proofpoint.

エグゼクティブ サマリー

2020 年版 State of the Phish

メールは最も重要なビジネスコミュニケーションチャネルであり、最大の攻撃経路でもあります。

サイバー攻撃者が標的、つまりユーザーを狙うときに、もっとも利用するのがメールです。彼らはメールを使った様々なフィッシング技術で、ユーザーに危険なリンクをクリックさせ、クレデンシャルを入力させ、送金や機密ファイルの送信などを行わせます。

このような脅威をより深く理解するために、今年第6回目となる*State of the Phish*レポートでは、エンドユーザーと情報セキュリティの調査結果、および12か月の期間で当社の顧客からユーザーに送信した5000万件以上のフィッシングシミュレーションメールを分析した結果をまとめています。また、サイバーセキュリティの用語と慣行についてユーザーが知っていることを評価し、情報セキュリティチームが直面しているフィッシング脅威について調査しています。最終的に、組織が人中心のアプローチを採用して今日のフィッシング脅威に対処する方法を明らかにしています。

主な調査結果は以下の通りです。

ユーザーの意識向上：社会人3,500人を対象としたグローバルな調査

- フィッシングの定義を正しく選択できたのは、わずか61%でした。
- ランサムウェアの定義を正しく選択できたのは、わずか31%でした。
- 主要な用語のテストでは、前回同様、ミレニアル世代は他の世代（ベビーブーム世代を含む）より正答率が低くなりました。
- 多くの人が、サイバーセキュリティのベストプラクティスを実行できていませんでした：
  - 45%はパスワードを使いまわしています。
  - 50%以上は、自宅のWi-Fiネットワークにパスワードをかけていません。
  - 32%は、バーチャルプライベートネットワーク（VPN）が何かを理解していません。
- 90%の社会人は、会社支給デバイスを私用で使っています。約50%は、友人や家族に会社支給デバイスを使用させています。

ITの課題：情報セキュリティプロフェッショナル600人を対象としたグローバルな調査

- 55%の組織では、2019年に最低1回フィッシング攻撃の被害を被っています。
- ほとんどの組織では以下のような様々なソーシャルエンジニアリング攻撃にあっています。
  - スピア フィッシング：88%
  - ビジネスメール詐欺（BEC）：86%
  - ソーシャルメディア：86%
  - スミッシング（SMS/テキストフィッシング）：84%
  - ビッシング（音声でのフィッシング）：83%
  - 悪意のあるUSBドロップ攻撃：81%
- 2019年には、33%の国際組織がマルウェアに感染し身代金を支払いました。（32%は感染したものの、支払いはしませんでした。）支払いの交渉をした組織のうち：
  - 9%が再度、身代金を要求する攻撃を受けました。
  - 22%は、身代金を支払った後もデータを復元できませんでした。
- 85%の組織は不審なメールの報告ボタンをエンドユーザーに利用させておらず、ユーザーをフィッシングの防御壁として活用できていません。

- 78%の組織では、セキュリティ意識向上トレーニングを行った結果、フィッシング攻撃に対する脆弱性の低下を数値化できました。

ユーザーアクション：Proofpointデータの分析

- Proofpointを利用している組織のエンドユーザーは、2019年に約920万通の不審なメールを報告しました。これは前年比で67%増です。2019年の第3四半期のみを見ても、ユーザーは何千もの重大な脅威を情報セキュリティチームに報告しています：
  - クレデンシャルを狙ったフィッシング攻撃が約20,000件
  - マルウェアペイロードを使った攻撃が4,000件以上（危険度の高いリモートアクセス型トロイの木馬（RAT）、バックドア、スティーラを含む）
- 報告率が高いということは、ユーザーがフィッシングに注意するようになってきているということを示しています。こういったユーザーは不審なメールを受け取った場合に情報セキュリティチームへ報告する可能性が高く、フィッシング対策を向上させてくれます。そのため、フィッシング攻撃シミュレーションの結果を分析する際は、誤答率よりも報告率に注目するべきです。例えば：
  - フィッシング攻撃シミュレーションの平均誤答率は、金融と教育業界は同程度でした（8%）。
  - しかしフィッシングテストの報告率では、金融業界が20%と最高だったのに対して、教育業界では5%と最低でした。
- 攻撃の標的と手法は日々変わりつつあります。そしてVery Attacked People™ (VAP) はVIPとは限りません。
- 人を中心とした視点から脆弱性を確認し、ユーザーが強固な防御壁となれるように、適切なツールを提供する必要があります。ユーザーは誰でも標的になり得ます。そのため、自社のデータと脅威インテリジェンスを用いたセキュリティ意識向上トレーニングプログラム（全社向け、及び対象を絞ったトレーニング）を開発することが重要です。

主な調査結果：アメリカ

- アメリカの社会人でフィッシングの定義を正しく答えられたのは、わずか49%でした。
- アメリカの社会人は公衆Wi-Fiを信頼している割合が最も高く：45%が、信頼できる場所（喫茶店やホテルなど）のWi-Fiは安全だと考えていました。
- アメリカの社会人のうち70%は友人や家族に会社支給デバイスを使用させています

主な調査結果：欧州、中近東、アフリカ

- フィッシングの定義の正答率はドイツが最も高く、66%でした。
- スミッシングとビッシングの定義の正答率が最も高かったのはフランスで、スミッシングで54%、ビッシングで48%でした。
- スペインではマルウェアの定義の正答率が79%と最も高かったものの、ランサムウェアの定義の正答率は22%と最低でした。
- イギリスはWi-Fiの安全策についての知識が最も少なく：21%が、自宅のネットワークの安全対策方法がわからないので何もしていないと回答しました。
- イギリスではフィッシング攻撃に繰り返し騙された社員に罰金を科す組織が最も多く、21%に上りました。フランスの組織ではこういった「繰り返し騙される社員」を解雇する割合が最も高く、13%の組織で行われていました。
- スペインの組織はすべて、2019年にソーシャル攻撃とスミッシング攻撃にあっています。
- ランサムウェア攻撃の身代金を支払ったドイツの組織のうち、半数以上の組織ではデータを復元できませんでした。

主な調査結果：アジア太平洋

- ランサムウェアの定義の正答率はオーストラリアが最も高く、42%でした。
- オーストラリアは34%の社会人がデバイス上でVPNを使う必要がないと考えており、他地域より高くなりました。
- オーストラリアは2019年にソーシャル、スミッシング、ビッシング攻撃にあった割合が最も低く、約60%でした。
- 日本の社会人の20%以上は、1つまたは2つのパスワードを複数のオンラインアカウントで使いまわしていました。
- スミッシングの定義の正答率は日本が最も低く、17%でした。
- 日本でフィッシングの被害にあった組織は42%のみで、世界平均の55%を大きく下回りました。
- 日本の組織で2019年にランサムウェアの身代金を支払ったのはわずか10%でした。

もっと詳しく

詳細は **proofpoint.com/jp** でご確認ください。

---

proofpointについて

Proofpoint, Inc.（NASDAQ:PFPT）は、サイバーセキュリティの主導的企業であり、組織の最大の資産であり同時に最大のリスクでもある「人」を守ります。Proofpointは、クラウドベースの統合ソリューションによって、世界中の企業が標的型脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000の過半数を超える企業を含むあらゆる規模のトップ企業が、メールやクラウド、ソーシャルメディア、Web関連の最も重要なセキュリティリスクおよびコンプライアンスリスクを低減させるために、Proofpointを利用しています。詳細は **www.proofpoint.com** でご確認ください。