Proofpoint Security Awareness Training コンテンツ一覧

ユーザー行動の変化を促してリスクを低減する

主な機能

コンテンツ ライブラリ
脅威、ユーザー、地域に基づいた各フォーマット形式の各種コンテンツ

基本カリキュラム
CISO およびセキュリティ専門家が実施する学習プログラムを新しいユーザーに対して迅速に展開

ユーザー アセスメント
ユーザー、グループ、部門ごとに、強みと弱みを把握

トレーニング モジュール
セキュリティおよびプライバシーを取り上げる幅広いトピックと豊富な形式のトレーニングをユーザープリファレンスに応じて提供

コンテンツのカスタマイズと配信
ユーザーごとにパーソナライズされた学習体験を提供。必要に応じて独自の学習管理システム (LMS) でコンテンツを配信

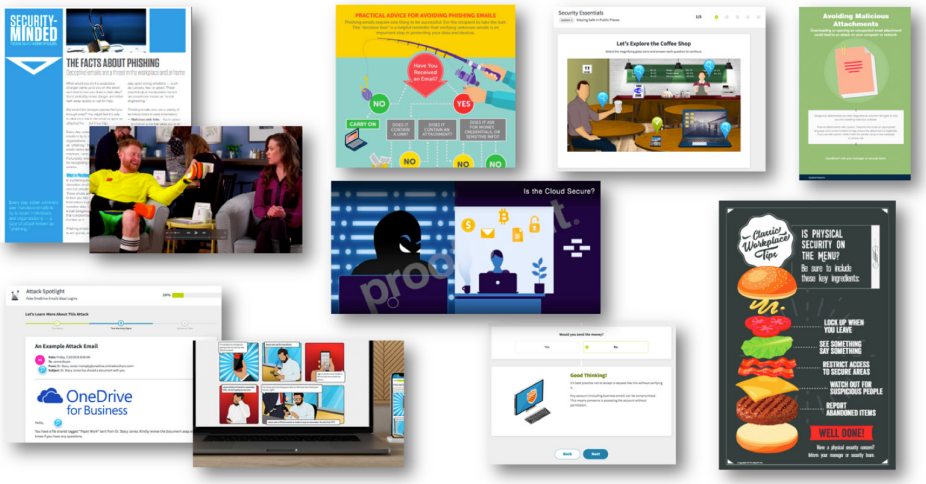
セキュリティ意識向上マテリアル
すぐに使用できるマテリアルを活用して意識向上キャンペーンを効果的、効率的に実現し、タイムリーな脅威アラートとレポートを実現

多言語対応
基本カリキュラムは 40 の言語で提供、その他のコンテンツは少なくとも 6 種の言語で提供

シミュレーション
豊富な脅威シミュレーションを用いてソーシャル エンジニアリング攻撃に対するユーザーの認識を評価

Proofpoint Security Awareness Training (PSAT) は、目に見える形でユーザーの行動に変化をもたらすことのできる実績のあるコンテンツを提供するソリューションです。適切なトレーニングを適切なユーザーに適切な時に提供することができるため、ユーザーは、セキュリティの脅威やプライバシー要件に対して、適切な対応をとることができるようになります。このソリューションを使って実現できることは、以下のとおりです。

- ユーザーの認識を評価してトレーニングを提供する
- セキュリティ意識向上キャンペーンのための豊富なマテリアルを活用する
- 報告を自動化する
- 不審な E メールに対処する



Proofpoint Security Awareness Training のコンテンツには、多様なトレーニングやリソースが含まれています。

基本カリキュラムと多言語対応

CISO およびセキュリティ専門家が実施するカリキュラムと学習プログラムで、ユーザーの行動変化を加速化させます。基本カリキュラムで基本的な知識を習得し、ユーザーの習熟度を高めていきます。ロール別の学習プログラムとエキスパート ガイダンスを利用することで、ユーザーの学習効果を高め、トレーニングを促進できます。

