

データが実証する
セキュリティ意識
向上トレーニングと
模擬フィッシング
演習の価値



Roger A. Grimes &
Dr. Martin J. Kraemer
共著

目次

はじめに	2
調査結果のポイント	2
KnowBe4業界別フィッシングベンチマーキングレポート	3
調査データについての詳細	4
頻繁にPSTを実施するかが重要である	5
継続的にトレーニングを実施することが重要である	6
Inside Man: Netflix品質の動画トレーニングの効果	7
KnowBe4内でのAIの使用	8
トレーニングとPSTに関してKnowBe4が推奨するベストプラクティス.....	9
本調査での除外事項	11

はじめに

KnowBe4をご検討中のお客様からよく寄せられる質問に、セキュリティ意識向上トレーニングと模擬フィッシング演習がサイバーセキュリティリスクの低減にどれくらい効果があるかを具体的に示すことができますか？というものがあります。当社はこれを示すため、KnowBe4を利用して、累計約500万回のフィッシング演習(Phishing Security Test:PST)を受け、年に一回以上の意識向上トレーニングを受けたことのある、約3,300万人のユニークユーザーからなる世界中の60,000社以上の企業、団体のこれまでのデータを分析、調査しました。この調査はこの種のものとしては、対象の顧客数と演習の回数ともに最大クラスのものであります。

調査結果のポイント

「データは嘘をつかない」。調査結果の主要なポイントは以下の通りです。

- フィッシング演習(以降PST)を頻繁に実施しているグループは、そうでないグループに比べて、フィッシングメールを検知する能力が明らかに高い。
- PSTを、より頻繁に実施したグループは、より良いフィッシングテスト結果を出した。PSTの実施回数は多ければ多いほど良い。
- PSTの頻度が高いグループほど、テスト結果は良かった。PSTの回数が多ければ多いほど良かった。
- 毎週PSTを実施したグループは、四半期に1回以下のPSTしか実施しなかったグループに比べ、リスク低減効果が2.74倍高い。
- トレーニング期間が長ければ長いほど、フィッシングテスト結果は良い。
- セキュリティ意識向上トレーニングとフィッシング演習の両方を頻繁に実施したグループが最も良い結果を出した。

これらの事実を示すデータの詳細は後述します。ちなみに、本調査は、業種、地域、受講トレーニングの種類(期間、難易度、コンテンツの種類、提供方法など)に関係なく、結果をまとめています。

以下は、セキュリティ意識向上トレーニングとフィッシング・セキュリティ・テスト(PST)の有効性を裏付ける代表的なデータです。この表は、トレーニング(縦軸)および模擬フィッシング演習(横軸)の頻度と、Phish-prone™ Percentage (フィッシングリンクをクリックしやすい従業員の割合 以下PPP)の平均改善率を示しています。

平均改善率は、最初のPST実施時のフィッシングリンクをクリックしやすい従業員の割合(PPP)と、PSTおよびトレーニングの実施頻度別に、その後記録されたPPPを比較して割り出したものです。数値が高いほど改善率が高いことを示します。

トレーニング頻度 ／PST頻度	毎月1回以上	毎四半期1回	毎年1回	毎年1回以下	総計
毎週1回以上	96%	84%	88%	89%	89.25%
2週1回	83%	77%	80%	82%	80.33%
毎月1回	74%	71%	74%	74%	73.39%
2か月1回	50%	60%	63%	72%	65.31%
毎四半期1回	53%	55%	52%	53%	53.00%
毎四半期1回以下	35%	35%	39%	41%	38.95%

表 1: 平均PST頻度と平均トレーニング頻度別のPPPの平均改善率(5年以上のKnowBe4ユーザー対象)

