

Sophos Phish Threat

セキュリティ上の最大の弱点「人」の脆弱性を改善

組織は、スパム、フィッシング、高度なソーシャルエンジニアリングなどの攻撃に絶えずさらされており、IT プロフェッショナルの 41%は、少なくとも 1日に 1回、フィッシング攻撃の攻撃対象になっていると報告しています。サイバー攻撃対策における最大の課題は、恰好の標的になる従業員の意識の低さです。効果的なフィッシング攻撃のシミュレーション、自動化されたトレーニング、包括的なレポート機能など、Sophos Phish Threat で従業員とビジネスを保護できます。

主な特長

- ▶ 500種類以上のメールテンプレート、60種類以上のトレーニングモジュール
- ▶ Windows / Mac 対応の Outlook アドインで訓練メールを報告
- ▶ 模擬攻撃やトレーニング結果のレポートを自動的に作成
- ▶ 10カ国語に対応
- ▶ 選べるホスティング拠点 (米国、英国、ドイツ)

一番弱いところがその企業のセキュリティレベル

大きな犯罪ビジネスであるフィッシング。過去数年において、フィッシング攻撃の数は飛躍的に増加しました。マルウェアの 66%は、悪意のあるメールの添付ファイルを介してインストールされ、高度な標的型フィッシング攻撃によるビジネスへの被害は、インシデント 1件につき平均 140,000米ドルとされています。サイバーセキュリティ対策において、大抵の組織では、ユーザーが恰好の標的となっていますが、フィッシング脅威に関する従業員トレーニングを実施することで、人間が「ファイアウォール」となり、このような脅威に対処することができます。

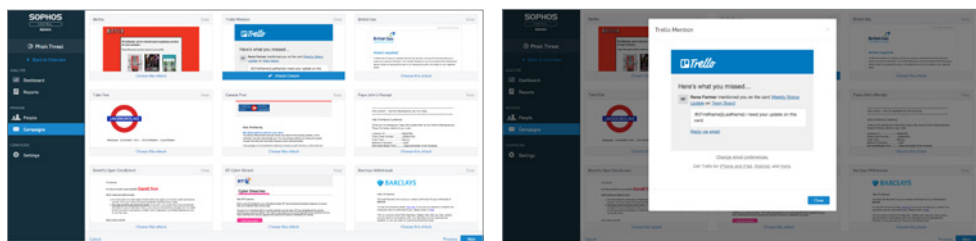
Sophos Phish Threat は、さまざまな種類のフィッシング攻撃をエミュレートすることで、社内のセキュリティ体制の弱点を特定しやすくします。また、興味深いトレーニングを通じて、従業員が問題を自己解決できるように教育し、組織の防御体制を強化します。

最新のフィッシング攻撃を基にしたシミュレーション

500種類を超える実践さながらの高度な訓練メールを、わずか数クリックで送信できます。

ソフォスでは、最新の脅威に対して、SophosLabs のアナリストが、グローバル規模で、数百万件のメール、URL、ファイル、および他のデータポイントを毎日監視しています。この絶え間ないインテリジェンスを活用して、最新のフィッシング攻撃手法を従業員トレーニングに取り入れており、さまざまな攻撃シナリオに対応する訓練用テンプレートが 10カ国語で利用可能となっています。

- ▶ 英語
- ▶ オランダ語
- ▶ ポルトガル語
- ▶ 繁体中国語
- ▶ ドイツ語
- ▶ イタリア語
- ▶ 韓国語
- ▶ フランス語
- ▶ スペイン語
- ▶ 日本語



初心者から IT リテラシーの高い従業員まで対象とした国際的なテンプレートも利用可能

効果的なトレーニングモジュール

60種類を超えるインタラクティブなトレーニングモジュールを活用して、疑わしいメールや、アカウント情報の窃取、パスワード強度、法規制へのコンプライアンスなど、特定の脅威について社内教育を実施できます。10カ国語に対応し、従業員にとって興味深く役立つ内容である一方で、将来起こり得る本物の攻撃に備えた対策を実施することができるため、管理者にとっても安心です。



