KnowBe4

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・分析プラットフォーム

継続的な脅威となる**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のセキュリティ意識向上トレーニングとは？

これまでの古いスタイルのセキュリティ教育（KnowBe4では“Old School”と呼んでいます）はもはや限界に達しています。今、すべての従業員が、日々進化するフィッシング攻撃やランサムウェア攻撃に頻繁にさらされているのです。

ベースラインテスト

無償の模擬フィッシング攻撃を通して社員一人ひとりがどれくらい攻撃被害を受けやすいかを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。

ユーザーのトレーニング

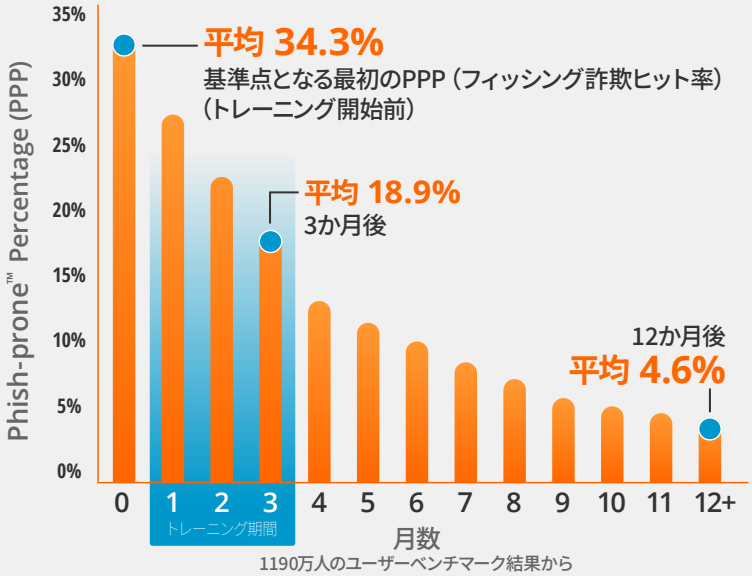
インタラクティブな教材モジュール、ビデオ、ゲーム、ポスター、ニュースレターなどを含む世界最大のセキュリティ意識向上トレーニングコンテンツライブラリー。スケジュールされたリマインダーメールの送信。自動化されたトレーニングキャンペーンの実施。

ユーザーへのフィッシング

完全に自動化されたクラス最高の模擬フィッシング攻撃、無制限に利用できる数千ものテンプレート、各種のコミュニティフィッシングテンプレート。

結果・効果の分析

エンタープライズクラスの最強のレポーティング。トレーニング状況とフィッシングテスト結果をともに統計とグラフ分析を表示。セキュリティ管理者に最適で、同時にROIも可視化します。



驚きの効果を実証

KnowBe4の膨大なユーザーデータベースを使って、12ヶ月間以上にわたり1,190万人のトレーニング受講者を対象に分析を行いました。2024年度の調査結果によると、警鐘を鳴らすレベルが続いています。業界全体の初期PPPベンチマークは2023年から1ポイント上昇し、34.3%に達しました。

しかし、“New School” (セキュリティ意識向上トレーニングと疑似フィッシング訓練の組み合わせ) を導入後90日で、この数字は34.3%から18.9%へとほぼ半減しました。さらに、1年後の結果では、これらのベストプラクティスに従うことでPPPを平均4.6%へと大幅に縮められることが実証されています。

自社のPPPを他社と比較してみてください。KnowBe4のサブスクリプション契約には、業界ベンチマーキング機能が含まれています。

出典：2024年のKnowBe4業界別フィッシングベンチマーキングレポート
注：PPPの初期値は、評価対象の全ユーザーに基づいて算出されています。これらのユーザーは、評価前にKnowBe4コンソールを使ったトレーニングを一切受けていません。その後の各期間の数値は、全ユーザーのうちKnowBe4コンソールでトレーニングを受けたユーザーのPPPを反映しています。

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

サブスクリプションレベルに基づき、KnowBe4 ModStoreを通じて1,300項目を超えるコンテンツライブラリーへのアクセスと3つのトレーニングアクセスレベルを提供。ライセンス体系が柔軟で、すべてのフィッシング機能に無制限にアクセスできます。さらに、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、学習コンテンツは35言語以上で利用できるため、学習者は自分の母語でよりトレーニングの理解度を深めることができます。