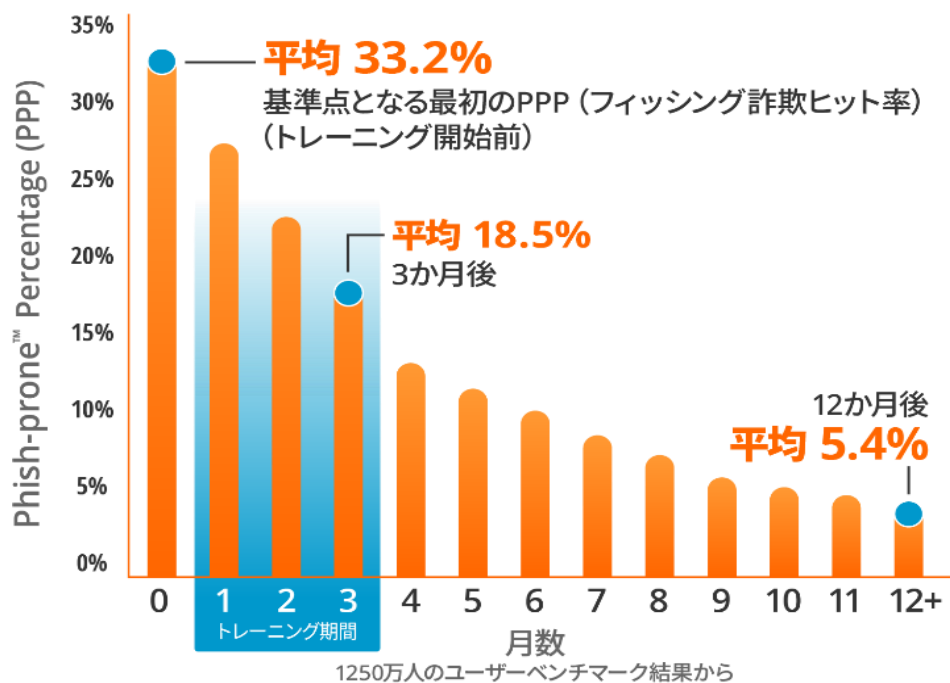
事実：フィッシング演習(PST)を頻繁に実施しているグループは、そうでないグループに比べて、フィッシングメールを検知する能力が明らかに高い

例えば、月1回以上のセキュリティ意識向上トレーニングと週1回以上のフィッシングシミュレーションテストの両方を受けたユーザーは、PPPが96%改善し、トレーニングやテストを頻繁に受けていない他のグループに比べて良い結果となっていました。若干の例外はあるものの、どのグループも、トレーニングやテストを多く行ったグループの方が、トレーニングやテストを頻繁に行わなかったグループよりも、良い結果を出しています。興味深いことに、本データによると、より頻繁なフィッシングテストによる影響は、より頻繁なトレーニングによる影響よりも大きい結果となっています。

本データからの事実として、ベストな効果を得るには、従業員全員がセキュリティ意識向上トレーニングの一環として、フィッシングテストをより頻繁に実施すべきであることが判明しました

KnowBe4業界別フィッシングベンチマーキングレポート

本ベンチマーキングレポート結果は、KnowBe4のお客様での改善結果から予測できるものであり、この成果は驚くべきものではありません。これまでのKnowBe4のお客様のデータでは、継続的な頻繁なフィッシングテストを続けた結果、時間の経過とともにPPPは改善され、フィッシングテストで誤ってクリックしたり反応したりするユーザーの数が減少することが以前から示されていました。セキュリティトレーニングや模擬フィッシング演習を実施したことがない組織では、フィッシングテスト(または実際のフィッシングメール)にクリックしたり、反応したりしてしまう可能性のあるユーザーの割合(KnowBe4ではこれをPhish-prone Percentage (PPP)として観測しています)が30%以上になります。トレーニングを継続的に実施し、頻繁にフィッシングの模擬演習を行うと、多くの場合、PPPは1年以内に5%程度まで低下します。(2023年の調査ベンチマーキング結果を参照)



出典：2023年のKnowBe4 業界別フィッシングベンチマーキングレポート

注：PPPの初期値は、評価対象の全ユーザーに基づいて算出されています。これらのユーザーは、評価前にKnowBe4 コンソールを使ったトレーニングをいっさい受けていません。その後の各期間の数値は、全ユーザーのうちKnowBe4 コンソールを使ったトレーニングを受けたユーザーのPPPを反映しています。

PPPが82%低下した実績は、KnowBe4の新規のお客様の平均値であり、この傾向はここ数年一貫して変わりはありません。また、PPPが5%を下回った実績を実現したお客様も多数存在しています。セキュリティ意識向上トレーニングとフィッシングセキュリティテスト(PST)の組み合わせがサイバーセキュリティ・リスクの低減に極めて有効であることを実証しています。これこそが、KnowBe4が世界最大かつ最も急成長しているサイバーセキュリティ企業の1つである理由です。

