ModStore Content bereit, der auf den Phish-prone Percentage Ihrer Organisation zugeschnitten ist.

Benutzermanagement

Die Active Directory-Integration von KnowBe4 ermöglicht den einfachen Upload und die automatische Aktualisierung der Daten von Nutzern und Nutzerinnen. Mit der Smart Groups-Funktion können mitarbeiterspezifische Phishing-Kampagnen, Trainingsmodule sowie das Reporting nutzer- und verhaltensbasiert angepasst werden.

Fortschrittliches Reporting

Mehr als 60 integrierte Report-Funktionen geben Ihnen einen ganzheitlichen und detaillierten Überblick über Ihre wichtigsten Awareness-Training-Indikatoren. Mithilfe von Reporting-APIs können Sie Daten aus Ihrer KnowBe4-Konsole abrufen. Darüber hinaus können Sie Reports für Führungskräfte erstellen. Mithilfe der darin enthaltenen Einblicke können Sie datengestützte Entscheidungen über Ihr Programm treffen.

Virtual Risk Officer™

Der innovative Virtual Risk Officer (VRO) nutzt maschinelles Lernen, um Vorhersagen zu Risiken zu treffen und Risiken auf Nutzer-, Gruppen- und Unternehmensebene zu identifizieren. Mit diesem kontinuierlichen Lernmodell können Sie datengestützte Entscheidungen in Bezug auf Ihr Security Awareness Program treffen.

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 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 mit PhishFlip entschärft und für Phishing-Simulationen verwendet.

PhishER Plus stellt eine KI-validierte Blockliste und PhishRIP-Funktionen bereit, mit denen sich aktuelle Phishing-E-Mails, die durch die Filter gelangt sind, proaktiv blockieren und entfernen lassen, BEVOR diese in die Posteingänge von Nutzerinnen und Nutzern gelangen. Das SOC-Team hat weniger Aufwand bei der Bedrohungsabwehr, was zu deutlichen finanziellen Einsparungen und der Freisetzung von InfoSec-Kapazitäten führt.

Wussten Sie, dass 88 % aller erfolgreichen Datendiebstähle mit einem menschlichen Fehler beginnen?
Holen Sie sich den kostenlosen Phishing Security Test und finden Sie heraus, wie viel Prozent ihrer Mitarbeitenden anfällig für Phishing-Angriffe sind.

knowbe4.com/de/free-tools/phishing-security-test

ELOVADE

Kontaktdaten für DE/AT:

ELOVADE Deutschland GmbH
knowbe4@elovade.com
DE: +49 6441 67118 842
AT: +43 820 0010 36
elovade.com/knowbe4

Kontaktdaten für CH:

ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/knowbe4