Proofpoint Security Awareness Training

オンラインによるセキュリティ意識向上トレーニングとフィッシング訓練メール

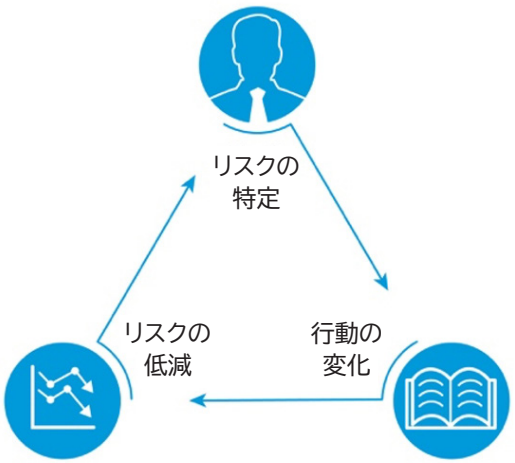
主なメリット

- ユーザーの行動を変えフィッシングやその他のサイバー攻撃によるリスクを低減
- 複数言語サポートにより全世界で一貫したトレーニングを提供
- インシデント対応の優先順位付け、インシデント対応の改善
- 動的なレポーティングと Results API で進捗を管理
- フィッシング攻撃の被害とマルウェア感染のリスクを最大 90% 低減

Proofpoint Security Awareness Training（PSAT）では、適切なトレーニングを適切な人に適切なタイミングで提供することができます。これにより、エンドユーザーがサイバー攻撃を識別できるようになり、組織を守る最後の砦になれるよう支援します。

サイバー攻撃の 90% 以上はユーザーを標的としているため[1]、従業員教育の実施は組織の保護に非常に有効な手段です。脅威を検知し、ユーザーに届く前にブロックするというテクノロジーだけではすべての脅威を阻止できません。ビジネスメール詐欺やフィッシングのメールを受け取ったときに、ユーザーがそれを脅威だと認識し適切な対処ができるようになることが重要です。このソリューションではユーザーにサイバー攻撃を防ぐ方法を教育します。これにより以下が実現できます。

- それぞれのユーザーが持つリスクの特定
- 従業員の行動の変化
- 組織のリスクを低減



1 Verizon:「2019 Data Breach Investigations Report（2019年度データ漏洩/侵害調査報告書）」2019年7月

リスクを特定する

攻撃を受けているユーザーを識別し、ユーザーの自己防御能力を評価

Proofpoint Very Attacked People™（VAP）レポートを用いれば誰が攻撃を受けているかを可視化できます。これらのレポートは Proofpoint Targeted Attack Protection（TAP）の機能の一部で、誰が狙われていてどのようなタイプの脅威が発見されたかなどの情報を提供します。

Proofpoint ThreatSim® フィッシング シミュレーションは、様々なフィッシング攻撃に対する組織の弱点を明らかにします。13 のカテゴリにわたる数千種類のフィッシングテンプレートがあり、以下のような脅威タイプを用いてユーザーを評価できます。

- 悪意のある添付ファイル
- 埋め込まれたリンク
- 個人データ提供の依頼

毎週新しいテンプレートを追加し、最新の攻撃傾向に対応できるようにしています。ダイナミック脅威シミュレーションのフィッシング テンプレートは、実際の攻撃により近づけるため、Proofpoint の脅威インテリジェンスやお客様からのリクエスト、その時々のトピックを反映して作られています。

シミュレーション攻撃にひっかかってしまったユーザーにはそのタイミングで受講できる「ジャスト・イン・タイム」のレッスンが送られます。ユーザーはその訓練の目的、実際の攻撃の危険性、そして今後どのようにすれば攻撃の罠を回避できるかを学ぶことができます。また、フィッシング シミュレーションで騙されたユーザーに自動的にトレーニングを割り当てます。

ウイルスに感染した外付けメモリデバイスについてユーザーがどれほど理解しているかも確認が必要です。**ThreatSim USB シミュレーション**ではウイルス感染させた USB デバイスの危険性をユーザーに教育します。USB シミュレーションはいつでも何度でもアクセス可能です。またシミュレーション攻撃にひっかかってしまったユーザーにそのタイミングで受講できる「ジャスト・イン・タイム」の教育も実施できます。

