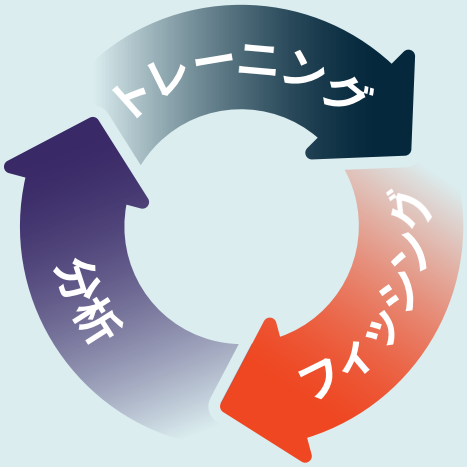
セキュリティ意識向上トレーニング・フィッシングシミュレーションプラットフォーム

日々進化するソーシャルエンジニアリングへの対策を実現可能にするベストプラクティス

KnowBe4セキュリティ意識向上トレーニング

今日、全従業員が巧妙化するフィッシング攻撃やランサムウェア攻撃に遭遇する機会が増えています。こうした脅威から組織を守るためには、わかりやすく効果的なトレーニングを通じて、社内にセキュリティ文化を根づかせることが重要です。

- **ベースラインテスト：**
  無償の模擬フィッシング攻撃により、従業員が攻撃に引っかかる割合をPPP (Phish-prone™ Percentage: フィッシング詐欺ヒット率) としてアセスメントし、トレーニング前の現状を把握。
- **トレーニング：**
  インタラクティブなトレーニングや動画、ゲーム、ポスター、ニュースレターなどを含む、世界最大のセキュリティ意識向上トレーニングコンテンツライブラリを利用して、ユーザーのセキュリティ意識を向上。スケジュールされたリマインダーメールの送信と自動トレーニングキャン
- **模擬フィッシング：**
  完全に自動化された本物そっくりの模擬フィッシング攻撃、無制限に利用できる数千種類のテンプレート、各種コミュニティに適したフィッシングテンプレートを提供。
- **結果・効果の分析：**
  エンタープライズクラスの詳細なレポーティングでは、セキュリティ管理者が把握しやすいよう、トレーニング状況とフィッシングテスト結果の両方を統計とグラフ分析で表示。



KnowBe4セキュリティ意識向上トレーニングの機能

無制限の利用

KnowBe4 ModStoreでの3つのトレーニングアクセスレベルを提供。サブスクリプションレベルに応じて1,300項目を超えるコンテンツライブラリへのアクセスが可能です。柔軟なライセンス体系で、すべてのフィッシング機能に無制限にアクセスでき、新機能も定期的に追加されます。

管理コンソールと学習コンテンツの多言語対応

3つのローカライズ設定 (フィッシング、トレーニング、管理コンソールの言語) でデフォルト言語を設定可能。これらのローカリゼーションオプションにより、管理者は10言語のうちのいずれかでKnowBe4コンソールを管理できます。また、ユーザーは35言語以上に対応した学習コンテンツで自分の母語を選択できるため、トレーニングをより深く理解できるようになります。

コンテンツマネージャー

コンテンツマネージャーを利用して、合格スコアの設定、自社ロゴの組み込み、テスト実施の許可、コンテンツスキップ不可の設定など、トレーニングコンテンツの設定を簡単にカスタマイズできます。すべてのサブスクリプションレベルで利用可能です。

コンテンツでの自社ロゴ使用

このセルフサービス機能を使えば、対象となるKnowBe4トレーニングの最初と最後にカスタマイズコンテンツを追加できます。自社ロゴやカスタムグラフィック、コーポレートカラーなど企業ブランドを構築する要素を追加して、ユーザーに伝えたいメッセージをカスタマイズできます。

独自コンテンツのアップロード

KnowBe4セキュリティ意識向上トレーニングプラットフォーム上に、自社独自の教育プログラムや他社の教育プログラムを追加することができます。KnowBe4の強力なLMS (学習管理システム：Learning Management System) を使用すれば、独自のSCORM準拠の教育コンテンツや動画コンテンツをアップロード可能。独自コンテンツとKnowBe4 ModStoreトレーニングコンテンツをすべて一箇所で管理できます。追加料金は一切かかりません。