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、テストアウトの許可、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により、対象のKnowBe4トレーニングモジュール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。お客様にお届けしたいメッセージに合わせて、自社ロゴやカスタムグラフィックス、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できます。

各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したいというニーズはございませんか？このような場合、KnowBe4の堅固なLMS（学習管理システム：Learning Management System）を使用すると、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して、すべてのKnowBe4 ModStoreトレーニングコンテンツとともに一箇所で管理することが可能です。しかも、追加料金は一切かかりません。

アセスメント

従業員各自がどれほどのセキュリティ知識を持っているか、またセキュリティカルチャー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ます。スキルをベースにしたアセスメントとセキュリティカルチャー調査を使って、時間の経過とともに変わる従業員のセキュリティ知識とセキュリティを意識した文化に対する感情を測定・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が用意されています。これに受講者独自の情報を加えてフィッシング攻撃シナリオをカスタマイズし、本番さながらの偽装添付ファイルを作成して、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ボタン

KnowBe4では、アドイン機能としてPhish Alertボタンを用意しています。このボタンによって、不審メールを安全に分析のためにセキュリティ担当者へ転送できます。Phish Alertボタンによって報告後は、受信ボックスから疑わしいメールを削除して今後の脅威の拡散を防止できます。すべてが、Phish Alertボタンをワンクリックするだけで完了します。

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、それぞれの模擬フィッシングメール体験を「セキュリティ教育の機会」へと転換。模擬演習メール内で見逃した点については、レッドフラグが評価指標として自動で立てられ、個人のスコアとして数値化されます。

AIを活用した模擬フィッシングとセキュリティ教育を推奨

各受講者に現在の知識レベルに合わせたよりパーソナルな体験を提供するのに、AIは絶大な威力を発揮します。AIを活用した模擬フィッシングによって、各受講者のセキュリティ教育とフィッシング履歴に応じて、最適な模擬フィッシングテンプレートを自動的に選択します。AIを活用した教育内容の推奨にもとづき、KnowBe4 ModStoreが組織全体のPPP（フィッシング詐欺ヒット率）に合わせた教育コンテンツを作成します。

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さらに簡単に。手動による変更管理は不要で、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) 機能を活用して、自社のフィッシングキャンペーン、学習課題、各受講者の振る舞いや受講者属性に基づいた是正学習などを自動化することが可能になります。

アドバンスドレポーティング機能

60種を超えるビルトインレポートが提供されており、全体を俯瞰する包括的なビューに加えて、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をサポートしています。各種のレポーティングAPIを通して、各自の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を使用すると、エグゼクティブレベルの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ドリブンな意思決定をサポートします。

Virtual Risk Officer™ (VRO)

革新的なVirtual Risk Officer (VRO) 機能は、機械学習を通して受講者毎、部署毎、企業レベル毎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いてデータドリブンな意志決定を下すことが可能になります。

コールバックフィッシング

管理者は、KnowBe4コンソールの新機能コールバックフィッシングを使用して、コールバックフィッシング模擬演習を実行し、受講者がこのトリックに引っかかるかどうかを確認することができます。まず受講者に、電話番号とコードが記載されたメールが送られます。受講者がその番号に電話をかけると、コードの入力を求められます。しかし、罠はここに仕掛けられています。1つめの失敗ポイントはコードを入力すること、そして2つめが個人情報や機密情報を提供することです。

PhishER Plus™

PhishER Plusは、報告されたメールメッセージを自動的に分析し、優先順位をつけて、組織全体の悪意のあるメールを特定し隔離する軽量なSOARプラットフォームです。さらに、PhishFlipが実際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することで、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。メールフィルターを回避した活発なフィッシング攻撃を、ユーザーがフィッシング攻撃にさらされる前に積極的にブロックおよび削除します。SOCチームが処理する修復作業の量を削減することで、予算と情報セキュリティにかかる時間を大幅に減らします。

KnowBe4 Japan合同会社 | 〒100-6510 東京都千代田区丸の内 1−5−1 新丸の内ビルディング 10F EGG | 電話：03-4586-4540 | www.KnowBe4.jp/www.KnowBe4.com | Email:Info@knowbe4.jp

05C06K04