yubico

EBOOK

企業全体のIDフィッシングを阻止する方法：強力な認証を展開するためのガイド

モバイル認証だけでは不十分な理由

目次

フィッシング攻撃の進化

1480万ドル

が、2021年のフィッシングの平均年間コストであり、2015年の380万ドルから増加しています[2]

世界中の組織の75%

が2020年にフィッシング攻撃を経験しました[3]

米国企業を標的としたフィッシング攻撃の74%

が成功しました[4]

フィッシング攻撃の96%

はメールで届きます[5]

近年、非常に脆弱なパスワード、ターゲットへのアクセスの容易さ、世界中で拡大するモバイル脅威など、さまざまな要因により、フィッシング攻撃が劇的に増加しています。アンチフィッシング・ワーキング・グループ（Anti-Phishing Working Group、APWG）が発表した調査によると、フィッシング攻撃の数は2020年にほぼ2倍、2021年の第[1]四半期には記録的なレベルになりました。同じ調査では、2021年1月に過去最高の245,771回の攻撃が記録されました。もちろん、フィッシング攻撃の実際の数はこれよりはるかに多い可能性があります。多くの攻撃が検出または報告されないためです。

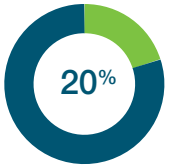
IDフィッシングとは

フィッシングとは、クレジットカード番号やパスワードなどの機密性の高い個人情報を漏らすように人々を誘導する詐欺行為です。フィッシング攻撃者は、信頼できる企業やその他の信頼できる事業体をかたり、正当な通信と思われるテキスト、メール、またはその他の電子通信を送信し、ユーザーをフィッシングウェブサイトに誘導します。これらのサイトは巧妙に作られていて、機密データや個人を特定できる情報を引き出すように設計されています。通常、フィッシング攻撃は、被害者に機密情報を晒させるか、マルウェアをダウンロードさせることを目的としています。

暴露される機密情報 これらのフィッシングメッセージの目的は、被害者をだましてユーザー名とパスワード、またはその他の機密データ（アカウントやシステムの侵害に必要なもの）を漏洩させることです。攻撃者は、信頼できる送信者からのメッセージであるかのように設計された電子メールを送信します。多くの従業員がビジネスアカウントと個人アカウントでパスワードを共用するため、フィッシング攻撃や侵害の成功率が高くなります。

マルウェアのダウンロード 多くのフィッシングメールは通常のスパムと同じように機能しますが、多くの場合、被害者のコンピュータをマルウェアやランサムウェアに感染させるという明確な意図があります。攻撃者は、履歴書が添付された電子メールを毎日受信する人事担当者などの「ソフトターゲット」を頻繁に追跡します。正当な履歴書の代わりに、悪性コードが埋め込まれた添付ファイルを受け取る可能性があります。この種の攻撃は時間がかかりますが、ハッカーの潜在的な報酬はその時間と労力に見合うものです。

2020年に悪意のあるデータ侵害に見舞われた企業の約**5分の1**が、認証情報の紛失または盗難により侵入されました[6]



全従業員のほぼ**20%**がフィッシングメールのリンクをクリックする可能性が高く、そのうち実に**67.5%**がフィッシングのウェブサイトに認証情報を入力します[7]

一般的なフィッシング攻撃

今日のフィッシング攻撃には、一般的な種類があります：

スピアフィッシング対フィッシング

スピアフィッシングは、標準的なフィッシングの標的バージョンです。定期的なフィッシング活動では、できるだけ多くの潜在的被害者に大量に通信します。対照的に、スピアフィッシングは非常に限定的であり、侵害したい特定の組織または特定の個人を狙います。攻撃者は、よりパーソナライズされたフィッシング攻撃により、成功する可能性を高めるために、ターゲットを注意深く調査します。

フィッシングメールは大量かつ非個人的に送信されるため、多くの場合、タイプミス、スペルミス、およびユーザーが悪意を検出できるその他の間違いが含まれています。信頼できるリンクとロゴは、こうした微妙なヒントを隠すのに役立ちますが、それでもエラーはあります。一方、スピアフィッシングメールは信頼できるソースから送信されたものであり、説得力のある詳細が含まれているため、検出がより困難になります。