模擬フィッシング演習はセキュリティ意識向上トレーニングの 欠かせない部分である

毎年、KnowBe4は業界別フィッシングベンチマーキングレポートをリリースしています。2023年度版業界別フィッシングベンチマーキングレポートをご希望の方は、次のURLからダウンロードしてください。

https://www.knowbe4.com/hubfs/2023-Phishing-by-Industry-Benchmarking-Report-Research_JA.pdf



本年度のレポートでは、3210万回以上の模擬フィッシング訓練／フィッシング攻撃テストの結果を集計し、35,681社における950万人以上のユーザーのデータセットを分析しています。上記のとおり、トレーニング開始後の最初の3か月で、一貫して、大きな改善が見られています。これについての詳細は、[日本語版業界別フィッシングベンチマーキングレポート](#)を参照してください。

2023年度版業界別フィッシングベンチマーキングレポートのデータは、2011年3月3日から2023年1月1日までにお客様が実施したトレーニングおよびPSTキャンペーンを匿名で収集・分析したものです。

調査データについての詳細

本ホワイトペーパーのデータは、過去10年間に収集された匿名化されたデータに基づいていますが、KnowBe4は設立当初から13年以上にわたってお客様とエンドユーザーに関するデータをKnowBe4のサービス向上のために蓄積しています。本データは、世界中の6万社を超えるKnowBe4顧客ベースから収集した3200万人以上のユーザーによる3200万回以上の模擬フィッシングテストの結果を匿名で収集・分析したものです。

このセクションでは、上記の調査結果の注目ポイントの背後にある生データを表示します。始める前に、データ指標である用語について定義します。

- **PPP=Phish-prone Percentage (フィッシング詐欺ヒット率)**: フィッシングセキュリティテスト(PST)に誤って反応したユーザーの割合。通常はメールを介して送信されますが、SMS、音声通話、USBなど他のメディアタイプを使って測定されることもあります。
- **フィッシングセキュリティテスト (PST)**: 模擬フィッシングテストは、受信者がフィッシング・メッセージを見破る能力をテストするためだけに使用されます。模擬フィッシング・メッセージを開くことは、必ずしも"失敗"ではありませんが、このメッセージに埋め込まれたリンクをクリックしたり、要求されたアクション(例えば、ログイン認証情報の提供、ファイルのダウンロード、プログラムの実行など)を実行したりすることはテストの不合格と判定されます。
- **トレーニング**: 割り当てられた受講セッション。ほとんどのトレーニング(セッション受講)は、インタラクティブなトレーニングセッションおよび/またはライブアクション動画を介して行われます。また、メールニュースやポスターによる注意喚起などもトレーニングには含まれることもあります。KnowBe4はPST(模擬フィッシング演習)もSATトレーニングの一環とみなしていますが、本ホワイトペーパーのデータでは、トレーニング(セッション受講)とPST(模擬フィッシング演習)は別物として集計されています。
- **集計対象**: データ集計の集計対象。
- **頻度**: トレーニングまたはPSTがどれくらいの頻度で行われたかを示します。
 - **>= 毎週PST**: PSTを毎週1回または毎週1回以上実施
 - **隔週PST**: PSTを2週に1回実施
 - **毎月PST**: PSTを毎月1回実施
 - **毎四半期PST**: PSTを毎四半期1回実施
 - **<毎四半期PST**: PSTを毎四半期に1回以下実施
 - **全サンプル**: 実施したすべてのPST
- **利用年数**: KnowBe4を利用している年数 最大13年