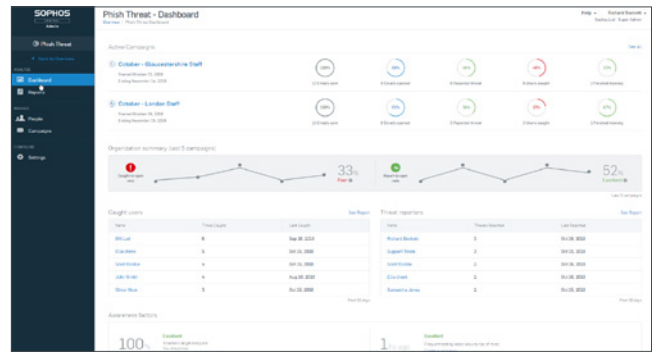
興味深いインタラクティブなトレーニングモジュール

包括的なレポート機能

直感的に操作できるダッシュボードでオンデマンドに表示可能なデータを活用して、組織のセキュリティ状態を把握したり、実際の費用対効果を説明したりできます。Sophos Phish Threat のダッシュボードを活用すると、攻撃シミュレーションの結果を基にした従業員の識別能力を一目で把握することができます。また、次のライブデータを含む「ウェアアネス ファクター」で、従業員全体のリスクレベルを表示することもできます。

- ・ 上位レベルのキャンペーン結果
- ・ 組織全体の傾向 - 見抜けなかった従業員と報告者
- ・ 攻撃を見分けられなかった従業員の総数
- ・ テストの範囲
- ・ 前回のキャンペーンからの経過日数

ドリルダウンレポートで、さらに掘り下げた詳細な訓練結果を、組織レベルまたは従業員レベルで確認することができます。製品に搭載されている Outlook アドインを使用すれば、従業員はメールクライアントから直接、訓練メールを報告できるため、管理者は従業員のセキュリティウェアアネスを正確にとらえることが可能です。この結果、組織全体のセキュリティレベルがどの程度なのか詳細に把握できます。



インタラクティブなレポート機能で、全体のリスクレベルと従業員のパフォーマンスを把握

Sophos Central で Sophos Phish Threat を管理

Sophos Phish Threat は、クラウド管理型の統合セキュリティ管理コンソールである Sophos Central の単一の画面から管理できます。ハードウェアの用意やソフトウェアのインストールは不要で、Sophos Central のメリットを活用できます。Sophos Central は、フィッシング攻撃シミュレーションおよび従業員トレーニングを、メール / エンドポイント / モバイルデバイスのセキュリティ対策などの機能と同時に管理できる、唯一のソリューションです。Sophos Central は、ソフォスがクラウド上で運営する、シンプルで操作が簡単な最新の単一プラットフォームです。詳細は sophos.com/ja-jp/central をご覧ください。

導入が簡単

Sophos Phish Threat は、すべて Web ブラウザで実行できるので便利です。Phish Threat メールを問題なく配信するには、Sophos Central のコンソールに表示される IP アドレス、および Phish Threat キャンペーンで使用するメールアドレスとドメインをホワイトリストに登録します。そして、CSV ファイルまたは Active Directory 同期ツールを使用して、ユーザーをインポートします。ユーザーのアップロードが完了したら、キャンペーンの送信を開始できます。

購入方法

Sophos Phish Threat のライセンスはユーザー単位 (テストへのアクセスは無制限) で購入可能 (1人~5,000人以上の各範囲の価格帯)。ライセンスの種類は 1つのみで処理が簡単なので、システム管理者は、今日の洗練されたフィッシング攻撃に対する従業員およびビジネスの保護に専念することができます。

30日間無償評価版
無償評価版の登録 (100ユーザーまで)
sophos.com/ja-jp/phish-threat

ソフォス株式会社営業部
Email: sales@sophos.co.jp