フィッシングインサイト 2021

フィッシングは四半世紀前から存在していますが、それは進化し続けているため、常に効果的なサイバー攻撃手法を持ち続けています。攻撃者は、パンデミックがもたらした多くの新しいフィッシングの機会をすばやく見つけ出し、新しい戦術と技術を開発します。

フィッシングは、組織にとって、複雑な多段的な攻撃の最初のステップであることがほとんどです。攻撃者は、ユーザーをだます目的で頻繁にフィッシングを使用して、マルウェアをインストールしたり、被害者のネットワークにアクセスを提供する認証情報を共有したりします。一見無害に見えるメールは、最終的にはランサムウェア、クリプトジャッキング、データ窃盗に繋がる可能性があります。

このレポートでは、世界中の IT 最前線にいる 5,400名の IT 専門家を対象とした独立調査に基づいて、フィッシングに関する最新の情報と数百万ドルのランサムウェアインシデントとなった実際のフィッシング攻撃の事例を提供します。

Verizon 2021 Data Breach Investigation Report によると、確認済みのデータ侵害の 36% がフィッシング関連です (2019年の 25% から増加)。これらの調査結果を使用して、お客様のフィッシングのセキュリティ状態を確認し、保護を拡張する機会を特定してください。

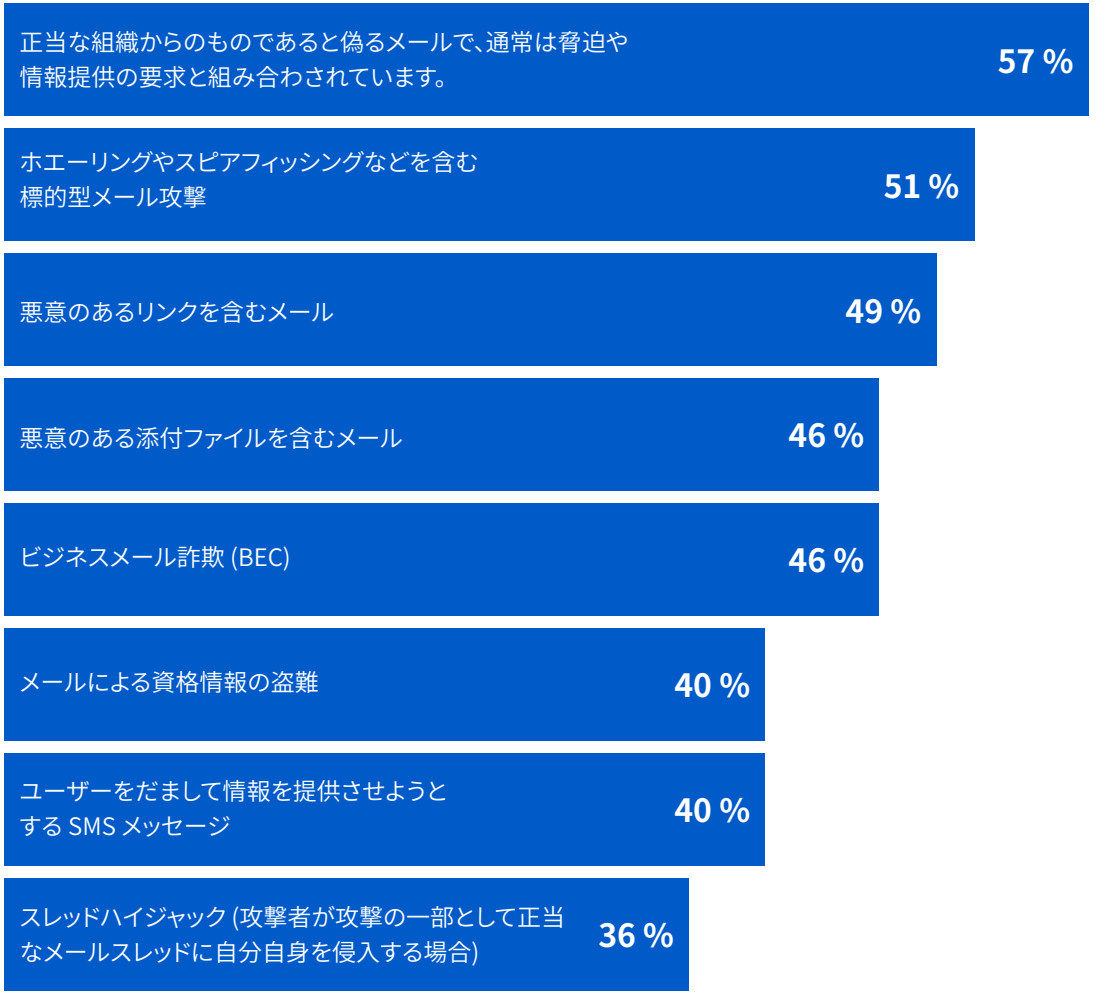
SOPHOS

1.フィッシングの意味合いは、ユーザーによって異なる

