KnowBe4

業界別フィッシングベンチマーキングレポート

2023年度版

目次

VERIZONの2023年度のデータ侵害調査レポートによると**データ漏洩の74%は人的要因によるものです。**単なるミス、認証情報の盗難、ソーシャルエンジニアリングなど、データ漏洩には人的要因が大きくかかわっています。

人的要因によるデータ漏洩への関心の高まりが効果を見せ始めていますが、まだ十分ではありません。

はじめに

サイバー犯罪者は様々な方法でデジタル環境にアクセスすることができます。技術的なセキュリティ管理によって「ハッキングによる侵入」がますます難しくなる中、サイバー犯罪者たちは、レジリエンスが比較的低いターゲットである人的レイヤーに目を向けています。人的レイヤーは、恰好の攻撃ベクトルです。犯罪者はあらゆる弱点を探し、仕事とプライベートの両方の場面でこれを攻撃してきました。残念なことに、多くの企業はテクノロジーに基づくセキュリティレイヤーを重要視し、人的レイヤーの重要性をあまり考慮していません。また、ほとんどの人はプライベートでのリスク予防措置を取らないため、脆弱なまま日々を過ごすことになります。

サイバー脅威は増加の一途をたどっており、犯罪者は試行錯誤を重ねた攻撃手法を利用すると同時に、人的防御レイヤーの効果を最小限に抑えることより洗練された新たな方法を開発してデジタル環境への侵入を試みています。サイバー攻撃から組織を最善の方法で守るためには、従業員がセキュリティカルチャーを推進するために必要な知識、適応した習慣、行動を身につけることが必要です。そのためにはトレーニングをより発展的かつ一貫性のある、本能的なものに変える必要があるでしょう。

すべての地域、業種、企業/組織規模において、フィッシング攻撃は前年比で大幅に増加しています。サイバー犯罪者は被害者を選びません。様々な種類のソーシャルエンジニアリングを通じて、仕事場でも娯楽であっても、昼夜を問わず、ターゲットとなる人に対する攻撃を慎重に構築しているのです。サイバー犯罪者は次の侵入戦略を考える際も、こうした人間の脆弱性を狙い続けてくることでしょう。私たちは、世界的な社会経済問題や健康問題に対処し続けながら、サイバー犯罪者のスキルを強化する人工知能の進歩とも闘わなければなりません。

2022年度、FBIのインターネット犯罪苦情センター (通称IC3) が受ける**アメリカ一般市民からの苦情数は増加しています。80万944件 (毎日2,175件以上) の苦情が報告されており、これは2021年から5%増加、潜在的な損失は103億ドルを超えました。**
さらに、ビジネスメール詐欺は**21,832件にのぼり、調整後の損失額は約27億ドルとなっています。**これらはあくまでも報告された事案のみです。投資詐欺と重要インフラへのランサムウェア攻撃は、最も利益性のある詐欺だということが立証されています。各業界は、システムが危険にさらされ手遅れとなる前に不審な行動を検知・保護・報告するための人的防御レイヤーを備える取り組みに着手しています。

セキュリティリーダーが問題に目を向けず、必要最低限のことしかしない、またはテクノロジーだけを重視し、旧態依然としたトレーニング方法に頼っている場合、これは潜在的な攻撃に対して組織を脆弱なままに放置していることになります。さらに、必要なコンプライアンストレーニングをセキュリティ意識向上トレーニングと混同していると、従業員の知識や能力に大きなギャップが生じるでしょう。 この2つの重点分野を組み合わせて、組織に悪影響を及ぼす可能性のある分野をすべてカバーする、総合的かつ包括的な学習プログラムを作成すべきです。

さまざまなスタイルやバージョンのコンテンツ、継続的なテストやコミュニケーションを含む包括的かつ集中的なプログラムを推進することは、強靭なセキュリティカルチャーを構築する上で必要な取り組みです。

データ漏洩の根本的な原因の大半は人的要因にあるとされている中、セキュリティリーダーがテクノロジーベースのセキュリティレイヤーにのみ投資し続けていると、脆弱性を軽減できるベストプラクティスとして有効な「セキュリティ意識向上トレーニング」と、頻繁に実施すべき「模擬ソーシャルエンジニアリングテスト」が見落とされてしまうリスクがあります。
このアプローチは、サイバー犯罪に対抗する従業員の準備レベルを高めるだけでなく、組織全体に強力なセキュリティカルチャーを推進する上で必要となる重要な基盤を築くものです。