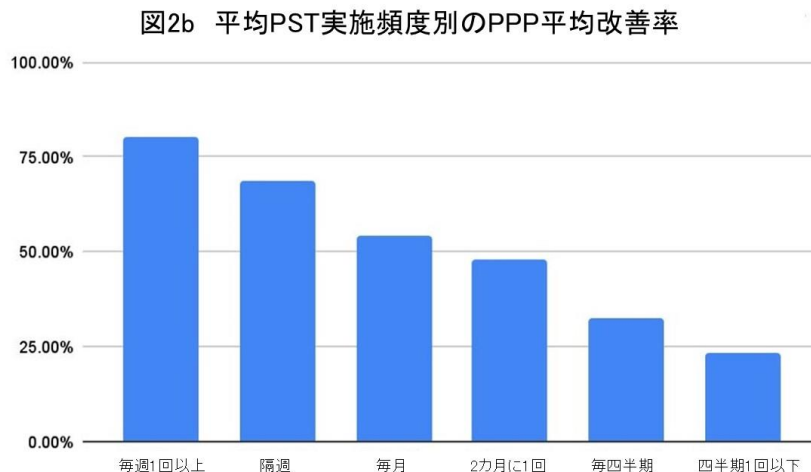
頻繁にPSTを実施するかが重要である

事実: PSTを、より頻繁に実施したグループは、より良いフィッシングテスト結果を出した。PSTの実施回数は多ければ多いほど良い

このデータは、より頻繁に模擬フィッシング・キャンペーンを実施しているユーザーの効果が高くなることを示しています。この事実は、次のデータから導き出されたものです。

平均PST実施頻度	初回のPST		最後のPST		実施通年PST総計			サンプル数
	失敗の回数	PPP%	失敗の回数	PPP%	失敗の回数	受信数	PPP%	
≥ 毎週PST	22,123	9.04	4,997	2.04	560,117	31,253,102	1.79	244,841
隔週PST	216,185	10.94	94,823	4.80	3,257,015	95,377,935	3.41	1,976,981
毎月PST	711,892	11.96	363,578	6.11	6,676,093	121,771,620	5.48	5,953,628
2カ月1回PST	1,179,605	12.26	642,506	6.68	10,446,663	163,520,367	6.39	9,620,102
毎四半期PST	640,906	13.26	431,178	8.92	3,425,455	38,389,891	8.92	4,834,048
<四半期PST	1,388,454	13.92	1,149,548	11.52	4,654,018	43,548,380	10.69	9,974,508
全サンプル	4,159,165	12.76	2,686,630	8.24	29,019,361	493,871,295	5.88	32,604,108

個々のデータからは一見して改善率が見えてこないと思われます。次の棒グラフをご覧ください。PSTの実施頻度が上がるにつれて、ユーザーの平均PPP改善率が明確に向上していることが分かります。



全グループにおいて、PSTの実施頻度が上がるにつれて、PPPは下降し、改善されています。例えば、実施通年PST(特定のユーザーで実施されたすべてのPST)において、平均ユーザーのPPPは、四半期に1回以下のPSTでは10.69%ですが、四半期に1回でのPSTでは8.92%、2カ月に1回のPSTでは6.39%、以降実施回数が増えるごとに、5.48%、3.41%と低下し、最終的に毎週1回以上のPSTでは1.79%までに改善されます。トレーニングも模擬フィッシング演習(PST)もともに実施していないユーザーのPPPが、ほとんどの組織で通常30%以上であることを考えれば、これは驚くべきリスクの減少です。毎週1回あるいはそれ以上の頻度でPSTを実施すれば、ユーザーの「クリック率」を2%以下にまで下げることができます。これは、KnowBe4を使用するだけで、リスクを80%削減できるという驚くべき成果です！

事実:PSTの頻度が高いグループほど、テスト結果は良かった。PSTの回数が多いほど良いほど良かった

この事実は、同じデータから導き出されています。PSTの回数が多いほど、PPP率は低くなっています。最初の表が示すように、週1回以上のPSTを実施したグループの改善率は96%であり、四半期に1回未満のPSTを実施したグループの改善率は35%にとどまっています。これは、週1回以上のPSTを実施したグループは、四半期に1回以下のグループよりもフィッシング・リスクを2.74倍減少させたことを意味しています。より頻繁にPSTを実施するメリットが示されています。

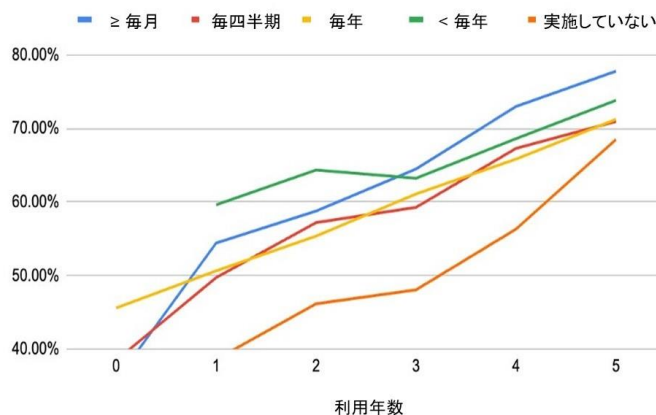
継続的にトレーニングを実施することが重要である

事実:トレーニング期間が長ければ長いほど、フィッシングテスト結果は良い

データによると、KnowBe4のトレーニングを利用したことのあるユーザーは、KnowBe4の利用期間が長いほど、またトレーニングを受ける頻度が高いほど、より良いパフォーマンス、つまり、模擬フィッシングテストのテスト結果が良くなっています。次の表は、利用年数によるPPPの改善率を示しています。

