DATA SHEET

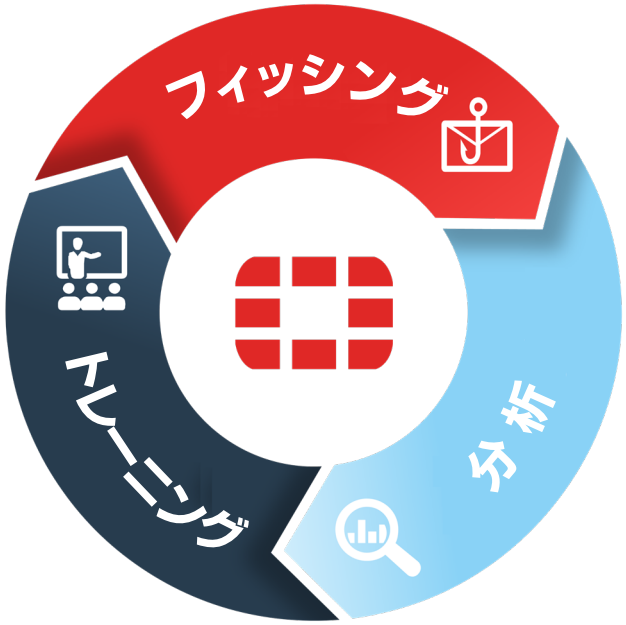
FortiPhish

フォーティネットのフィッシングシミュレーションサービスとセキュリティ意識向上トレーニング

E メールは今もサイバー犯罪者にとって、機密データを不正取得する、銀行口座や金融データへのアクセスを手に入れる、ランサムウェアを使ってデータをアクセス不能にするといった攻撃を画策する際の最大の脅威ベクトルであり続けています。事実、ベライゾンの「2020 年版データ侵害調査報告書」によると、企業の重役へのスピアフィッシングやホエールフィッシングを含むフィッシングやプリテキスティング（犯罪者が説得力のあるもっともらしい口実や話を使って疑いを持たないユーザーを騙し、犯罪者に有益な行動を起こさせる手法）の 96% が、E メール経由で届いています。これらの攻撃によるデータ侵害、知的財産の損失、不正な資金移動などで、企業の評判失墜や多額の金銭的損失が発生しています。

セキュリティに対する意識向上トレーニングにも限界があります。入社や退社で従業員が入れ替わり、年に 1 回程度のオンラインコースなどのトレーニングを実施したとしても、学んだことをいつまでも覚えていられるわけではありません。

FortiPhish は、セキュリティに関する十分な知識を持たないユーザーがもたらすリスクに対処し、潜在的な脅威を予測して検知するセンサーの役割をユーザーが担うようにすることができます。FortiPhish は、意識向上トレーニングの実施のほかに、実際に確認された最新のフィッシング事例のシミュレーションを利用した高度なテストを組み合わせた、先進的なサービスです。知識の強化学習を実施すると同時に、フィッシングやその他のソーシャルエンジニアリングによる誘導への十分な注意に必要なツールをユーザーが手に入れることができます。



FortiPhish の活用

課題

Web や E メール経由で送り込まれるゼロデイマルウェアやフィッシングの脅威は、データの損失、侵害、ランサムウェアによる被害の発生につながる恐れがあります。

解決策

セキュリティ意識向上トレーニングに高度なシミュレーションを組み合わせることで、ソーシャルベースの攻撃から組織を保護するために必要な知識とツールをユーザーに提供します。

メリット

- フォーティネットの NSE Institute が実施するセキュリティ意識向上トレーニングによって、ユーザーは適切なセキュリティプラクティスに従って行動できるようになります。
- フィッシングシミュレーションは、E メール経由で送り込まれる潜在的な脅威をユーザーが特定できるかどうかをテストします。

FortiPhish
www.fortiphish.com

トレーニング
www.fortinet.com/support/training

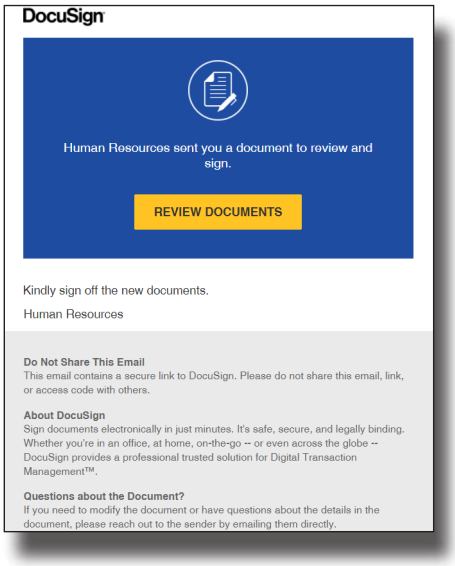
FortiCare 24 時間 365 日のサポート
www.fortinet.com/jp/support