スピアフィッシング

特定の企業または個人をダイレクトに狙ったフィッシングは、スピアフィッシングと呼ばれます。[8] ネットで広く拡散される一般的なフィッシングとは異なり、スピアフィッシングの攻撃者は、ターゲットの個人情報を収集して活用し、正当に見えるようにすることで、成功の可能性を高めます。たとえば、攻撃者はスピアフィッシングを使用して、信頼できる同僚や他のユーザーになりすまし、従業員をだまして財務データやその他の機密情報にアクセスする可能性があります。

ホエールフィッシング

ホエールフィッシング、トラップフィッシング、または単にホエーリングは、上級管理職など注目度の高いターゲットを狙う一種のスピアフィッシング攻撃です。ホエーリングとスピアフィッシングの違いは、その企業での被害者の役割です。スピアフィッシングは通常、特定の低職位の従業員を追跡しますが、ホエーリングは組織内の上位の個人のみを対象とします。

キャットフィッシング（Catphishing）とキャットフィッシング（Catfishing）

キャットフィッシング（Catphishing）の攻撃者は、人のリソースや情報にアクセスするため、または被害者に強制的に何かをさせるために、オンラインで誰か（何か）になりすまします。キャットフィッシング（Catfishing）は、他と関連していますが特にロマンチックまたは性的な概念であり、フィッシング攻撃者はSNSのアカウントを作成し、リソースにアクセスまたは制御するために、ソーシャルな関係へと被害者を誘い込みます。

ビジネスメールのセキュリティ侵害に対するフィッシングのコストが高い

フィッシング攻撃の劇的な増加は憂慮すべきことですが、企業組織への侵害における高度化と成功レベルも同様です。たとえば、ビジネスメール侵害（Business Email Compromise、BEC）詐欺は、BEC攻撃の平均電信送金要求が2020年第3四半期の48,000ドルから2021年第1四半期に85,000ドルに増加しており、検出が困難になると共に金額が上がっています。[9]

一部のBEC攻撃は、貴重な企業データにアクセスするために上級管理職になりすますことを専門としています。たとえば、あるタイプの詐欺では、攻撃者は幹部を装って、経理部門からの最新の売掛管理報告書などの内部財務文書へのアクセスを要求します。売掛管理報告書には、すべての未払いの顧客アカウント、および顧客の連絡先名とメールアドレスが一覧表示されます。この情報を使用して、詐欺師は被害者のすべての顧客に連絡し、攻撃者が管理する新しい銀行口座に延滞した請求額を支払うように指示します。[10]

クローンフィッシング

クローンフィッシング攻撃は、リンクや添付ファイルが含まれるような正当なメールの内容をコピーします。クローンフィッシングは元のメールを盗み、元の送信者から送信されたように見える悪意のあるバージョンに置き換えます。

ボイスフィッシング/ビッシング

一部のフィッシング詐欺は、政府機関や銀行などの信頼できる送信者からのものであると主張する音声メッセージを送信します。これらのメッセージは、問題を解決したり機密情報を提供したりするために、ボイスオーバーIP（voice over IP、VoIP）サービスを使用して偽の番号に電話をかけるように被害者に指示します。同様に、ビッシングまたはボイスフィッシングは、書面のメッセージを飛び越え、この種のVoIPシステムと偽の発信者IDデータを使用して、信頼できる組織を偽装し、機密データを引き出します。

SMSフィッシング/スミッシング

SMSフィッシングまたはスミッシングは、悪意のあるリンク、携帯電話番号、またはその他のエサをSMS経由で配信します。モバイルブラウザの性質上、URLが完全に表示されない場合があるため、スミッシングの検出は困難です。さらに、スミッシングメッセージは、他の自動メッセージと同様に、予期しない形式または奇妙な形式で届くことがよくあります。

攻撃方法（スピアフィッシング、ホエールフィッシング、スミッシング、ビッシング）に関係なく、その全体的な目標は、被害者をだまして、企業の認証情報、金融口座やその他の口座へのアクセス、個人情報などの貴重な情報を出させることです。[11]問題は、ハッカーが収集できる情報が多ければ多いほど、同僚、金融サービス担当者、会社の幹部、さらには家族などの信頼できる実体になりすますことが容易になることです。