Proofpoint CyberStrength® は Web ベースのナレッジ評価ツールです。メールや USB ドライブ以外にもさまざまなセキュリティ上の課題に対応しており、例えばモバイル デバイスの使用、ソーシャル エンジニアリング詐欺、Web ブラウジングなどのトピックも含んでいます。35 以上の言語の数百の質問ライブラリから事前定義されたアセスメントを選んで、ユーザーに合ったトレーニングを自動的に割り振ることができます。また自組織のポリシーや手順についての理解度を測るために、カスタマイズした質問を作成することも可能です。ユーザーが持つ基礎知識を評価した後は、様々な分野でユーザーが直面するリスクを低減するための推奨案を提示します。

行動を変化させる

実際の脅威、ユーザーの行動と知識レベルに基づいたトレーニングの提供

豊富で関連性の高いコンテンツはトレーニングの鍵になります。またユーザーの行動を変化させるためにも非常に有効です。セルフサービスの **Customization Center** では、ユーザー毎に関連性の高いコンテンツを割り振ることができます。トレーニングの文章、画像、質問項目、画面などはフル カスタマイズが可能です。**Learning Science Evaluator** の効果を継続させるためのリアルタイムのガイダンスも提供されます。

トレーニングはいつでもどこでも、どのデバイスからでも受けることができます。各モジュールにかかる時間は 5-15 分程度なので、業務の妨げになりません。Proofpoint のインタラクティブ モジュールは U.S. セクション 508 スタンダードと Web コンテント アクセシビリティ ガイドライン（WCAG）2.0 AA スタンダードに準拠しています。

Proofpoint のトレーニング モジュールでは、実績のある学習科学の原則を用いて、フィッシング攻撃から内部脅威まで様々なリスクを説明します。これには以下のようなコンテンツが含まれます。

- **トレーニング モジュール：**
  動画、インタラクティブなコンテンツ、ゲーム コンテンツを含むトレーニング モジュールを提供します。これらは 35 以上の言語に翻訳され、地域に合わせてローカライズされています。
  - 特定のコンプライアンス及びプライバシー トレーニングが必要な場合は、パートナーである TeachPrivacy からコンテンツを提供します。
  - さらに Defence Works の買収により、エンターテイメントの要素を含むコンテンツも提供できるようになりました。
- **意識向上のための各種素材：**
  ビデオ、インフォグラフィック、ニュースレター、記事、ポスター、画像などの各種素材を提供しています。これにより、トレーニングをさらに充実させることができます。
- **管理者向けプログラム：**
  管理者向けに効果的なプログラムを実施するのためのガイドを提供します。

また **Proofpoint 脅威インテリジェンス**からユーザーに最も関連性の高い攻撃や攻撃で使われたおとり文書を抽出してユーザーにアドバイスを提供できます。**Attack Spotlight** シリーズでは、最新の脅威を識別し、被害を未然に防ぐ方法を教育するショート コンテンツをタイムリーに提供します。

リスクを低減する

知識のあるエンドユーザーは潜在的な脅威を報告し、攻撃対象を減少させる

Proofpoint PhishAlarm® メール クライアント アドインを使用すれば、ユーザーはワンクリックで不審なメールを報告できます。不審なメールを報告したユーザーにはポップアップ メッセージあるいはメールですぐに感謝を伝えます。これにより、ユーザーが今後も協力し、組織の最後の防護壁となり続けるよう動機づけをすることができます。またこのアドインを使えばユーザーからメールヘッダーや添付ファイルなどの情報を入手する必要がなくなるため、ユーザーに不審なメールを転送してもらう必要がなくなります。

Proofpoint PhishAlarm Analyzer では、ユーザーから報告されたメールを複数の Proofpoint 脅威インテリジェンスとレピュテーション システムを用いて自動的に分析します。またメールの詳細情報やカテゴリ（悪意のあるメール、スパム、その他）などの概要を含む脅威レポートも提供します。これによりインシデント レスポンス チームはメールの調査や優先順位付けなどの作業を行う必要がなくなります。**Proofpoint 脅威インテリジェンス**は、100 名以上の脅威研究者で全世界の B2B 及び B2C メールの 5 分の 1 以上を分析し、またクラウド及びソーシャル脅威も分析しています。そのため、データの詳細さ、範囲、有効性において、Proofpoint 脅威インテリジェンスに並ぶものはありません。