フィッシングとは何でしょうか？ソフォスの調査によると、IT 専門家の間でさえ、フィッシング攻撃と見なされるものには大きなばらつきがあります。最も一般的な理解では、正当な組織からのものであると偽るメールで、通常は脅迫や情報提供の要求と組み合わされています 通常、脅威や情報の要求とが組み合わされています。これは回答者の 10人に 6人 (57%) 未満が選択するオプションで最も一般的な回答でしたが、フィッシングの理解に幅があることを意味しています。

回答者の 46% は、ビジネスメール侵害 (BEC) 攻撃をフィッシングと見なし、3分の1（36%）以上は、フィッシングは攻撃者が自分自身を攻撃の一部として正当なメールのスレッドに挿入するようなスレッドハイジャックを含むと見なしています。

次のうち、フィッシング攻撃と思われるものはどれですか？



これらのオプションのうち、フィッシング攻撃と思われるものはどれですか？[5,400人] いくつかの回答オプションを除く

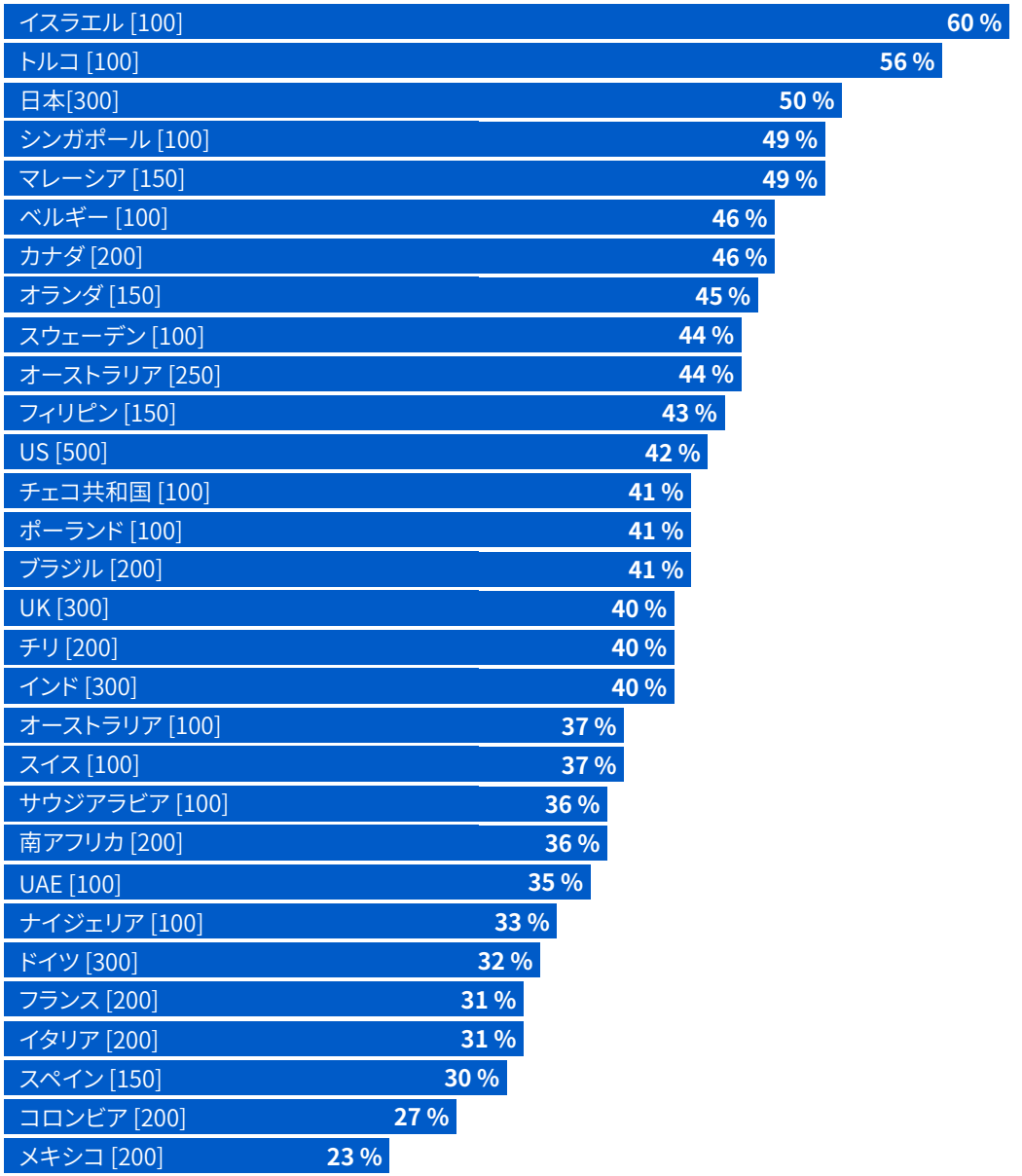
文化的要因は、フィッシングに対する人々の理解に大きな影響を及ぼします。たとえば、情報を提供してユーザーを騙そうとしている SMS メッセージをフィッシング詐欺と考えるイスラエルの回答者の割合は、メキシコの 2倍以上です（60% 対 23%）。多くの IT 専門家は、このことをフィッシングではなくスミッシングと呼んでいますが、信頼している企業からのものを装う偽のメッセージは、送信手段に関係なく同じ影響を与えます。