COVID-19はすでに拡大しているフィッシングの流行を助長

> すべてのユーザートレーニングとパスワード制限が実施されているとしても、今日の重要システムへのアクセスを保護するには、ユーザー名とパスワードだけでは不十分です。悪意のある攻撃者は、パスワードスプレーまたはソーシャルエンジニアリングを使用してアクセスできます
>
> **ミッションビエホ市 ITディレクター Jackie Alexander[12]**

COVID-19のパンデミックが始まって間もなく、従業員はオフィス作業から自宅作業に一斉にシフトしました。多くの場合、これらのユーザーは、家族用のノートPCや配偶者のタブレットなどの個人用ネットワークやデバイスからビジネスアプリやデータにアクセスしていました。これらのパスワード保護は、弱い傾向にあります。安全でない個人用デバイスやアプリに加えて、パンデミックに起因する恐怖と不確実性は、フィッシング詐欺が繁栄するための理想的な条件を生み出しました。COVID-19フィッシングの脅威は非常に蔓延しているため、連邦取引委員会などの多くのセキュリティ組織は、インターネットベースの詐欺の認識を高めるために、定期的に警告を発しています。[13]

2021年の後半以降、少なくともパートタイムで自宅で働く人々の割合は、コロナウイルス発生前の16.4%と比較して、2倍の34.4%になると予想されています。[14] 組織とそのユーザーの両方でより多くの警戒が必要となるこれら劇的な労働力の変化にもかかわらず、多くのセキュリティ問題（特に会社のアプリへのパスワードベースの認証）が依然として残っています。企業のアプリケーションとデータを安全に保つには、従業員のセキュリティ意識とトレーニングだけでなく、企業全体をIDフィッシング攻撃から保護するための強力でフィッシング耐性のある認証も必要です。

「2021年データ漏えいのコスト報告」によると、データ漏えいコストは2020年～2021年で386万ドルから424万ドルに10%増加しました。また、リモートワークが要因ではなかった場合と比較して、リモートワークが侵害の原因となった場合は107万ドルのコスト差があります。これはCOVID-19によって上昇しました。さらに、従業員の50%以上がリモートで作業している組織は、50%以下がリモートで作業している組織よりも、侵害を特定して封じ込めるのに58日長くかかりました。報告ではまた、最初の攻撃ベクトルとしてのフィッシングの平均総コストが2番目に高い465万ドルであり、悪意のある内部関係者（461万ドル）、ソーシャルエンジニアリング（447万ドル）、侵害された認証情報（437万ドル）がそれに続くと述べています。[15]

最新のフィッシング対モバイルベースの認証

モバイル認証だけでは不十分な理由

> ユーザー名とパスワードだけよりも、どのような形式であれMFAが優れていますが、ほとんどのMFAはフィッシング詐欺に遭う可能性があります。すべての従業員がフィッシングされないために、より強力な認証が必要であることに気付くのにそれほど時間はかかりませんでした。
>
> **Datadog IT担当シニアディレクター Daniel Jacobson[16]**

すべてのタイプの多要素認証（MFA）が、最新のフィッシング攻撃を防止する役割を果たしているわけではありません。ユーザー名やパスワードと同様に、SMS、ワンタイムパスコード（OTP）、プッシュ通知などのモバイルベースの認証も、マルウェア、SIMスワッピング、中間者攻撃（MiTM）攻撃によって侵害される可能性のある「共有シークレット」に依存しています。2018年、攻撃者はクラウド上のReddit従業員アカウントと、SMSベースの2要素認証で設定されたソースコード・ホスティング・プロバイダーを侵害しました。[17]

以下は、一般的に使用されるモバイルベースの認証フォームであり、それぞれにフィッシングに関連する長所と短所があります。

テキストまたは通話によるOTPまたはSMS

今日、世界中で50億人以上が携帯電話を所有しているため、SMSを介したOTPがMFAの一般的な方法となっています。[18] ただし、SMSネットワークと電話は、民間企業、政府、犯罪組織、さらには高度なハッカーによっても悪用される可能性があります。また、番号ポーティング詐欺やプレテキスト/ビッシングに対しても脆弱です。