利用年数は、ユーザーがこれまでKnowBe4を何年利用してきたかを示します。

図1c 平均トレーニング頻度と利用年数別の平均PPP改善率



Inside Man: Netflix品質の動画トレーニングの効果



“The Inside Man”は、KnowBe4のNetflix品質のトレーニングビデオシリーズです。これらの実写ビデオは高画質で、キャリアのある俳優を起用し、プロのクルーとともに実際のセットで撮影されています。Netflixが提供しているテレビシリーズに限りなく近いものなのです。競合他社には、このシリーズに近いトレーニングコンテンツはありません。すべてのユーザーから高い評価を受けており、次のシーズンはいつ出るのかというリクエストが頻繁に届いています。

想像できますか？従業員から「もっと受けない！」と言われる サイバーセキュリティトレーニングを！

「The Inside Man」第5弾「シーズン5」の日本語吹替版については、以下のURLをアクセスしてください。

<https://www.knowbe4.jp/press/annouce-jp-vesion-of-inside-man-s5>

次に、“The Inside Man”を少なくとも1エピソード以上視聴したユーザーのデータを示します。視聴前の平均的な視聴者のPPPは13%-17%に対して、少なくとも1エピソードを視聴した後、視聴者のPPPは5%～8%に下がり、視聴エピソード数が増えるにつれてPPP値はさらに下がります。

他のトレーニングに加えてエピソードを視聴したユーザー							
	視聴エピソード の総数	エピソード 視聴前	1エピソード 以上視聴後	10エピソード 以上視聴後	20エピソード 以上視聴後	50エピソード 以上視聴後	サンプル数
PPP値	1-9	16.85	7.72	--	--	--	6,665,967
	10-19	14.87	7.57	6.46	--	--	1,139,830
	20-49	14.15	6.66	6.15	5.50	--	640,670
	50以上	13.10	5.51	5.21	5.01	4.43	133,274
PPP変化率 (エピソード 視聴前との 対比)	1-9	--	-9.13	--	--	--	6,665,967
	10-19	--	-7.31	-8.41	--	--	1,139,830
	20-49	--	-7.49	-8.00	-8.65	--	640,670
	50以上	--	7.59	-7.89	-8.09	-8.67	133,274

次の表に示すように、KnowBe4のトレーニングとして「The Inside Man」しか視聴していないユーザーにおいても明らかな効果が出ています。1エピソードを視聴しただけで、視聴前のPPPは8%～11%から5%～7%へと下がり、50エピソード以上視聴した場合は最終的に4%まで下がっています。

KnowBe4のトレーニングとして「The Inside Man」しか 視聴していないユーザー							
	視聴エピソード の総数	エピソード 視聴前	1エピソード 以上視聴後	10エピソード 以上視聴後	20エピソード 以上視聴後	50エピソード 以上視聴後	サンプル数
PPP値	1-9	10.76	6.89	--	--	--	387,544
	10-19	10.25	6.72	6.45	--	--	191,072
	20-49	9.27	5.42	5.23	5.23	--	174,192
	50以上	7.97	4.86	4.99	5.11	3.96	4,310
PPP変化率 (エピソード 視聴前との 対比)	1-9	--	-3.87	--	--	--	387,544
	10-19	--	-3.53	-3.80	--	--	191,072
	20-49	--	-3.85	-4.03	-4.04	--	174,192
	50以上	--	-3.11	-2.98	-2.85	-4.01	4,310

「The Inside Man」だけを視聴することはお勧めしませんが(飽きられないように、トレーニングコンテンツやカテゴリを定期的に変更することをお勧めします)、他のトレーニングコンテンツを使用せずに「The Inside Man」のみを視聴した場合でも、PPPが大幅に減少しました。楽しみながら学ぶ効果は非常に高いと言えるでしょう。

注:ごく一部のお客様は、弊社のトレーニングモジュールを自社独自のeラーニング管理システムにインポートすることで、弊社のプラットフォーム外で弊社のコンテンツを利用しています。そのため、KnowBe4のデータでは「The Inside Man」を視聴しただけと表示されていても、KnowBe4では追跡されていないトレーニングモジュールを修了している可能性があります。