フィッシング攻撃が増加の一途をたどる中、サイバー犯罪者は、従業員に必要な知識・注意力・エネルギーが不足していることを逆手に取り、従業員を騙してフィッシングを仕掛けてきます。つまりストレスが多く、注意力散漫で、教育のなされていない従業員が一人いるだけで、悪質な行為者に狙われてしまうということです。

セキュリティリーダーは、従業員がフィッシングメールを受け取ったときにどう行動するかを知っておく必要があります。リンクをクリックするでしょうか？だまされて認証情報を漏らすでしょうか？マルウェアに感染した添付ファイルをダウンロードするでしょうか？セキュリティチームに知らせずにメールを放置したり削除したりするでしょうか？
あるいは、フィッシングの疑いを報告し、人的防御レイヤーとして積極的な役割を果たすでしょうか？**各企業や組織の従業員がこうしたフィッシング攻撃の被害をどれくらい受けやすいかを示したのが、Phish-prone™ Percentage (PPP: フィッシング詐欺ヒット率) と呼ばれるものです。**フィッシングリスクを測定可能な指標に変換することで、リーダーたちは侵害のリスクを数値化し、「人」を標的にしたサイバー被害のリスクを低減するトレーニングを導入することができるのです。

> セキュリティリーダーは、従業員がフィッシングメールにどう反応するかを知っておく必要があります。**メール内にリンクがあった場合、果たしてクリックするでしょうか？**

業界別リスクの現状把握

企業や組織に対して算出されるPPPは、従業員がソーシャルエンジニアリングやフィッシング詐欺に対してどれくらい脆弱であるかを示しています。標的となった従業員の中にはだまされてリンクをクリックしたり、マルウェアに感染したファイルを開封したり、または組織の資金をサイバー犯罪者の口座へ送金したりしてしまう人もいます。PPPの数値が高いほどリスクも大きく、攻撃被害を受けやすい従業員の数も多いということになります。PPPは低く抑えることが理想とされています。そのためには、従業員がサイバーセキュリティに精通し、こうしたリスクを認識して未然に防ぐことが必要です。

つまり、PPPの数値が「低い」からといって、企業や組織のヒューマンファイアウォールが脆弱であるわけではありません。むしろ、PPPが低い方がセキュリティは強化されています。PPPは実際の状況も踏まえて見るとさらに有効活用することができます。PPPを確認した後で多くのリーダーは、「自社の状況は他社と比べてどうなのか」、「PPPを低下させるのにできることは何か」、「自社でより良いチームを構築するにはどうすればよいのか」といったことを自問します。

本レポートは、自社のPPPレベルを同業他社と比較し、脆弱性ランキングが示唆するものを理解したいというニーズに応えて、KnowBe4が業界を横断して毎年実施している調査をまとめたものです。脆弱性を業種/組織規模別に分類し、組織のセキュリティをより強化してよりレジリエントなセキュリティカルチャーを築くために役立つパターンを探求します。