Proofpoint Closed-Loop Email Analysis and Response（CLEAR）ソリューションは、報告されたメールを Proofpoint Threat Response Auto-Pull（TRAP）に自動的に送ります。そして Proofpoint TRAP では自動的にメールを隔離し、インシデントをクローズします。あるいはインシデント レスポンス チームにメッセージを送付します。管理者はエンドユーザー向けにカスタマイズしたレスポンス メッセージを表示するよう設定することができます。これによりユーザーの行動を促進し、セキュリティ意識の高い文化を構築できます。

すべての機能を備えたレポーティングで結果を分析する

Proofpoint の包括的レポートにはユーザーごとの進捗状況が表示されます。これにより、ユーザー知識のベンチマーク、トラッキング、進捗の確認、ROI の測定などが容易になり、詳細な情報からハイレベルな情報まで、全体像を可視化できます。アセスメント、攻撃シミュレーション、トレーニングにおけるユーザーの成績も確認できます。また、ダッシュボードを使えば、データのフィルタリング、アセスメントの比較、方法の変更などが簡単に実行できます。

レポートはダウンロード/エクスポート可能なので、他の人に共有したり、より詳細な分析や比較などをおこなうことができます。例えば、これらの情報と他のセキュリティ イベントとの関連性を評価する、といったことも可能になります。また、レポートの自動作成や自動送付（自分や関係者等）もスケジューリングできます。

さらに、**Proofpoint Results API** ではトレーニング、フィッシング、ナレッジ評価、ユーザー、メールに関するレポートや分析結果などをビジネス インテリジェンス ツールや学習管理システムに統合することもできます。

対応言語 (2020年6月現在)

言語	CyberStrength®	フィッシング攻撃シミュレーションとPhishAlarm® [1]	インタラクティブトレーニングモジュール[2]	意識向上ビデオキャンペーン	教育マテリアル[3]
アラビア語	✔	✔	✔	✔	
ビルマ語	✔	✔	✔	✔	✔
中国語(簡体字)	✔	✔	✔	✔	✔
中国語(繁体字)	✔	✔	✔	✔	✔
チェコ語	✔	✔	✔		
デンマーク語	✔	✔	✔	✔	
オランダ語	✔	✔	✔	✔	✔
英語(アメリカ)	✔	✔	✔	✔	✔
英語 (オーストラリア)	✔	✔	✔		
英語 (イギリス)	✔	✔	✔		
フィンランド語	✔	✔	✔	✔	
フランス語 (カナダ)	✔	✔	✔	✔	
フランス語 (ヨーロッパ)	✔	✔	✔	✔	✔
ドイツ語	✔	✔	✔	✔	✔
ギリシャ語	✔	✔	✔		
ヘブライ語	✔	✔	✔	✔	
ヒンディー語	✔	✔	✔		
ハンガリー語	✔	✔	✔	✔	✔
アイスランド語	✔		一部		
インドネシア語	✔		✔		
イタリア語	✔	✔	✔	✔	✔
日本語	✔	✔	✔	✔	✔
クメール語			✔		
韓国語	✔	✔	✔	✔	
マレー語	✔	✔	✔	✔	✔
マラーティー語					一部
ノルウェー語	✔	✔	✔	✔	
ポーランド語	✔	✔	✔	✔	✔
ポルトガル語 (ブラジル)	✔	✔	✔	✔	✔
ルーマニア語	✔	✔	✔		
ロシア語	✔	✔	✔	✔	✔
スロバキア語	✔	✔	✔		
スペイン語 (ヨーロッパ)	✔	✔	✔	✔	
スペイン語 (ラテン)	✔	✔	✔	✔	✔
スウェーデン語	✔	✔	✔	✔	
タイ語	✔	✔	✔	✔	
トルコ語	✔	✔	✔	✔	
ウクライナ語	✔	✔	✔		一部
ベトナム語	✔	✔	✔	✔	✔

1 いくつかのThreatSim® フィッシングテンプレートとTeachable Momentはブルガリア語でも提供されています。

2 チェックマークのついた言語では、すべてのインタラクティブトレーニングモジュールが翻訳されています(保護されるべき医療情報を除く)。メールセキュリティ、セキュリティエッセンシャル、URLトレーニングモジュールでは他の翻訳オプションも提供しています。

3 教育マテリアルはマレー語、マラーティー語、ウクライナ語でも提供されています。

詳細

詳細は proofpoint.com/jp でご確認ください。