フィッシング攻撃の理解や定義に関して IT 専門家の間でこのようにさまざまな違いがあるということは、IT スタッフ以外の従業員にも同様またはそれ以上にさまざまな解釈が存在すると考えるのが妥当です。

フィッシングの意味合いが、ユーザーによって異なることを理解することは、フィッシングの認識と教育プログラムを作成、または実行するすべての人にとって重要な洞察です。フィッシングトレーニングを効果的に行うには、フィッシングの基本定義を共有して、学習内容を正しいコンテキストで理解できるようにすることが重要です。

ポイント：教育資料やユーザー意識向上トレーニングを提供する際は、フィッシングの意味合いが、ユーザーによって異なる点をご留意ください。適切なコンテキストがない場合、トレーニングの効果は低下します。

フィッシング攻撃をするためにユーザーをだまして情報を提供させようとする SMS メッセージをフィッシングだと考える回答者



これらのオプションのうち、フィッシング攻撃と思われるものはどれですか？[回答した組織数] ユーザーをだまして情報を提供させようとする SMS メッセージ

2.パンデミック以降、フィッシング攻撃が大幅に増加

調査回答者の 70% が、パンデミック以降、組織へのフィッシング攻撃が増加していると報告しました。すべての業種が影響を受け、中央政府が最も高い増加 (77%) を経験し、ビジネス/プロフェッショナルサービス (76%)、医療機関 (73%) があとに続きました。

業種間のわずかな違いは、四捨五入前* だとわずか 10% ほどで、攻撃者は通常は無差別で、かつ攻撃の成功の可能性を高めるためになるべく多くのユーザーにアプローチしようとしていることが分かります。

SophosLabs の調査、攻撃者は次に書かれているようなパンデミック、および自宅や職場の境界のあいまいさによってもたらされた機会を、早速活用したことを明らかにしました。

