knowbe4

Plattform für Security Awareness Training und Phishing-Simulationen

Schützen Sie sich besser gegen Social Engineering

KnowBe4 Security Awareness Training

Klassische Security Awareness Trainings bieten heute einfach nicht mehr genügend Schutz. Sie müssen eine Kultur aufbauen, in der Sicherheit an erster Stelle steht, sowie motivierendes und effektives Training bereitstellen.

- **Baseline Testing**
  Mit einer ersten kostenfreien Phishing-Simulation ermitteln wir, wie anfällig Ihre Nutzerinnen und Nutzer für Angriffe sind (Phish-prone™ Percentage).
- **Nutzerinnen und Nutzer schulen**
  Bei uns finden Sie die weltweit größte Bibliothek für Security Awareness Training Content mit interaktiven Modulen, Videos, Games, Postern, Newslettern und automatisierten Trainingskampagnen mit Erinnerungs-E-Mails.
- **Nutzerinnen und Nutzer testen**
  Greifen Sie auf branchenführende, voll automatisierte simulierte Phishing-Kampagnen, Tausende Vorlagen mit unbegrenzter Nutzung sowie ständig aktualisierte Community-Phishing-Vorlagen zu.
- **Ergebnisse analysieren**
  Detaillierte Reports und Statistiken zu Trainingskampagnen und Phishing-Simulationen stellen eine solide Entscheidungsgrundlage für das Management dar.

Funktionen im KnowBe4 Security Awareness Training

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 Administratorinnen und Administratoren die KnowBe4-Konsole in einer von zehn Sprachen verwalten, während Sie Ihren Nutzerinnen und Nutzern 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, Optionen zum Freitesten 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 Nutzerinnen und Nutzer ab.

Eigenen Content hochladen

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

Assessments

Wo stehen Ihre Nutzerinnen und Nutzer 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 Nutzerinnen und Nutzer direkt im Einzelfall geschult werden.

Phish Alert Button

Der KnowBe4 Phish Alert Button erlaubt es Nutzerinnen und Nutzern, 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. Nutzerinnen und Nutzer erhalten direktes, automatisiertes Feedback zu den verborgenen „Red Flags“ der E-Mail.

KI-gestützte Empfehlungen für Phishing und Training Content

Bieten Sie Ihren Nutzerinnen und Nutzern mithilfe von KI ein personalisiertes Training, das dem aktuellen Wissensstand Ihrer Nutzerinnen und Nutzer entspricht. KI wählt automatisch die beste Phishing-Vorlage für die einzelnen Nutzerinnen und Nutzer 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.

Funktionen im KnowBe4 Security Awareness Training | Fortsetzung

Nutzerverwaltung

Die Active Directory-Integration von KnowBe4 ermöglicht den einfachen Upload und die automatische Aktualisierung der Daten von Nutzerinnen und Nutzern. Mit der Smart Groups-Funktion können 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 Administratorin oder Administrator 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.

PhishER Plus™

PhishER Plus ist eine schlanke Incident-Response-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 sich 88 % aller erfolgreichen Datenschutzverletzungen auf einen menschlichen Fehler zurückführen lassen?

Holen Sie sich den kostenlosen Phishing Security Test und finden Sie heraus, wie viel Prozent ihrer Mitarbeitenden „Phish-prone“ (anfällig für Phishing-Angriffe) sind.

knowbe4

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

0341-A 0925