KnowBe4
Human error. Conquered.

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

巧妙化し続け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？

ますます巧妙化するハッカーの手口に対応するには、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）ではもはや限界がきています。今、あらゆる組織の「人」は、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。グローバルなエンタープライズ顧客から生まれた新しいスタイルのセキュリティトレーニング（**KnowBe4** では“**New School**”と呼んでいます）の実現が急務になっています。

ベーストラインテスティング

ベーストラインテスティングは、無償の模擬フィッシング攻撃を通して社員ひとりひとりがどれくらい攻撃被害を受けやすいかを PPP（Phishing Prone Percentage: フィッシング詐偽ヒット率）としてアセスメントし、トレーニング前の現状を把握。

セキュリティトレーニング実施

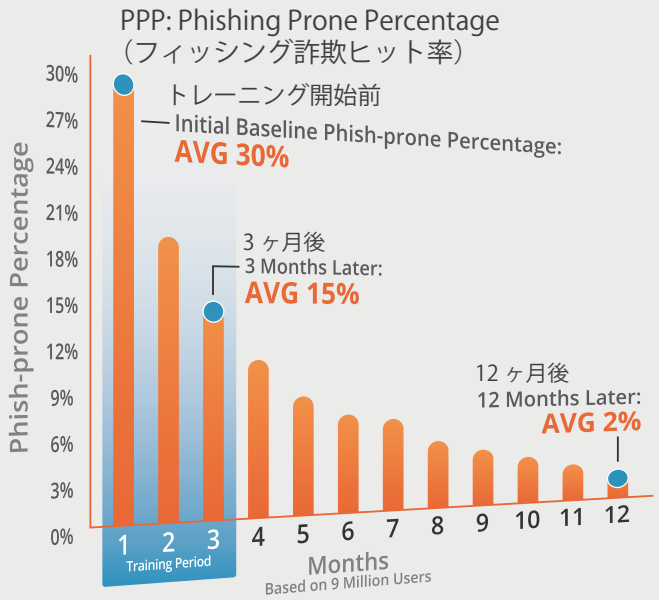
インタラクティブな教材モジュール、ビデオ、ゲーム、ポスター、ニュースレターなどを含む世界最大のセキュリティトレーニングコンテンツライブラリー。多言語に対応したオンデマンド・対話型の eラーニングとテストを組み合わせ、様々な利用形態のクラウドベースのトレーニングを実現。テスト結果分析に基づき、個人、部署にカスタマイズされたトレーニングプログラムが自動的に数分で作成・展開可能。

各受講者へのフィッシングテスト

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と豊富なランディングページを活用した本番さながらの攻撃の疑似体験。不審メールを見抜く力を大幅に向上。USB、音声による多彩な攻撃もシミュレーション可能。同時に、社員から IT 管理者へ不審メールを報告する仕組みも整備。

テスト結果分析

トレーニング状況とフィッシングテスト結果の両方に対する統計とグラフ分析を示す豊富なレポーティング機能。個人、部署、会社全体の被害リスクをスコア化し、PPP（Phishing Prone Percentage: フィッシング詐偽ヒット率）を可視化。個人スコアの改善が必要な社員へは、追加トレーニング受講へ自動的に誘導。同時に、ROI も可視化。



900 万人の利用者（社員数）調査結果から

驚きの効果を実証

KnowBe4 の受講者データベースを使って、12 ヶ月間にわたり約 900 万人のトレーニング受講者を対象にベンチマークし、2019 年度の調査結果は驚きの効果を実証しました。

全業種でのトレーニング実施前のベンチマークによると、トレーニング開始前の PPP（Phishing Prone Percentage: フィッシング詐偽ヒット率）は 30%というリスクの高さが結果として報告されました。

この数値が、KnowBe4 の“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）実施後の 90 日で、30%から 15%へ半減しました。さらに、1 年後の結果では、平均で 2%へ大幅に削減できました。

自社の PPP を他社と比較してください。年間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標準で含まれています。

KnowBe4のセキュリティ意識向上トレーニングがいかに効果的かを確認してください

KnowBe4はセキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。2019年9月現在、2万8千社を超える企業や組織・団体がKnowBe4を採用して、防御の最終ラインとして「人」による防御壁を構築しています。