プッシュ通知ベースのアプリ

プッシュ通知ベースのアプリは、ユーザーにコンテキストを提供するため、コードを入力して情報を開示するのではなく、承認ボタンまたは拒否ボタンをタッチしてログインするかどうかを決定できます。

ただし、フィッシング攻撃者は、ユーザーのデバイスに類似したISPでボットを使用できます。ユーザーが承認メッセージを注意深く読まないと、セキュリティ侵害が発生する可能性があります。

プッシュ通知ベースのOTPコード

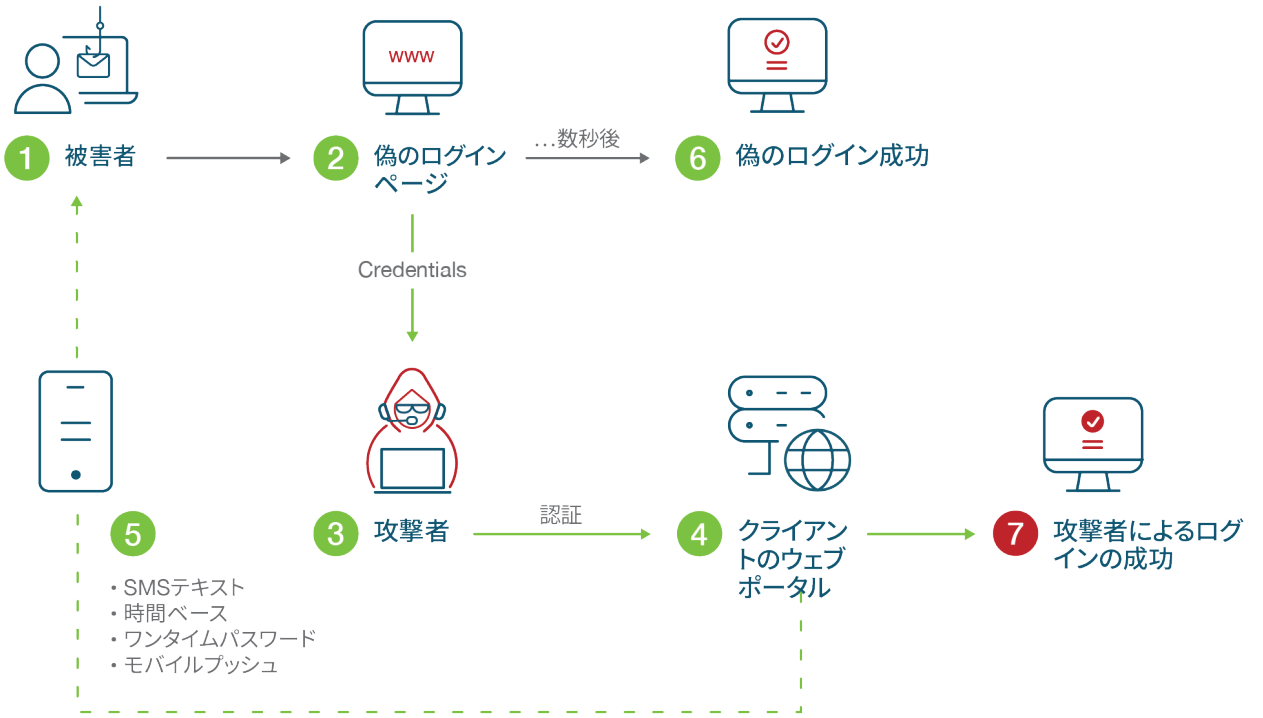
プッシュ通知を介したOTPは、正しく実装されている場合、ハッカーが傍受するのは困難ですが、すべてのOTP実装と同様に、フィッシングはユーザーにコードの開示を促す場合があります。

OTPアプリ

OTPアプリは、通常、ハードウェアトークンまたはQRコードに秘密の「シード」を埋め込みます。これらのシードは、現在時刻またはカウンターと組み合わされて、シードでのみ予測できるコードを生成します。

OTPコードを検証するには、安全性の高いサーバーにシークレットシードが存在する必要があります。また、シードメーカーの壊滅的な侵害は、顧客に損害を与えます。残念ながら、OTPコードは、ユーザーをだまして偽のウェブサイトにアクセスさせることで最終的に盗まれる可能性があります。その後、ハッカーはコードを実際のサイトに転送してアクセスできるようになります。