KnowBe4内でのAIの使用

KnowBe4を検討しているお客様からよく寄せられるもう1つの質問は、「人工知能(AI)がフィッシング対策を改善することができるか?」です。答えは、明確に「はい」です。KnowBe4は、2017年に導入した「AIDA™ (Artificial Intelligence Driven Agent)」を始めとして、様々な形態でAIを使用しています。AIDAはAIを使用して、どの模擬フィッシングテンプレートをユーザーに送信すべきかを決定しています。KnowBe4のフィッシングテンプレートでは、実際に発生しているフィッシングメールを参考にして、文面、内容やレイアウトを逐次更新しています。

お客様の管理者は、希望に応じて、ユーザーをテストするために独自のフィッシングテンプレートを選択(または作成)したり、完全にランダムにテンプレートを選択させたり、AIDAにテンプレートを選択させたりすることができます。

KnowBe4のAIドリブンのフィッシング

AIDAを使用して、テンプレートを選択させると、結果としては、なんと、フィッシングに引っかかる確率は高くなります。これは、皆さんの意に反するではないかと思いますが、事実です。では、何故でしょうか。その理由は、次の通りです。

KnowBe4では、46,000種以上の異なるフィッシングテンプレートが使用された約6億5,000万回のフィッシングテストに対して、1)管理者が選択したテンプレート、2)完全なランダムに選択されたテンプレート、3)AIDAが選択したテンプレート別にPPP失敗率を分析しました。結果は、AIDAが選択したテンプレートは他の2つのテン

プレート(2.7%)に対して高いユーザーPPP失敗率(7.1%)となりました。

前述の通り、AIDAは機械学習のテクノロジーを活用することで、これまでのユーザーのトレーニング受講およびフィッシングメール演習の履歴データをベースに、最適なフィッシングテンプレートを自動選択して、ユーザー毎にパーソナライズされたフィッシング演習キャンペーンを自動生成しています。これにより、ユーザーごとにユニークなフィッシングテンプレートの動的な選択を自動化することができ、パーソナライズされたキャンペーンを自動作成することで、すべてのユーザーが個々のレベルに合わせた模擬フィッシング演習を受けることができます。

フィッシングテンプレートは、難易度が5段階に分かれています。AIDAは、パーソナライズされた適切なテンプレートを自動的に選択し、指定があれば次の難易度を選択していきます。そのために、AIDAの初期PPP失敗率が高くなります。しかしながら、時間の経過に伴い、ユーザーの攻撃を見付け出す能力が継続的に高まり、セキュリティカルチャーの強化につながることが実証されています。

また、KnowBe4では、**新製品「PhishER Plus」**を含む他のいくつかの機能でAIを使用し、フィッシングやその他の悪意のある攻撃の検知を支援しています。サイバー攻撃者がAIを悪用してサイバー攻撃を仕掛けているというAIの影部分が報道されていると思いますが、KnowBe4を含む多くのITプレイヤーはAIを長年使って、ユーザーエクスペリエンスを向上させる一方で、サイバーセキュリティ・リスクを軽減させています。

注: 今回のデータには、従来の手動フィッシング・キャンペーンとAIDAを利用した自動フィッシング・キャンペーンの両方で使用された19,475種のテンプレートが含まれています。601,468,868件の収集データでは、手動選択されたテンプレートが利用されていましたが、48,299,578件の収集データではAIDAで自動選択されたテンプレートが利用されました。