アセスメント

従業員一人ひとりがどれくらいのセキュリティ知識を持っているか、セキュリティ文化をどれだけ理解しているかを評価し、ベースラインセキュリティの評価指標の確立に役立てることができます。スキルアセスメントとセキュリティカルチャー調査を使って、従業員のセキュリティ知識とセキュリティ文化への取り組みなどを時系列で測定・監視します。

独自のフィッシングテンプレートとランディングページ

システム内には数千もの便利なテンプレートを用意。これにユーザー独自の情報を加え、本番さながらの偽装ファイルを添付して、自社独自の標的型スピアフィッシングキャンペーンを展開できます。各フィッシングメールテンプレートには、それぞれカスタムランディングページを設定可能。インシデントの発生ごとに異なる教育コンテンツを追加できます。

Phish Alert Button

KnowBe4では、アドイン機能としてPhish Alert Buttonを用意しています。ユーザーがこのボタンを押して不審なメールを報告すると、セキュリティ担当者が分析でき、受信ボックスから疑わしいメールを削除して被害の拡大を防ぎます。必要なのはPhish Alert Buttonをワンクリックするだけです。

ソーシャルエンジニアリングインディケーター

特許取得済みのテクノロジーによって、模擬フィッシングメールを「セキュリティ教育の機会」へと転換。模擬メール内で見逃した危険なサインをすぐに表示します。

AIを活用した模擬フィッシングとトレーニングの提案

AIを活用して、各ユーザーの知識レベルに合わせたよりパーソナルな体験を提供します。各ユーザーのトレーニング状況とフィッシングテストの結果に応じて、最適な模擬フィッシングテンプレートを自動的に選択。さらにAIによるトレーニング提案に沿って、KnowBe4 ModStoreでは組織全体のPPP (フィッシング詐欺ヒット率) ™に合わせたトレーニングコンテンツを表示します。

KnowBe4セキュリティ意識向上トレーニングの機能

ユーザー管理

KnowBe4のActive Directoryインテグレーションによって、受講者データのアップロードがより簡単に。手動による変更管理が不要となり、大幅な時間短縮を実現します。さらに、Smart Group (スマートグループ) 機能を活用すれば、自社のフィッシングキャンペーン、学習課題、各従業員のふるまいや受講者属性に基づいた是正学習などを最適化できます。

詳細レポートの機能

60種を超えるビルトインレポートが利用可能。全体を俯瞰できる包括的なレポートに加えて、時系列に主要なトレーニング評価指標を追跡する詳細レポーティングにも対応しています。各種のレポーティングAPIにより、KnowBe4コンソールからデータを抽出できます。さらに、エグゼクティブレポートではわかりやすくてまとまったレポートをカスタマイズして作成・配信できます。このレポートから得られるインサイトは、プログラムに関するデータ主導の意思決定をサポートします。

Virtual Risk Officer™ (VRO)

機械学習を使用した革新的なVirtual Risk Officer (VRO) 機能は、受講者、部署、企業レベルごとのセキュリティリスクを予測・特定します。この継続的な学習モデルによって、自社のセキュリティ意識向上プログラムにおけるデータ主導の意思決定ができます。

コールバックフィッシング

管理者は、KnowBe4コンソールのコールバックフィッシング機能を使用して模擬演習ができます。この機能を使って受講者がこうした攻撃に引っかかるか確認しましょう。まず受講者のもとへ電話番号とコードが記載されたメールが届き、受講者がその番号に電話をかけると、コードを入力するよう求められる仕組みです。

PhishER Plus™

PhishER Plusは、簡易インシデントレスポンスプラットフォームです。報告されたメールを自動的に分析して優先順位をつけ、組織全体の悪意のあるメールを特定し隔離します。さらに、PhishFlipなら本物のフィッシングメールを模擬フィッシングキャンペーンに変換し、トレーニングの機会に変えることができます。

PhishER Plusは、AIによって検証されたクラウドソーシングのブロックリストとPhishRIP機能を搭載。ユーザーに被害が及ぶ前に、メールフィルターをすり抜けたフィッシング攻撃を検知してブロック・削除します。SOCチームによる対応件数を削減し、予算と情報セキュリティ対策に費やす時間を大幅に減らします。

データ侵害の88%は、「人」を標的とした攻撃によって起きています。

無料のフィッシングセキュリティテストで、フィッシング攻撃の被害に遭いやすい従業員の割合を調べましょう。

KnowBe4 Japan合同会社 | 〒107-0052 東京都港区赤坂 9−7−1 ミッドタウン・タワー 18F
03-4586-4540 | www.knowbe4.ja | info@KnowBe4.jp