画像タイトル：最新フィッシングがモバイルベース認証を破る方法



上の図は、モバイルベースの2要素認証（2FA）を回避するフィッシング攻撃の成功例を示しています。手順1で、攻撃者は被害者に、実際のウェブサイトに非常によく似た偽のログインページに誘導するリンクを含むフィッシングメールを送信します。手順3で、被害者は、攻撃者が収集したユーザー名とパスワードから、実際のウェブサイトのログイン画面に入ります。手順4で、2要素目にOTPコードが必要なため、実際のウェブサイトはOTPコードを被害者に送信し、被害者は偽のログインページに入ります。手順5で、攻撃者はOTPコードを収集して実際のウェブサイトに入力し、アカウントにアクセスします。攻撃者は通常、アカウントのセキュリティ設定を更新して、被害者を締め出します。

従業員のセキュリティトレーニングだけでは、フィッシング攻撃を防ぐのに十分ではありません。攻撃によって従業員、パートナー、またはベンダーが侵害されると、重大な損害が発生するまで誰も気付かずに、組織内をすばやく移動できます。ハッカーは、十分な情報を収集するだけで、ファイルを要求する同僚、請求書の支払いを要求するベンダー、機密性の高い事業の財務情報を要求するCEOなど、信頼できるソースであるかのうように簡単に見せかけることができます。こうした攻撃の大きな成功により、2018年以降、複数の業界の企業に260億ドル以上のコストがかかっています。[19]

全社規模のIDフィッシングから保護するためのベストプラクティス

企業リソースを保護するには、強力な認証を優先するベストプラクティスのIDおよびアクセス管理戦略が必要です。多くの企業組織はSMSやOTPなどの認証方法に移行していますが、これらのアプローチはSIMスワッピング、マルウェア、MitM攻撃などの脅威に対して脆弱です。ステルスSMS転送などの比較的新しい脅威により、近い将来、OTPのセキュリティリスクが高まる可能性があります。[20]

セキュリティと経済的リスクを除けば、モバイルベース認証は、コールセンター、クリーンルーム、製造フロア、研究所など、モバイルデバイスを禁止する多くの作業環境で実行できません。したがって、どのMFAも優れているわけではありませんが、組織は、企業全体のIDアクセス制御を強化するために、より安全でスケーラブルでフィッシングに強い方法を必要としています。すべての形式のMFAが同じではないことを覚えておくことが重要です。

以下に概説するのは、組織を企業全体のIDフィッシングから保護するための4つの方法です。

1 防御の最前線として強力な認証を展開する。

定義上、強力な認証はフィッシング対策以上のセキュリティを提供します。使いやすさ、展開の容易さ、迅速なスケーラビリティを提供します。これらはすべて、ユビキタスなパスワードベース認証からの移行を容易にするために重要です。強力な認証は、従業員全体、さらにはサプライチェーン全体で一貫して適用するために、使用が非常に直感的で、展開に費用対効果が優れている必要があります。

幸いなことに、多くの企業組織は、危険なパスワードベース認証を2FAおよびMFAに置き換え始めています。これらは比較的単純なアプローチであり、消費者向けアプリでも一般的な認証方法になりつつあります。また、管理コストとパスワードによるリスクを減らすために、認証プロセスの一部としてのパスワードを完全に排除する動きもあります。ただし、パスワードレスのセキュリティを実現するためには、最初のステップとして、レガシーで脆弱なMFAアプローチから移行し、最新のMFAを確実に実施しなければいけません。当社が実証したように、モバイルベースのMFAはハッキングされる可能性があります。さらに、モバイルデバイスが完全に制限されている場合など、特定の事業シナリオではオプションでさえありません。

また、セキュリティの意識に欠ける労働者や、ダークウェブでIPを販売するなど、復讐や金銭的利益のために会社のリソースを積極的に侵害する労働者から発生する可能性のある社内脅威リスクを管理することも重要です。悪意のある脅威が会社全体に広がるのを防ぐには、異常行動や不正アクセスの試みに起因する脅威を迅速に特定し、封じ込める機能が必要です。機械学習と人工知能は最も堅牢な分析機能を提供しますが、シンプルなMFAレポートも、潜在的な認証の脆弱性に対する有用な洞察を提供できます。