- 在宅勤務の急速な普及。攻撃者は、ユーザーが在宅勤務やオフィス以外の環境で仕事をすることに適応しながら、彼らのガードが緩くなることを望んでいる可能性があります。
- ホームデリバリーの増加。パンデミックの最初の数か月、多くの人々がオンラインショッピングに目を向けたため、宅配会社を装うフィッシングメッセージが一般的になりました。
- パンデミックに対する幅広い懸念。攻撃者は、パンデミックをテーマにした詐欺を使って、人々の不安や COVID-19 に関する必須情報を悪用しました。人々の懸念が高いことで、クリックする前にメッセージが正当なものであるかどうかを確認する可能性が低くなることを攻撃者は予想していました。

業種	パンデミック以降、組織に対するフィッシング攻撃の増加を経験した回答者
中央政府および政府外公共機関 [117]	77%
ビジネス/プロフェッショナルサービス [361]	76%
医療 [328]	73%
メディア/レジャー/エンターテイメント [145]	72%
エネルギー/石油・ガス/公共サービス [197]	72%
小売 [435]	71%
教育 [499]	71%
その他 [768]	71%
地方自治体 [131]	69%
流通/輸送 [203]	68%
金融サービス [550]	68%
建設/不動産 [232]	68%
IT/テクノロジー/通信 [996]	68%
製造/生産 [438]	66%

パンデミック以降、組織に対するフィッシング攻撃数の変化を感じましたか？[回答した組織数] はい、大きく増加しました。はい、少し増加しました。

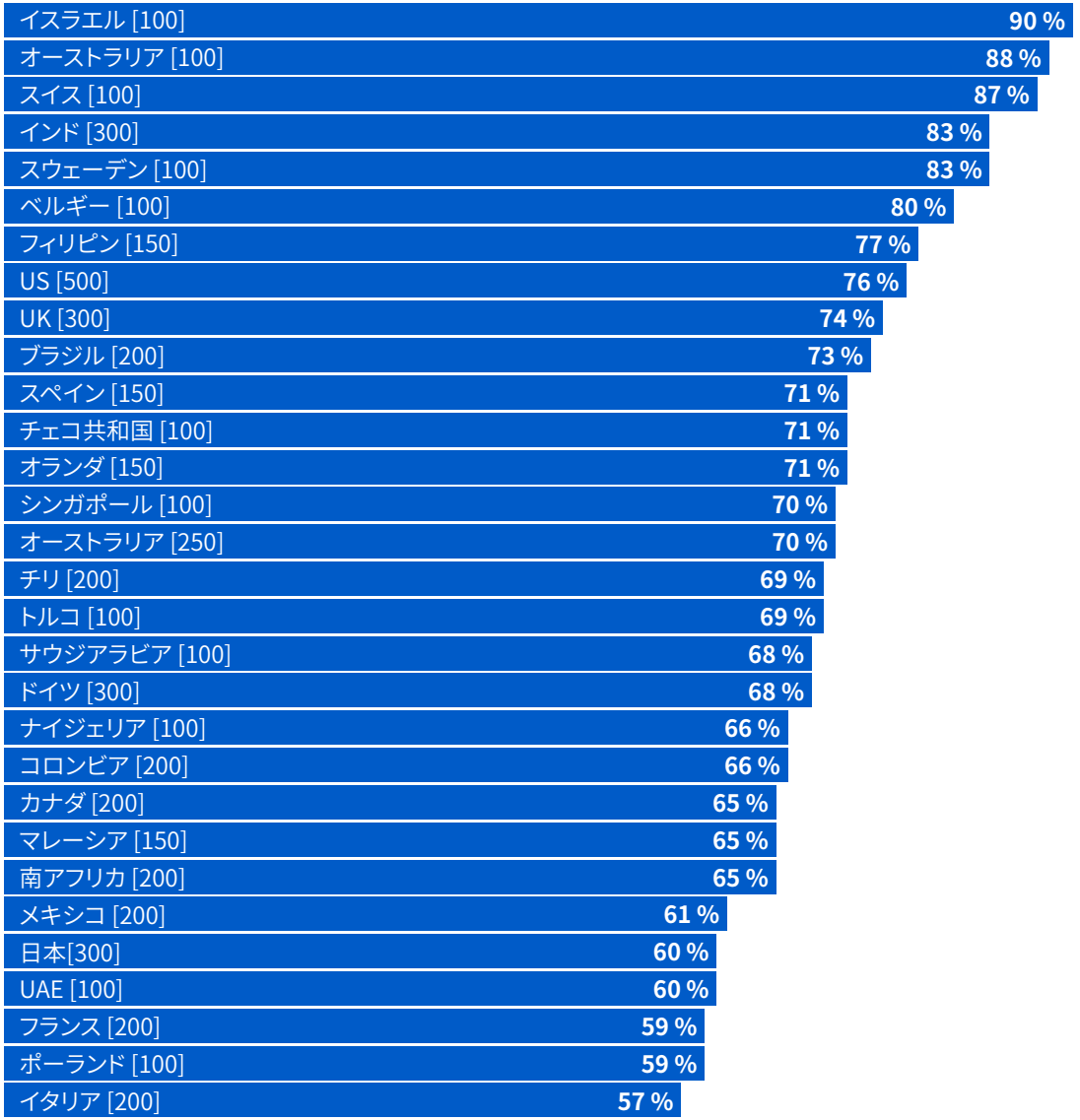
*四捨五入前、中央政府の回答者の 76.92% を、製造業の 66.43% と比較すると増加の実際の差異は 10.48% と報告されています。