基本コースは 40 以上の言語に翻訳されています。追加コースと意識向上マテリアルは 6言語以上でご利用いただけます。

アセスメント コンテンツ：ユーザーにとって必要なことを理解する

セキュリティやプライバシーの問題を扱う場合は、各ユーザーの知識のギャップについて理解することが欠かせません。プルーフポイントでは、パーソナライズされたセキュリティ意識向上トレーニングの実施や、組織全体のセキュリティ リスクの特定を支援しています。

ThreatSim の攻撃シミュレーションは、実際の攻撃に対するユーザーの脆弱性を評価するもので、フィッシングや USB 攻撃のシミュレーションが含まれています。CyberStrength ナレッジ アセスメントは、重要なセキュリティ トピックに対してユーザーが知識を持っているかを評価します。

THREATSIM のフィッシングおよび USB による攻撃シミュレーション

攻撃シミュレーション テンプレート

複数の脅威タイプについてユーザー アセスメントを実施します。脅威タイプには、悪意のある添付ファイル、埋め込まれたリンク、USB 攻撃や、個人情報を聞き出そうとするものなどが含まれます。1,000 を超えるコンテンツが、36 以上の言語で提供されています。

テンプレートのカテゴリー

- Cloud / クラウド関連
- Commercial / ショッピング関連
- Consumer / 消費者向け
- Corporate / 社内向け
- Proofpoint Threat Intel / プルーフポイント脅威インテリジェンス
- Seasonal / 季節の挨拶関連
- USB関連
- 業種関連

ティーチャブル モーメント ランディング ページ

ユーザーが疑似フィッシング メールに応答した、まさにその時の「ジャスト イン タイム」のレッスンを提供します。これらのランディング ページでは何か起こったのかを説明し、本物の攻撃であった場合に伴うリスクも伝えます。さらに将来の攻撃を回避する方法も助言します。

ティーチャブル モーメントの種類

- Custom / カスタマイズ
- Embedded / TIPSが埋め込まれたもの
- Error Messages / エラー メッセージ
- Interactive / インタラクティブ
- Video / ビデオ入り

CYBERSTRENGTH ナレッジ アセスメント

カスタマイズできる問題と事前定義されたナレッジ アセスメント

攻撃シミュレーション以外にも、さまざまなトピックについてユーザーを評価します。400 以上ある既定の問題から選択することも、組織独自の問題を設定することも可能です。さらに、事前定義されたナレッジ アセスメントとして、各カテゴリーで 17 のアセスメントが用意されています。

事前定義されたナレッジ アセスメント

- 55, 33 and 22-question broad assessments / 55、33、22 の質問による知識評価
- GDPR
- Internal Threat / 内部脅威
- Online Safety / オンラインの安全
- Password Protection / パスワード保護
- Payment Card Industry / クレジットカード業界
- Phishing / フィッシング
- Personally Identifiable Information (PII) / 個人識別情報 (PII)
- Preventing Compromise / 侵害防止
- Protected Health Information (PHI) / 保護されるべき医療情報 (PHI)
- Protecting Personal Data / 個人データの保護
- Securing Your Email Advanced / 電子メールの保護アドバンスド
- Securing Your Email Fundamentals / 電子メールの保護基本
- Security Safeguards / セキュリティ保護策
- Security on the Go / 外出時のセキュリティ

プルーフポイント トレーニング モジュール

多くの受賞歴を持つ柔軟なトレーニング モジュールには、インタラクティブなものや、ゲーム形式やビデオ形式のものなどがあります。モジュールは、ユーザーの行動の変化を促すよう、学習の効果を増大させる科学的理論に基づいて作成されており、脅威状況の変化に対応させるためプルーフポイントの脅威インテリジェンスから作成されています。

モジュールについて

- レッスンは短く、焦点を絞って構成されています平均で 5 分から 15 分程度で完了でき、集中力を切らすことなく、学び、理解することができます。
- コンテンツは、ユーザーに合わせて内容をカスタマイズすることが可能です。Customization Center では、セルフサービスで、テキスト、スクリーン、画像、質問、回答、コンテンツの順序などを編集することができます。
- アセスメント結果に基づきユーザーを自動的にトレーニングに登録することができます。これにより、適切な時に適切なトレーニングを受けることができます。
- インタラクティブ モジュールはモバイル フレンドリーでアクセスしやすい設計となっており、U.S. Section 508 スタンダードと Web Content Accessibility Guidelines (WCAG) 2.0 AA スタンダードに準拠しています。