2023年度 各国業界別フィッシング ベンチマーキング調査

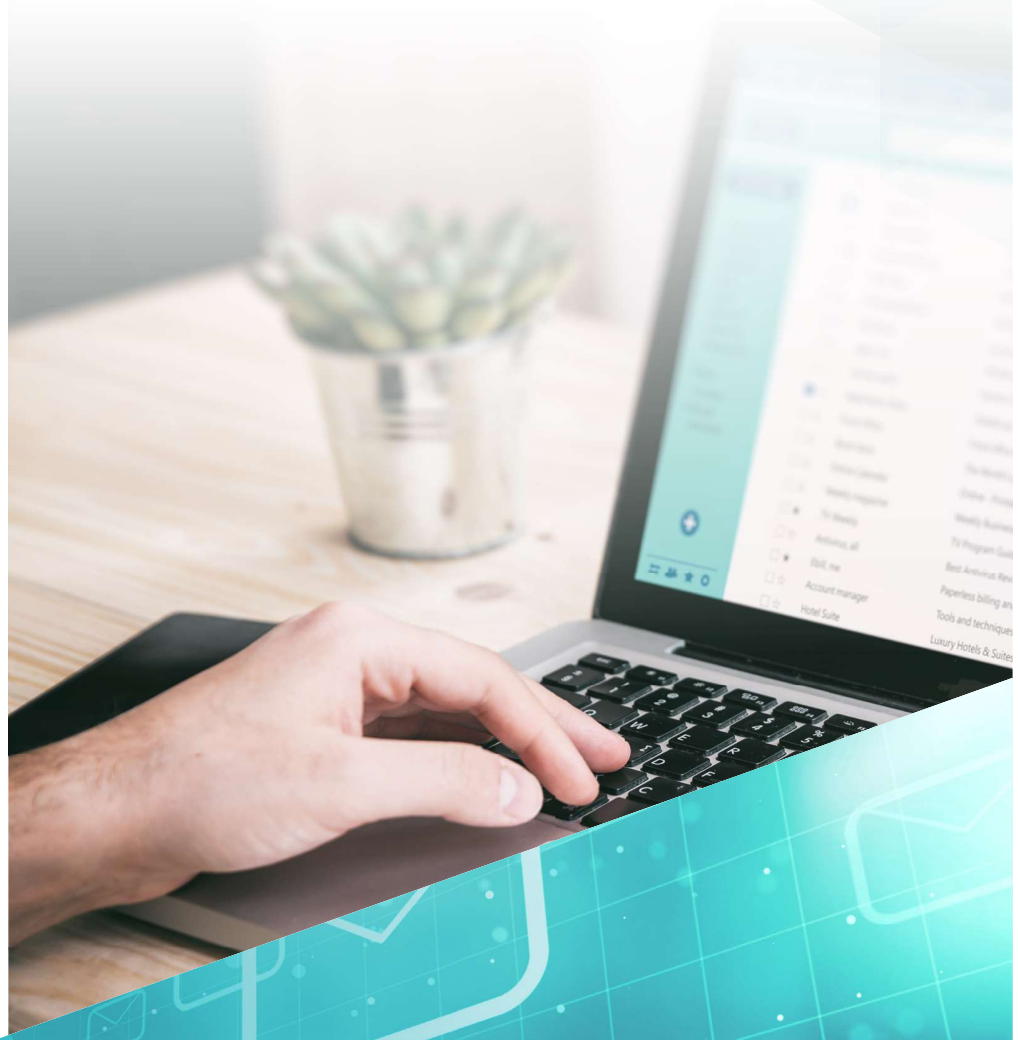
同業他社と比較してどのような評価を受けているかを知りたい組織は多いと思いますが、有効な結果を出すためには、科学的で実績のある方法と組み合わされた確かなデータが必要です。どの企業も、「自社と同じような他の企業とどのように比較するか」という点において大きな疑問を抱いていることでしょう。2023年度業界別フィッシングベンチマーキング調査は、この疑問への解答またはその対策を示唆するために、19業種を横断した3,210万回を超える模擬フィッシング攻撃テストにおいて、35,681社の中から1,250万人を超えるユーザーのデータ統計を分析したものです。

今年の調査の手法

まず、すべての調査対象を業界と規模によって分類しました。それぞれの調査対象のPPPを算出するために、KnowBe4プラットフォームを使用して模擬フィッシング攻撃テストキャンペーンを実施し、この間に誤ってフィッシングメールのリンクをクリックしたり、偽装添付ファイルを開封したりした従業員の数を測定しました。

2023年のレポートでも、これまでと同様に次の3つのベンチマークフェーズを検討しています。

- **フェーズ1:** ベースラインベンチマーキング (トレーニング開始前の事前テスト)
- **フェーズ2:** トレーニング開始後90日までのベンチマーキング
- **フェーズ3:** トレーニング開始1年後からそれ以降のベンチマーキング



トレーニングの効果分析

セキュリティ意識向上トレーニングの効果を判定するために、KnowBe4ではフェーズ1からフェーズ3の各フェーズにおいて次の質問への回答を集計し、トレーニングの成果を測定しました。

フェーズ1

トレーニングせずに模擬フィッシングメールを送信した場合の初期のPPP結果はどうでしたか？

このベースライン ベンチマーキングによって、トレーニング前に従業員がどれくらいフィッシング攻撃被害を受けやすかったかを確認できます。測定対象の個々のユーザーに対して、トレーニング前に模擬フィッシングメールを送信し、これに誤って反応したかを測定します。

フェーズ2

トレーニングを完了し、トレーニング後の90日以内に模擬フィッシング攻撃テストを受けた後のPPP結果はどうでしたか？

最初のトレーニング完了後の90日以内に行われた模擬フィッシングテストの成果をこの質問で判定します。

フェーズ3

その後の継続的なトレーニングと月一回の模擬フィッシング攻撃テストを行った後のPPP結果はどうでしたか？

この質問によって、12か月以上の継続的なトレーニングおよび模擬フィッシング攻撃テストを行った後のセキュリティ意識向上スキルを測定することができます。1年以上前にトレーニングを完了したユーザーを対象に、直近のフィッシング詐欺テストの成績を測定します。