業種ごとの全体的な差異はほとんどありませんでしたが、この調査では、パンデミック以降、国によって報告されたフィッシング攻撃の増加に大きな差があることが明らかになりました。たとえば、イスラエルの回答者の 90% は、イタリアの 57% に比べてフィッシングが増加していると回答しています。これらの結果は、回答者によるフィッシングの定義、および攻撃の追跡や測定能力に影響されますが、最前線での IT 専門家の実際の経験に関する貴重な洞察が分かります。

フィッシングメールにはさまざまな種類があるのと同様に、その背後にはさまざまなサイバー犯罪者が存在します。熟練した攻撃者グループは、通常、オーストラリア、スイス、スウェーデンなどの GDP が高い国に標的型攻撃を集中させて、収益を最大化にします。このことが、これらの国でフィッシングの増加が大きくなっている可能性があります。同時に、フィッシングは、マス市場の「spray and pray」攻撃にも使用されます。攻撃者は、多くの人数を攻撃することで、最終的には誰かが詐欺に遭うことを望んでいます。

ポイント: フィッシング対策の努力は怠らないでください。サイバー犯罪者はこの手法を増やしているので、業種や国はこれを見逃さないでください。

パンデミック以降、組織に対するフィッシング攻撃数の増加を経験した回答者



パンデミック以降、組織に対するフィッシング攻撃数の変化を感じましたか？[回答した組織数]
はい、大きく増加しました。はい、少し増加しました。

3.ほとんどの組織では、フィッシングに対処するためにサイバーセキュリティ意識向上プログラムを実行

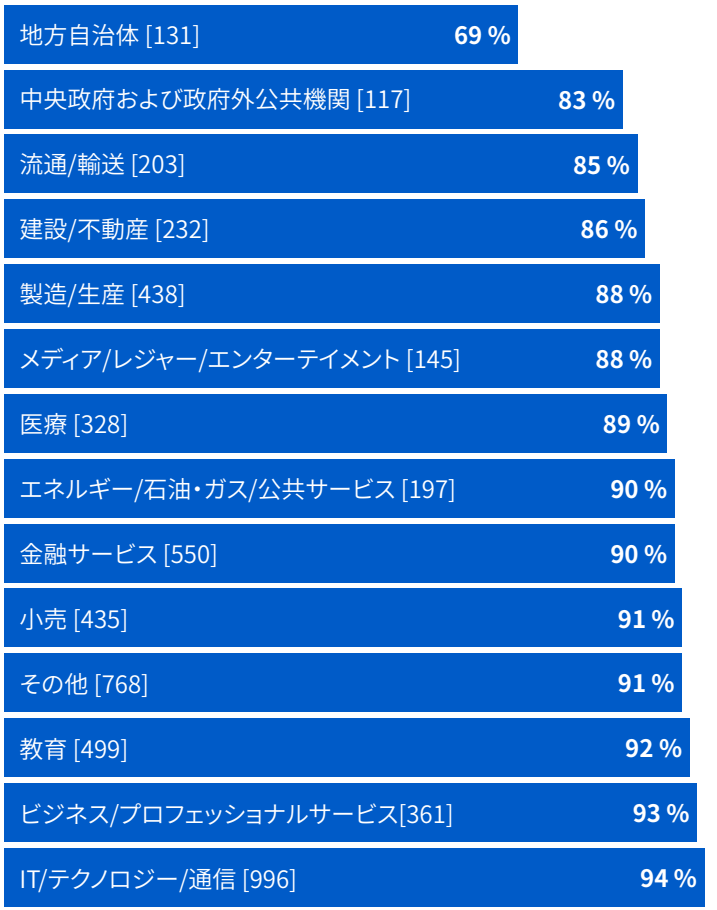
90% の組織が、フィッシングに対処するためにサイバー意識向上プログラムを導入しており、さらに 6% の組織がフィッシングの設定を計画しています。

最も一般的なやり方はコンピュータベースのトレーニングで、58% の組織が使用しています。半数以上 (53%) が人間主導のトレーニングを使用し、43%がフィッシングシミュレーションを実施しています。16% の組織は、3つの手法 (コンピュータベースのトレーニング、人間主導のトレーニング、フィッシングシミュレーション) すべてを意識向上プログラムで組み合わせています。