トレーニング モジュールのトピック

- Application Security / アプリケーションのセキュリティ
- Anti-Fraud and Bribery / 詐欺と賄賂対策
- Anti-Money Laundering / マネーロンダリング対策
- Avoiding Dangerous Attachments / 危険な添付ファイルを回避
- Avoiding Dangerous Links / 危険なリンクの回避
- Business Email Compromise / ビジネス メール詐欺
- Compromised Devices / 侵害デバイス
- Data Protection and Destruction / データ保護と破壊
- Email Security / メールセキュリティ
- Email Security on Mobile Devices / モバイル端末でのメールのセキュリティ
- FERPA
- GDPR
- Healthcare / 医療
- Insider Threats / 内部脅威
- Phishing / フィッシング
- Malware / マルウェア
- Mobile Security / モバイル セキュリティ
- Passwords / パスワード
- PCI / クレジットカード業界
- Physical Security / ビデオ：物理的セキュリティ
- PII and Personal Data Protection / 個人情報の保護
- Privileged Access Awareness / 特権アクセス意識
- Ransomware / ランサムウェア
- カスタマー サービス、財務部門、管理部門向けのロールベース モジュール
- Safe Social Networking / 安全なソーシャル ネットワーク
- Safe Web Browsing / 安全な Web の閲覧
- Secure Printing / 安全に印刷する
- Security Beyond the Office / オフィス外のセキュリティ
- Security Essentials / セキュリティエッセンシャル
- Travel Security / 出張中のセキュリティ
- URL Training / URL トレーニング
- USB Device Safety / USB デバイスの安全性
- Working From Home / 在宅勤務
- Workplace Security in Action / 職場でのセキュリティの実践
- ビデオ：Workplace Security in Action / 職場でのセキュリティの実践

TeachPrivacy トレーニング モジュール

プルーフポイントは、トレーニングのコンテンツや種類の幅を広げるため、TeachPrivacy とも協力しています。パートナーのコンテンツは、すべて当社の学習開発チームが内容を確認しています。

TeachPrivacy は、プライバシー規制や要件の分野で深い専門性があります。同社の幅広いコンテンツから、プライバシーやコンプライアンスのトレーニングを組織独自の課題や文化に合わせて実施することができます。

TeachPrivacy のトピック

- California Health Privacy / カリフォルニア州医療プライバシー
- CCPA / カリフォルニア州消費者プライバシー法
- FERPA
- FTC Red Flags / FTC のレッド フラッグ
- GDPR
- GLBA / グラム リーチ ブライリー法
- HIPAA / 医療保険の携行と責任に関する法律
- Malware and Privacy / マルウェアとプライバシー
- PCI / クレジットカード業界
- Privacy for Federal Government Contractors / 連邦政府コントラクター向けプライバシー
- Texas Health Privacy / テキサス州医療プライバシー
- Ransomware / ランサムウェア

コンテンツのカスタマイズと配信

セルフサービスの Customization Center では、ユーザーごとに関連性の高いコンテンツを割り振ることができます。またユーザーに合わせて、文章表現、画像、質問をカスタマイズし、トレーニングを最適化できます。モジュール、レッスン、ページは複製することができ、必要な変更をすばやく、リアルタイムで行うことができます。トレーニング モジュール（質問付き）から意識向上モジュールにワンスイッチで切り替え可能です。

学習効果を維持するため、Learning Science Evaluator がコンテンツを管理し、フィードバックを提供します。たとえば、コンテンツの長さや量、質問の数が適切でない場合はそれを通知してくれます。

SCORM ベースのファイルを利用する独自の学習管理システム (LMS) を導入している場合は、学習モジュールをカスタマイズして、自社の LMS 用にエクスポートできます。複数のモジュールを 1 つにまとめたり、モジュールの優先順位を設定できます。