概要

FortiPhish は、フォーティネットの NSE Training Institute を通じて提供されるコンテンツを活用する、セキュリティ意識向上トレーニングのクラウドベースのシミュレーションサービスです。悪意のある E メールやソーシャルエンジニアリングによって送り込まれる脅威に対するユーザーの意識の育成、維持、定着、強化は、FortiPhish Cloud の継続的なテストとシミュレーションサービスを利用することで、その効果が最も高くなります。

FortiPhish のフィッシングシミュレーションは、フィッシング手法に関する FortiGuard Labs の確かな知識を利用し、ユーザーを標的にする信憑性の高いフィッシングキャンペーンをシミュレーションできます。

FortiPhish では豊富な分析機能も提供されるため、フィッシングや関連のソーシャルエンジニアリング攻撃を特定するユーザーの能力を評価し、組織のフィッシング対策の取り組みにおいて行動改善に向けた支援を必要とするユーザーを特定できます。



フィッシング

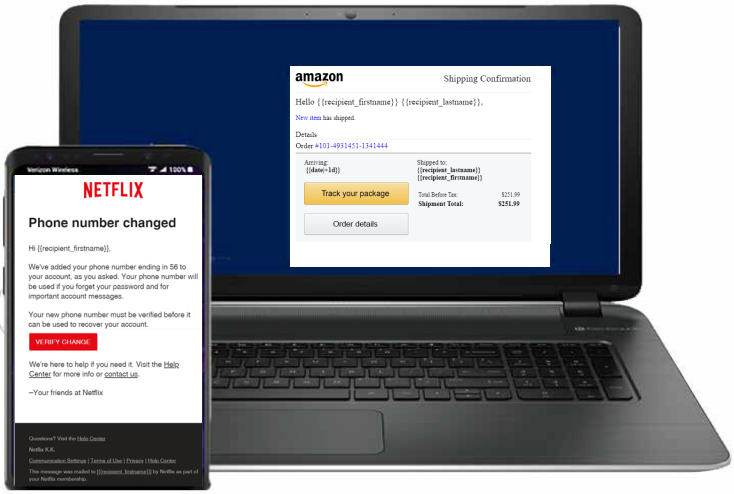
実際のフィッシング攻撃をシミュレーションし、ユーザーの意識や備えをテストすると同時に、クリックしてしまった場合の適切な対処方法を徹底します。

分析

結果を分析し、プログラムの傾向を可視化するとともに、リスクのあるユーザーや改善すべき領域を特定します。分析結果を将来のトレーニングに反映させることで、組織全体のセキュリティに関する意識がさらに強化されます。

トレーニング（ロードマップ）

ユーザーを対象にトレーニングを実施し、フィッシング、スピアフィッシング、ホエールフィッシング、プリテキスティング、なりすまし、ビジネスメールの流出など、E メールによって送り込まれる脅威がもたらすリスクと、それらを特定する方法を周知します。



FortiPhish の主な特長

クラウドベースのフィッシングシミュレーションサービス

- 事前に定義された多言語のフィッシングメールを活用して、ユーザーの反応をテストします
- ユーザーが不審なリンクをクリックしてしまい、情報が流出する可能性をテストします

管理レポート

- E メール開封率を把握し、攻撃の分析結果を可視化します
- 長期的な改善の進捗をユーザーグループ毎にトラッキングします

NSE Institute トレーニング

- NSE トレーニングパッケージを活用した強化トレーニングを実施します

ライセンス形態

機能	FortiCloud Premium	スタンダード	アドバンスト *
月あたりの対応フィッシングメール数	30	mailbox（user）サブスクリプション 下記ライセンス情報参照	mailbox（user）サブスクリプション
多言語対応：管理	●	●	●
基本テンプレート	●	●	●
ユーザ定義（手動または CSV 形式）	●	●	●
「攻撃キャンペーン」収束後のレポート	●	●	●
フィッシングテンプレート（日本語含む多言語対応）		●	●
ユーザー定義：LDAP		●	●
イベント別のテンプレート			●
カスタムテンプレート			●
「攻撃キャンペーン」収束後の NSE トレーニング			●

* トレーニングモジュールを統合したアドバンストサービスを提供予定

ライセンス情報

製品	説明
FortiPhish Premium Account License	Standard subscription for 25 mailboxes, 12 months, includes support
	Standard subscription for 500 mailboxes, 12 months, includes support
	Standard subscription for 10,000 mailboxes, 12 months, includes support

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