調査によると、フィッシングに対処するためのサイバーセキュリティ意識向上プログラムの実施に関しては、政府機関が遅れをとっており、地方自治体 (69%) と中央政府 (83%) の 2つが最下位を占めています。政府機関は影響力の高いサイバー攻撃の標的になることが多いため、このことが懸念されます。中央政府は恐喝型のランサムウェア攻撃を経験する可能性が高く、地方自治体はランサムウェア攻撃でデータを暗号化される可能性が高いです。

ポイント：フィッシングに対処するサイバーセキュリティ意識向上プログラムをまだ持っていない 10% にいる場合は、すぐにそのプログラムを実行してください。

サイバーセキュリティ意識向上プログラムを使用して、フィッシング対応



お客様の組織には、フィッシングに対処するサイバーセキュリティ意識向上プログラムがありますか？[5,400人] はい、コンピュータベースのトレーニングプログラムを実施しています。はい、フィッシングシミュレーションを実施しています。

90%

フィッシングに取り組むためにサイバーセキュリティ意識向上プログラムを実行する割合

58%

コンピュータベースのトレーニングプログラムを実行

53%

人間主導のトレーニングプログラムを実行

43%

フィッシングシミュレーションを実行

お客様の組織には、フィッシングに対処するサイバーセキュリティ意識向上プログラムがありますか？[5,400人] はい、コンピュータベースのトレーニングプログラムを実施しています。はい、フィッシングシミュレーションを実施しています。

4.確立されたフィッシング意識向上プログラム

フィッシング意識向上プログラムの約 3分の 2（65%）は、過去 10年以内の攻撃者手法の変化に対する組織の対応を反映して、1年から3年前に実装されました。2010 年半ばの Web ベースの攻撃に対するサイバー防御の改善により、攻撃者はメールなどの新しいベクトルに切り替えることを余儀なくされ、その結果、ユーザー教育プログラムに対する強いニーズが生まれました。

世界的なパンデミック以降、フィッシングが広範囲に蔓延していることを考えると、企業の 98% が COVID-19 が攻撃される前にフィッシング意識向上プログラムを導入していたことは心強いことです。これらのプログラムのおかげで、従業員は昨年のフィッシングメールの集中砲火に耐えられるようになりました。