セキュリティ意識向上マテリアル

プルーポイントでは、組織のトレーニング イニシアティブを補強するためのモジュール、ビデオ、ポスター、画像、ニュースレター、記事、インフォグラフィックなどさまざまな意識向上マテリアルを提供しています。こうしたマテリアルは、サイバーセキュリティについて、ユーザーとの間で継続的に話し合えるように作成されています。セキュリティの問題を常に念頭におきながら、組織全体のリスクを低減できるようになっています。

- ほとんどの意識向上マテリアルは、組織のロゴをつけてカスタマイズすることができます。オリジナルのファイルは、セキュリティ意識向上マテリアル ポータルからアクセスできます。
- マテリアルの多くは 20 か国の言語でご利用いただけます。

Attack Spotlight と脅威アラート

市場をリードするプルーフポイントの脅威インテリジェンスを活用すれば、誰がどのように攻撃されるのかを把握して、対象となるユーザーに適切なトレーニングを提供することができます。脅威インテリジェンスからは常に新たな脅威についての情報が提供されるため、トレーニングや意識向上のアクティビティをただちに新しいリスクに対応させることもできます。

Attack Spotlight: ユーザーは、Attack Spotlight で最新の脅威を学ぶことができます。このタイムリーなコンテンツは、プルーフポイント脅威インテリジェンスが確認した現実のフィッシング攻撃、テクニック、餌 (ルアー) を基に、毎月、作成されています。

- COVID-19 (Coronavirus) (新型コロナウイルス)
- DocuSign Phishing (DocuSign フィッシング)
- Domain Fraud (ドメイン詐欺)
- Dridex (ドライデックス)
- Fake Browser Updates (偽のブラウザー アップデート)
- Fake OneDrive Emails Steal Logins (OneDrive ログインを窃取する偽の E メール)
- Fraudulent Shipping Notifications (不正な発送通知)
- Look-Alike Websites Trick Users (そっくり Web サイトでユーザーに罠を仕掛ける)
- Microsoft Office 365 Credential Phishing (Microsoft 365 (Office 365) 認証情報フィッシング)
- OneDrive Phishing Campaign (OneDrive フィッシング キャンペーン)
- Phishing Campaign Delivers Dangerous Trojan (フィッシング キャンペーンで危険なトロイの木馬を送信)
- Scammers Mimic Real Banking Emails (詐欺師は本物の銀行メールを真似る)
- Malicious Cloud Applications (悪意あるクラウド アプリケーション)

脅威アラート: プルーフポイント脅威インテリジェンスで実際に見られた具体的な脅威をユーザーに直ちに警告します。

- COVID-19 Credential Phishing (U.S. Retailers) (新型コロナウイルス認証情報フィッシング (米国小売業者)
- COVID-19 Phish Spreading Malware (U.S. Infrastructure) (新型コロナウイルス フィッシュ拡散マルウェア (米国インフラ))
- WebEx Credential Phishing Lures (WebEx 認証情報フィッシング ルアー)
- Zoom Credential Phishing Lures (Zoom 認証情報フィッシング ルアー)
- Zoom Phishing Attacks Spread Malware (Zoom フィッシング攻撃拡散マルウェア)
- More Every Week (毎週次々と更新)

意識向上ビデオ: ユーザーの関心を引くビデオを使って楽しみながらセキュリティ意識の重要性をユーザーと共有することができます。50 本を超えるビデオの一部をご紹介します。

- Awareness Video: Think Before You Click (Great Saves) / 意識向上ビデオ : クリックする前に立ち止まって考える (Great Save [グレートセーブ])
- Awareness Video: Is the Cloud Secure? / 意識向上ビデオ : クラウドは安全ですか?
- Awareness Video: Use Caution on Public Wi-Fi / 意識向上ビデオ : 公衆 Wi-Fi に気を付ける
- The Defence Works ビデオ : Not Particularly High Tech / 特別にハイテクというわけではない
- The Defence Works ビデオ : Oh… My Password! (なんということ!パスワードが!)
- The Defence Works ビデオ : Swiped Right Into Trouble (スワイプでトラブルに巻き込まれる)
- 60 Seconds to Better Security: What is Smishing? (60 秒でわかる : スミッシングとは?)
- 60 Seconds to Better Security: What is Phishing? (60 秒でわかる : フィッシングとは ?)
- 60 Seconds to Better Security: What is BEC? (60 秒でわかる : ビジネスメール詐欺 (BEC))
- その他多数