KnowBe4のトレーニングにはどんな機能が含まれるか？

無制限の利用：
年間サブスクリプションレベルに基づいて 900 項目を超える教育コンテンツライブラリーへのアクセスを許可する 3 つのアクセスレベルを提供。柔軟なライセンシングによって、すべてのフィッシング機能への無制限のアクセスが可能になります。また、ライセンス数には制限がありません。さらに、KnowBe4 では強力な新機能を定期的に追加しています。

学習意欲を高めるインタラクティブなトレーニング：
インタラクティブなトレーニングは、全く新しい"学びと経験"（"New School"）を提供し、学習する喜びと意欲を向上させます。現在、15 ヶ国の言語をサポートしており、ユーザーインターフェイスとして言語を自在に選択することができます。これによって、直感的な学習を可能にし、学習効果を高めます。また、オプションとしてのゲーミフィケーション機能によって、スコア表を見て同僚と達成レベルを競い合ったり、レベルクリアのバッチを獲得するなど、ゲーム感覚で自社の組織を安全に守るために、新しい学習法で、意識と習慣を身に付けることができます。

新機能　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、SCORM 準拠の自社教育コンテンツや動画コンテンツを KnowBe4 ModStore にアップロードして、すべてのトレーニングコンテンツを一箇所に置き、集中管理しながら、社内展開することが可能です。

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：
KnowBe4 が用意した数千もの既存テンプレートに加えて、受講者独自の情報をベースにフィッシング攻撃シナリオをカスタマイズして、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。それぞれのフィッシングメールテンプレートには、それぞれのカスタムランディングページを設定させることでき、インシデント発生時点の教育を可能にします。

フィッシュアラート（Phish Alert）ボタン：
KnowBe4 では、各種メーラーの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メール脅威へのリスク低減対応ができ、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プラットフォーム」に変えます。模擬演習フィッシングメールの判断に誤まり、クリックしてしまった受講者には、暗黙のうちにレッドフラグが評価指標として立てられ、個人のスコアとして数値化されます。

ASAP（Automated Security Awareness Program-自動化セキュリティ意識向上プログラム）：
ASAP によって、自社の組織に対応したカスタマイズされた教育トレーニングプログラムを自動的に構成されます。自社にとっての最適な教育トレーニングプログラムが数分で作成され、実装できます。

受講者管理：
KnowBe4 の Active Directory インテグレーションによって、容易に受講者データをアップロードすることが可能になり、手動による変更管理を不要とし、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。

セキュリティロール：
特定の受講者グループを設定したい場合に、アクセスレベルと管理権限を組み合わせて、自在に設定できます。権限移譲の設定によって、ロールベースで、特定のデータを表示するだけに制限したり、特定のグループ向けのフィッシング、教育トレーニングや受講者管理を許可するように設定したり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。また、複数のアカウントに対して、ロールアップレポーティングによって集計した結果表示を容易に生成することが可能になります。

Virtual Risk Officer™（バーチャルリスクオフィサー）：
革新的な Virtual Risk Officer（VRO）機能によって、受講者毎、部署毎、企業レベル毎のセキュリティリスクをスコア化でき、自社のセキュリティ対策立案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。さらに、ユーザーイベント API を活用することで、サードパーティープラットフォーム（例えば、Mimecast、Splunk など）からセキュリティ関連のカスタムイベントを KnowBe4 コンソールへプッシュ型で連携させることができ、受講者のリスクスコアに随時反映させることが可能になります。

PhishER：
教育トレーニングとフィッシングテストが進むにつれて、セキュリティ担当への不審メールの報告が増加してきます。これは、セキュリティ担当者にとって新たな問題となります。この問題を解決するためのオプショナルなアドオンが PhishER で、大量な不審メールの報告に対応してくれます。PhishER を実装することで、セキュリティ担当者を支援し、メール脅威を迅速に特定して、防御することが可能になります。（詳しくは、PhishER データーシートをご参照ください）

情報漏えいの91%は、「人」を標的としたスピアフィッシング攻撃よって引き起こされていることをご存じですか？

無償のフィッシングテストを試してみてください。自社の従業員がフィッシングに対してどれだけ脆弱であるかを確認してみてください。

www.KnowBe4.com/PST

KnowBe4 Japan 合同会社 〒100-0004東京都千代田区大手町1-9-2 大手町フィナンシャルシティグランキューブ3 階
Global Business Hub Tokyo | www.KnowBe4.com / www.KnowBe4.jp | お問い合わせ：Info@knowbe4.jp

2019年9月発行