ポイント: フィッシング詐欺の意識向上に関する資料や活動を定期的に確認、更新し、ユーザーにとって関連性があり関心が持てるものであることを確認してください。

フィッシングに対処するサイバーセキュリティ意識向上プログラムをお客様の組織はいつ実装しましたか？	
昨年	2%
1 ～ 2年前	30%
2 ～ 3年前	35%
3 ～ 4年前	20%
4 ～ 5年前	12%
5年以上前	0%
不明	1%

フィッシングに対処する意識向上プログラムを組織に導入していると答えた回答者 [4,866人]

5.積極的な追跡手段がトレーニングの有効性評価に影響を与える

フィッシングに対処するためにユーザーの意識向上プログラムを実行しているほとんどすべての組織 (98%) が、その取り組みの影響を評価しています。結果の測定と追跡により、組織はプログラムを最適化して結果を改善することができます。

最も一般的なやり方は、IT チームに報告されたフィッシングメールの数 (68%) やユーザーによるフィッシングの報告レベル (65%) を追跡することです。優れたユーザーの意識向上と行動を反映するこれらのポジティブに焦点を当てた評価基準が最も一般的であることは心強いことです。フィッシングを特定したり、その意識を高めることで、IT チームはユーザーがフィッシング詐欺に陥るのを事前に防止できます。

組織の半数 (50%) は、フィッシングメールのクリック率を追跡しています。ネガティブな評価基準 (詐欺に引っかかることに焦点を当てた評価) では、クリック率が IT チームに対して、最も必要とする意識向上のターゲットはどこかを知るデータを提供し、組織内の現実を反映するようにコンテンツを作成します。ポジティブとネガティブの両方のデータポイントが多いほど、追跡しやすくなります。

ポイント：評価の結果を踏まえてユーザーの教育プログラムを定期的に見直し、ポジティブな振る舞いを認識し、高く評価することに焦点を当ててください。

98%
意識向上プログラムの効果を評価

68%
IT 部門が発行したフィッシング関連のチケットの数を追跡

65%
ユーザーが作成したフィッシングメールの報告レベルを追跡

50%
フィッシングメールのクリック率を追跡

意識向上プログラムの影響を評価するために何を追跡していますか？[組織がフィッシングに対処するための意識向上プログラムを実施している 4,866人の回答者] IT 部門が発行したフィッシング関連チケットの数、ユーザーによるフィッシングメールの報告レベル、つまりフィッシングメールのクリック率。フィッシング認識プログラムの効果は評価していません。回答オプションの一部を除く

導入事例：フィッシングメールがいかに何百万ドルものランサムウェア攻撃をもたらしたか

Sophos Rapid Response チームは、大規模なランサムウェア攻撃を受けた企業から支援の依頼を受けました。攻撃が封じ込められた後、Rapid Response チームはインシデントを調査して、その攻撃がどのように始まったかを理解しました。分かったことは次のとおりです。

攻撃の 3カ月前に、従業員はフィッシングメールを受信していました。このメールは、他のオフィスにいる同僚から送信されたようです。攻撃者が同僚のメールアカウントにアクセスして、同僚の従業員になりすましてメッセージを信頼させた可能性があります。

このメッセージは非常に短く、つたない英語で書かれていました。従業員にリンクをクリックしてドキュメントを確認するようにそこには書かれていました。実際、このリンクは悪意のある Web リンクであり、従業員がリンクをクリックすると、攻撃者はドメイン管理者のアクセス資格情報を取得できるようになります。

Rapid Response チームは、フィッシングメールは、初期アクセスブローカーによって送信されたと考えています。彼らはまず組織の環境へのアクセスを保護し、その後ランサムウェアやデータの盗難などのさまざまな攻撃で使用することを目的とした他の攻撃者にアクセスを販売することに焦点を当てたサイバー犯罪者です。

今回ケースでは、被害者の IT チームが介入し、フィッシング攻撃をシャットダウンしました。それで終わりのように見えました。

しかし、8週間後、悪意のある攻撃者が被害者のコンピュータに Cobalt Strike と PowerStploit PowerView の 2 つのツールをインストールして実行しました。これらは、ペネトレーションテスターや悪意のある目的を持つサイバー犯罪者が合法的に使用できる商用ツールです。おそらく攻撃者は PowerView を使用してネットワーク偵察を実行し、その一方で Cobalt Strike が永続性を確立し、攻撃者がネットワークに留まることができるようになりました。