インフォグラフィック: 安全な PC 作業の基礎を強化するには、次のようなわかりやすい資料が便利です。

- ビジネス メール詐欺攻撃 の認識と回避
- Internet of Things (IoT (モノのインターネット))
- Phishing Decision Tree (フィッシングの決定木)
- Phishing (フィッシング) : A Scammer’ s Sinister Scheme (詐欺師の陰謀 (レギュラー版および拡張版))
- Tax-Related Schemes (税金関連スキーム)
- ランサムウェアの理解
- その他多数

ニュースレターおよび記事

- 新年度のスタート、危険なリンクや添付ファイル、ホリデー ショッピング、内部脅威、パスワード、フィッシング、物理的セキュリティ、旅行のコツなどの様々なトピックを説明する、セキュリティの話題を取り上げたニュースレターや記事です。

ポスター: メッセージを可視化して学習を補強します。

- 悪意ある添付ファイルの回避
- Be Smart About Mobile Security (モバイル セキュリティは賢明に)
- 行先が不明 - URL のセキュリティ
- Dangerous USB Devices (危険な USB デバイス)
- Is Physical Security on the Menu?
  (物理的セキュリティはできていますか?)
- Not All Offers Are as Sweet as They Seem
  (すべてのオファーが見た目どおりの甘いものではありません)
- その他多数

その他

- アートワークや追加コンテンツの作成方法
- 「Cybersecurity Consequences
  (サイバーセキュリティの対応)」ゲーム
- 「Lock Before You Walk
  (離れる時は ロックを しましょう)」ポストイット メモ
- ミーム
- ポストカード
- その他多数

プログラム マテリアル

プログラムの成功は、参加者の全員が参加する理由や期待されていることを理解することにかかっています。このため、セキュリティ意識向上プログラムのコンテンツには、プログラムを効果的に実施するための管理者向けエキスパート ガイダンスが含まれています。また、おもな関係者やユーザー向けのコミュニケーション資料も提供しています。プログラム マテリアルは、次の 4 つのカテゴリーに分けることができます。

- ベスト プラクティス
- 成功の鍵
- キャンペーン

これらは、プログラム管理者が組織内で信頼を得てセキュリティの文化を醸成することに役立つものです。

ベスト プラクティス:ベスト プラクティスのマテリアルは、プログラム管理者が効果的に行動の変化を促すための最適のマテリアルです。プログラムが新しいものであるか、または既にしばらく実施されているものであるかは問いません。コンテンツには、スケジュール、ベスト プラクティス、プログラム実施にかかる計画案などが含まれています。

キャンペーン:キャンペーンは管理業務を容易にし、また多くの情報から集約されたユーザー エクスペリエンスを生み出すために役立ちます。キャンペーンでは、内部コミュニケーション資料や、組織内の複数チャネルを通じて行われるセキュリティ意識向上イニシアティブのために必要なコンテンツが含まれています。

成功の鍵:ポッドキャスト、ウェビナー、リサーチその他のコンテンツで管理者のために提供されるものです。重要なオーディエンスに向けてセキュリティ意識向上トレーニングの重要性を働きかけ、トレーニングへの賛同を取り付け、セキュリティ対応のモデルに関する議論を促すために用いられます。プレゼンテーションは、事前に準備と録画が行われた、フィッシング、個人情報の盗難、ソーシャル エンジニアリングなどの多様なトピックを扱ったマテリアルです。対面でのトレーニング、またはオンラインでのトレーニングのセッションに活用できます。

詳細

トレーニング モジュールのデモ版のお試しとセキュリティ意識向上マテリアルは、
https://www.proofpoint.com/jp/resources/try-security-awareness-training からご覧ください。