このような理由から、強力なMFAは、今日の差し迫ったセキュリティ要件を満たすだけでなく、攻撃の高度化に起因する新しい脅威ベクトルを処理するための適切なポジショニングを可能にする、複数のプロトコルをサポートする必要があります。最新のMFAソリューションは、複数の地域にまたがる多様な従業員だけでなく、パートナー、ベンダー、サプライヤー、さら にはエンドカスタマーから成る、企業のより大きなエコシステムでも簡単に導入できる必要があります。

サプライチェーン全体のセキュリティがこれまで以上に重要になっています。さらにこれを実現することにより、強力な認証が顧客とパートナーにより良いセキュリティを提供します。これは競争の激しい市場での重要な差別化要因になる可能性があります。

2 リスクベースのステップアップ認証アプローチを実装する

実際、すべてのセキュリティ戦略は段階的に実施する必要があり、すべての企業やユースケースに万能のアプローチはありません。これらのフェーズでは、次のような主要なフィッシングターゲットの保護に最初に取り組むことが重要です：

- **価値の高いアプリ：**これらには、メール、顧客注文および支払いアプリなどの生産性向上アプリ、およびシステム管理などの特権アプリが含まれます。これらのアプリやその他のアプリを保護するには、アプリにアクセスするユーザーと、アプリのアクセス元を特定して確認することが重要です。たとえば、ユーザープロファイリングと機械学習は、行動アルゴリズムとコンテキストアルゴリズムをアプリのセキュリティに適用することで、より堅牢なIDおよびアクセス管理（identity and access management、IAM）を提供するのに役立ちます。そのため、たとえば、従業員が異常なデバイス、ネットワーク、または場所から特権アカウントアプリにアクセスしようとしている場合、その異常にフラグを付けたり、エスカレーションしてユーザーのIDを確認したりできます 。
- **価値の高いユーザー：**エグゼクティブ、ドメイン管理者、その他の特権を持つ従業員など、特定の種類のユーザーは、機密データにアクセスするため、攻撃量が増える可能性があります。このタイプのユーザーは、非常に価値がありながら比較的簡単に侵害できるため、最も攻撃される人（Very Attacked Person、VAP）とも呼ばれます。強力な認証は、悪意のある存在、許可されていない存在が盗まれた認証情報を使用してアクセスするのを防ぐのに役立ちます。[21]
- **価値の高いリソース：**特定の企業リソースを保護することも、リスクベースのセキュリティアプローチの一部です。たとえば、SMS OTPが禁止されているモバイル制限エリアでどのタイプの認証が機能するかを検討してください。これは、ユーザーが1日に数回共有ワークステーションやアプリにログインする必要がある研究所や開発エリアで特に当てはまります。強力な認証は、ユーザーの信頼できるIDを検証することで、これらのリソースを悪意のある攻撃者やフィッシングやマルウェアなどの脅威から保護できます。

FIDO2は2018年に発表されたFIDO Allianceの最新仕様のセットです。これにより、ユーザーは一般的なデバイスを活用して、モバイルとデスクトップの両方の環境でオンラインサービスを簡単に認証できます。FIDO認証メカニズムは、フィッシングに強いだけでなく、サイバー犯罪者が暗号化されたメールメッセージなどの安全なネットワーク通信を盗聴、傍受することで行われるリプレイ攻撃に対し、強力に対抗することが可能です。リプレイ攻撃では、ハッカーがメッセージを遅延または再送信することで、受信者が、不正な銀行口座に預金するなど、ハッカーが望んでいる誤った方向へ導かれる可能性があります。

3 長期的なMFA展開戦略を作成する

パスワードレスの旅について、覚えておくべき最も重要なことは、まだその旅が始まったばかりだということです。一夜にしてそこにたどり着くのは不可能であり、またMFAの取り組みが完全に完了することは決してありません。脅威の状況は絶えず進化しており、それと戦うために設計されたテクノロジーも進化しています。