攻撃者の調査活動の約 2週間後、すべてが静かになりました。Rapid Response チームは、このことを初期アクセスブローカーがこの企業へのアクセス資格を望む購入者を探しているためだと考えています。

販売されると、新しい「所有者」はそのアクセス資格情報をすぐに活用しました。彼らはすぐにネットワークに侵入し、より多くのマシンに Cobalt Strike をインストールし、情報の収集と窃盗を開始しました。

一番初めのフィッシングメールから 3カ月後に、攻撃者は現地時間の午前 4時に REvil ランサムウェアを解き放ち、250万ドルの身代金を要求しました。

AI を搭載した Sophos Email のフィッシング対策を入手

高度な機械学習により、**フィッシング詐欺師とBEC攻撃を特定**

主要なフィッシングインジケーターをリアルタイムでスキャンすることで、**ソーシャルエンジニアリングの手法をブロック**

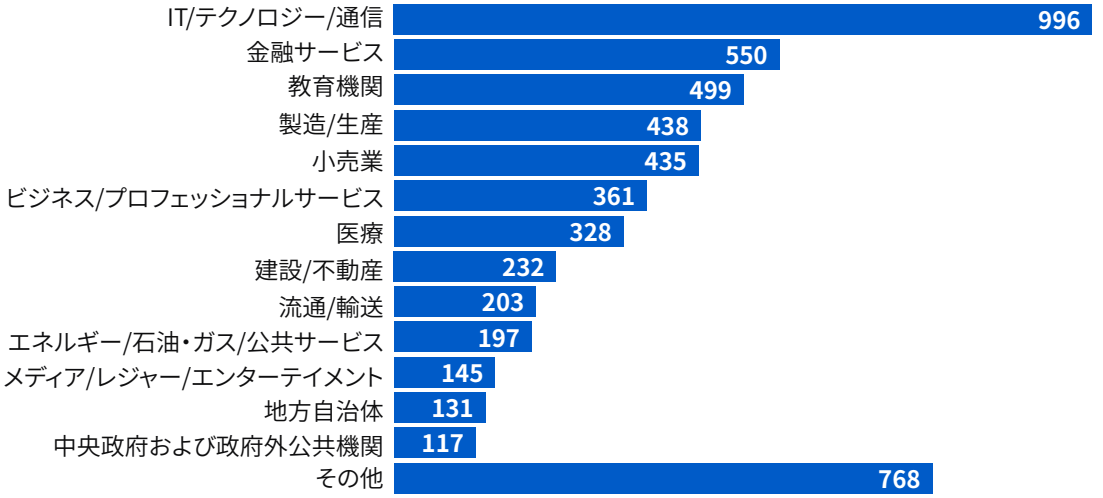
配信前および配信後の保護により、**悪意のあるリンクやマルウェア**を阻止

詳細と無償評価版はこちらから sophos.com/email

調査について

ソフォスは、独立系の調査会社 Vanson Bourne 社に委託して、30か国にわたる中規模（100～5,000人の従業員）の組織の 5,400人の IT 意思決定者に調査しました。調査は、2021年 1月と 2月に実施されました。また、回答者は、民間部門および政府/公共部門の両方からとなります。

業種別の回答者数



国別の回答者数

国	回答者数	国	回答者数	国	回答者数
オーストラリア	250	インド	300	サウジアラビア	100
オーストリア	100	イスラエル	100	シンガポール	150
ベルギー	100	イタリア	200	南アフリカ	200
ブラジル	200	日本	300	スペイン	150
カナダ	200	マレーシア	150	スウェーデン	100
チリ	200	メキシコ	200	スイス	100
コロンビア	200	オランダ	150	トルコ	100
チェコ共和国	100	ナイジェリア	100	アラブ首長国連邦 (UAE)	100
フランス	200	フィリピン	150	英国	300
ドイツ	300	ポーランド	100	米国	500

2021-08-13 WPJA (NP)

SOPHOS