AIDAについては、次の日本語プレスリリースを参照してください。

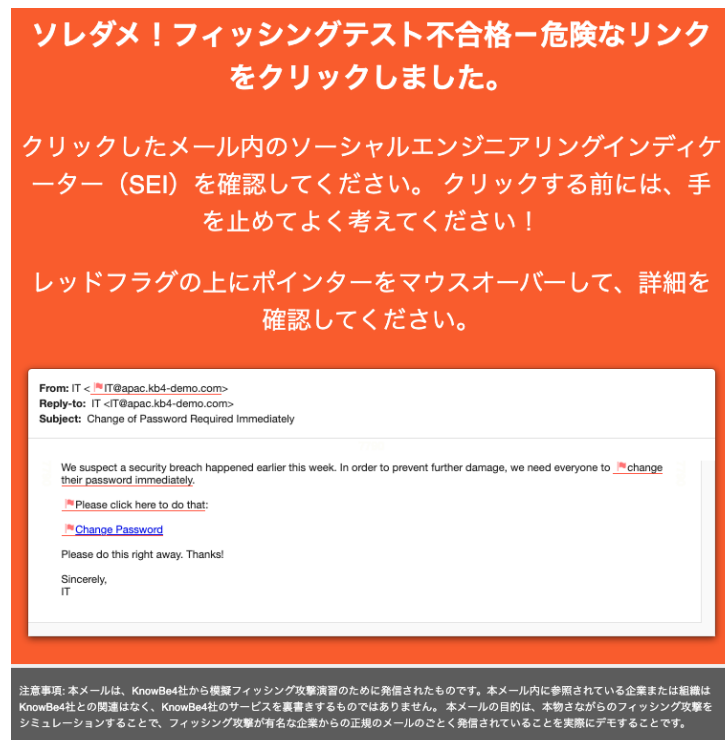
<https://www.knowbe4.jp/press/knowbe4-launches-artificial-intelligence-driven-phishing-feature>

トレーニングとPSTに関してKnowBe4が推奨するベストプラクティス

KnowBe4は、測定可能なサイバーセキュリティ・リスク低減を短時間でお届けする方法論を提示しています。この方法論では、次のベストプラクティスを推奨しています。

- セキュリティ意識向上トレーニングを推進するには、上級管理職(CEO、CFO、CIO、CSO など)からのサポート(エグゼクティブスポンサー)が必須です。上級管理職もセキュリティ意識向上トレーニングを受講し、PSTに参加し、自ら、組織のためになるものであると周知してください。
- 新入社員には、入社時に詳細で幅広いセキュリティ意識向上トレーニングを実施してください。このトレーニングは、一般的なソーシャルエンジニアリングとハッキングのテーマで構成され、最初のセッションとしては30～60分の研修にすることが理想的です。少なくとも年に1回以上は繰り返す必要があります。
- さらに、全ユーザーを対象に、少なくとも月1回、3～5分程度の短時間の注意喚起を実施してください。そのトピックは、最新の攻撃動向やリスクなどが、理想的です。
- トレーニングの内容としては、単なるプレゼンテーションではなく、ビデオ、クイズ、ゲームなどを駆使した興味を引く様々な形態で実施すべきです。
- PSTは毎月、あるいはそれ以上の頻度で実施すべきです。PSTの実施頻度が高いほど、PPPが改善されます。もちろん、管理者は、PSTの実施頻度が多すぎてユーザーの不満を招かないように注意が必要です。どれぐらいの頻度だと多すぎるのかは、組織によって異なりますので、ユーザーのフィードバックに基づいて実施頻度は柔軟に変更しましょう。

- PSTの演習フィッシングメールに引っかかってしまった人には演習であることを伝えるとともに、気づけたであろうメール中の怪しい項目をその場で指摘してあげることが重要です。



- PSTを実施する場合は、フィッシング演習を実施することを事前に伝えてください。しかし、いつ実施するかは伝えないようにすべきです。
- PSTを実施する場合は、ユーザーごとに異なるテンプレートを使い、異なる時間に配信すべきです。すべてのユーザーに同じフィッシングメールを同じ時間に送らないようにしてください。
- PSTを行うことは前もって管理職に伝えておくべきですが、いつ、どのようなメッセージを送るかは明確にしないことが重要です。
- 昇給、ボーナス、昇進など、困難を招くような内容のPSTは送るべきではありません。ユーザーを怒らせたり、クレームの対象になったりすることは避けましょう。PSTに適切な有効な題材はたくさんあります。
- フィッシングの疑いがあるメールを報告するための簡単な方法を導入し、その使用方法を端的に説明しましょう。KnowBe4では、無料のフィッシングアラートボタン(PAB)を用意しています。Outlookボタンと統合して利用することをお勧めします。<https://www.knowbe4.jp/ja/free-phish-alert>
- 複数のPSTに不合格となったユーザーには、是正トレーニングを指示してください。是正トレーニングに加えて、1対1のコーチングを与えるべき場合もあります。一定期間内(例えば1年間)にPSTの不合格回数が増えた場合は、追加トレーニングを受けさせるべきですが、ペナルティを課すべきではありません。目標は、すべてのユーザーがヒューマンファイアウォールの一部となり、組織の資産となるようにすることです。誰もがフィッシング攻撃を認識できるようになることです。
- 全社に展開する場合、TeamsやSlackを通じてフィードバックチャネルを設定することができます。PSTに従業員が引っかかったときには、的確なアドバイスを与え、連帯して組織一丸となってサイバー攻撃に立ち向かう姿勢が重要です。