ただし、組織は今から、合理的に実行できることを始められます。たとえば、ベンダーや請負業者を基盤とする企業なら、重要なビジネスアプリにアクセスするときに強力な認証を義務付けることができます。モバイルOTPを使用するMFAを含めればり、ユーザー名とパスワードだけに比べて優れた認証方法となります。他の組織は、さらに進んで、ハードウェアのセキュリティキーを従業員とサプライチェーン全体に展開したいと思うかもしれません。パートナーは、最初にユーザーのテストケースから開始することで、この展開計画を支援できます。これにより、ハードウェアのセキュリティキーが複数のデバイス、アプリ、および最新システムとレガシーシステムの両方で機能することを確認できます。最終的に、これらのセキュリティキーはVAPに展開され、その後、より広範な従業員に展開されます。

ハイブリッドワーカーやリモートワーカー、または地理的に分散したサプライチェーンを持つ企業の場合、物理的な展開に対応できるハードウェアのセキュリティキープロバイダーと提携すると良いかもしれません。こうすれば、プロバイダーは、自宅、オフィス、世界中の職場など、どこにいてもユーザーにセキュリティキーを手渡すことができます。このサービスは複雑な配送ロジスティクスを排除できるため、多くの大企業が費用対効果の高い方法でパスワードレスへの旅を加速できます。

4 FIDO2とパスワードレス認証の準備する

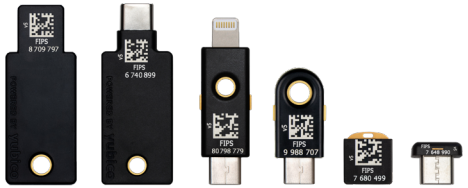
MFAの実装がパスワードレスへの第一歩です。さらには、FIDO2による認証などの標準ベースのソリューションは、フィッシングに対するさらに強力な保護を提供します。

セキュリティと使いやすさを向上させるために、FIDO2仕様にはWebAuthnが含まれています。これは、ウェブサイトがログインページを更新して、サポートされているブラウザとプラットフォームにFIDOベースの認証を追加できるようにするウェブベースのAPIです。これにより、ユーザーは一般的なデバイスを活用して、モバイルとデスクトップの両方の環境でオンラインサービスを簡単に認証できます。WebAuthn機能は、バイオメトリクス、モバイルデバイス、FIDOセキュリティキーを使用してユーザーが簡単にログインできるようにするために不可欠です。パスワードよりもはるかに安全な、非常に堅牢な形式の強力なMFAを提供します。[22] FIDOベースの強力な認証により、企業は今、強力な多要素認証を展開し、将来はパスワードレスへと移行できます。

YubiKeyによる最新で強固な認証

The YubiKey 5 Series シリーズ
左から右に向かって: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano, YubiKey 5C Nano.

YubiKey Bioシリーズ - FIDO Edition
左から右に向かって: YubiKey Bio FIDO Edition, YubiKey C Bio FIDO Edition.



The YubiKey 5 FIPSシリーズ
左から右に向かって: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS.

Yubicoのフィッシング対策ハードウェアセキュリティソリューションであるYubiKeyは、強力なユーザーIDとデバイス認証を備えた「何も信頼せず、すべてを検証する」ゼロトラストセキュリティアプローチをサポートします。YubiKeyはセキュリティ専用に設計されており、フィッシングやその他の形式のアカウントの乗っ取りを阻止し、強力な認証を大規模に提供します。モバイル認証とは異なり、ネットワーク接続やデータ保存、クライアントソフトウェアのインストールは必要ありません。

YubiKeyは次のことができます:

- 1回のタップまたはタッチで強力なハードウェア認証ができ、フィッシング攻撃やアカウントの乗っ取りを防ぎます
- Microsoft、Okta、Ping、Duoなどの主要なIDアクセス管理ソリューションを含む数百のアプリケーションとサービスと連携します
- 単一キーで複数のプロトコルをサポートし、レガシーアプリケーションと最新アプリケーションの両方で強力な認証を可能にし、高いROIを実現します
- FIPS 140-2は、NIST SP800-63Bガイドラインの最高認証保証であるレベル3の要件（AAL3）を満たすように検証されています（全体的なレベル1証明書#3907およびレベル2証明書#3914、物理的セキュリティレベル3）
- デスクトップPC、ラップトップPC、モバイルデバイス、タブレットの複数のフォームファクターで利用できます