本調査での除外事項

KnowBe4は、本調査分析では、トレーニング、PST、PPPに関して、約5億件の個別のユーザーレコードを調べました。しかし、本調査の対象には、KnowBe4が蓄積している膨大なデータベースにあるすべてのデータが含まれているわけではありません。これは、データの共有を拒否するお客様やシステムの使用期間が1日未満の新規ユーザーなどのデータを除外したり、データに偏りが生じる可能性のあるケースを取り除いたりしたためです。使用したデータを明確化することで、どのような種類のデータセットがデータに含まれなかったかを明記します。使用したデータは、次の通りです。

本調査の集計に使用したデータセットに含まれるもの：

- 少なくとも25人のユーザーに対して実施されたPSTキャンペーン（データセットが小さいと、結果が大幅に歪む可能性が高い）
- 実施PSTキャンペーンのうちで、管理者によって "hidden" とマークされていないもの
- 実施PSTキャンペーンで、「Scam of the Week」、「Security Hints and Tips of the Week」テンプレートに（テスト用PSTではない）に含まれていないもの
- 少なくとも1日以上KnowBe4を使用しているユーザー
- 管理者によってアーカイブされていない、または停止されていないユーザー
- アクティブかつ有料で、調査分析を許可しているアカウント
- テスト/デモなどのトライアルユーザーでない、有料のアカウント

その他の注意事項は次のとおりです。

- トレーニングの期間、コンテンツの種類、トレーニングコンテンツの品質がPPP値にどのような影響を与えたかは追跡していません。すべてのトレーニングおよびフィッシング演習のデータが、本調査の目的のために総合的に集計されています。しかしながら、コンテンツ品質について言えば、高品質のトレーニングコンテンツとフィッシングコンテンツは、低品質のものよりも、PPPを下げる効果があると推定されます。
- フィッシング演習の難易度（複雑さ、成熟度など）を上げていくことをお客様にお勧めします。初期の難易度の低いテストではユーザーが良いスコアを取りますが、その後、難易度を上げることでユーザーのスコアは下がります。これはフィッシングテストに「合格」することが難しくなるからです。本調査の目的では、難易度に関係なく、すべてのフィッシングテストのデータが総合的に集計されています。

この調査結果をご覧になった方は、フィッシングテストによるフィッシングに引っかかってしまう確率を低くするという結果は得られたが、実際のフィッシング攻撃に対する防御力を強化したという結果は示せていないと思われることでしょう。

- 実際のフィッシング攻撃に対して、当社のお客様と、当社をご利用でないお客様を比較するデータ（このデータはPSTとトレーニングの効果を証明する上で究極のデータと言えますが、当社顧客以外の詳細なデータを持っていません。）の分析を行なっていません。KnowBe4は、こうした比較データを調査していて、データから得られた結果を将来、ホワイトペーパーで発表したいと考えています。

このような注意点はありますが、KnowBe4は、13年以上にわたる約5億件の個人レコードからなる非常に大規模なデータセットが、PSTとトレーニングを利用することでサイバーセキュリティのリスクを大幅に低減できることを強く裏付けていると考えています。さらにポイントとしては、トレーニングとフィッシング訓練を繰り返し実施すればすれほど、サイバーセキュリティのリスクはより低減されていることです。

その他の関連情報



フィッシングセキュリティテスト

あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。



セキュリティプログラムビルダー

あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。



Phish Alertボタン

あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。



無償Email Exposure Checkツール

あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。



無償なりすましドメインテスト

ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



<KnowBe4について>

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスト、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2023年9月現在、6万5千社を超える企業や団体がKnowBe4を採用して、防御の最終ラインとして「人」による防御壁を構築しています。

詳しくは、www.KnowBe4.jp をアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社 〒100-6510 東京都千代田区丸の内1-5-1
新丸の内ビルディング10F EGG 内

Tel: 03-4586-4540 | www.KnowBe4.jp | Email: info@knowbe4.jp

© 2023 KnowBe4, Inc. All rights reserved. 本資料に記載されている他社の製品および会社名は、各社の商標または登録商標です。