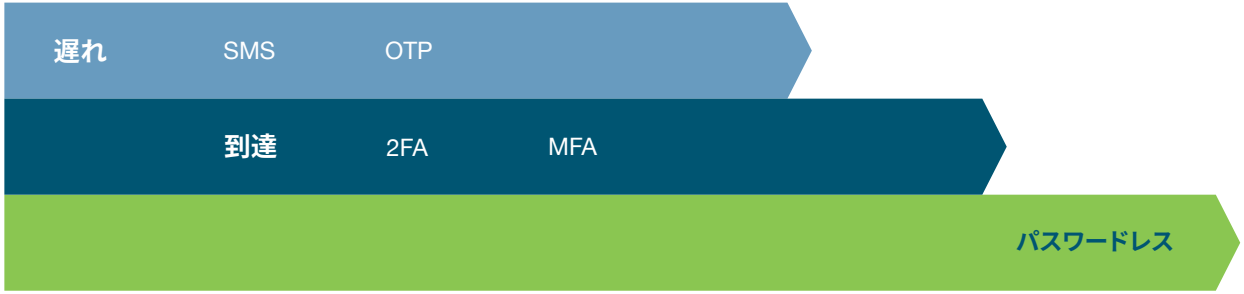
OTP、OpenPGPなどの単一のYubiKeyで複数の認証プロトコルを、Smart Card、FIDO U2F、FIDO2/WebAuthnなどの強力な認証プロトコルをサポートすることで、YubiKeyは、さまざまなレガシーおよび最新インフラストラクチャの強力な認証を柔軟に提供します。YubiEnterprise Deliveryを使用すると、YubiKeysをユーザーに直接送れるため、ハイブリッドワーカーとリモートワーカーを簡単に保護できます。

YubiKeyはパスワードレスへの架け橋

パスワードレスへの道は旅です。一夜にして移行できません。YubiKeyを使用すると、組織は、対処の必要がある既存インフラストラクチャとユースケースに応じて、FIDO2パスワードレス、スマートカードパスワードレス、ハイブリッド戦略を実装できます。YubiKeyは最も幅広いセキュリティプロトコルをサポートしているため、単一のセキュリティキーでさまざまな最新およびレガシーのアプリケーションとサービスを使用でき、組織は業務やユーザーの生産性を損なうことなく、段階的にパスワードレスに移行できます。

フィッシングを防止し、パスワードレスへの旅を始める

> YubiKeyがフィッシングや中間者（man-in-the-middle）攻撃を阻止し、メールフィッシングを困難にすることを知れば、さらに快適になります。
>
> **Kane Narraway　コーポレートセキュリティマネージャー Kane Narraway**[23]



パスワードは日常生活の一部のように思えますが、ユーザーエクスペリエンスとセキュリティのニーズが変化しています。フィッシング攻撃を防ぐには、パスワードを完全に排除する必要があります。パスワードレスへの道を歩み始めたばかりの組織にとって、特権管理者アカウントやリモートワーカーなど、ターゲットを絞った価値の高いユーザーを保護することから始めることが重要です。これらのユーザーを保護することは、短期的に大きな影響を与え、長期的にセキュリティロードマップ計画継続のための時間をもたらします。

最も重要なことは、今すぐ始めることです。なぜなら、突如として現れたリモートワーカーは、今後何年にもわたって存在するからです。企業のすべての従業員（および企業のリソース）をフィッシング攻撃から保護するには、脆弱な認証方法を捨て、完全にパスワードレスの企業へと変貌する必要があります。

YubiKeyは、強力で最新の認証を使用して、パスワードレスへの進化の道をサポートするように設計されました。詳細については、www.yubico.comを参照してください。

Sources

[1] https://apwg.org/trendsreports/

[2] The 2021 Cost of Phishing Study, Ponemon Institute

[3] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[4] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[5] https://www.verizon.com/business/en-gb/resources/reports/dbir/

[6] https://www.ibm.com/security/data-breach

[7] https://terranovasecurity.com/2020-gpt-report/?utm_campaign=En_GPTReport2020&utm_medium=Google&utm_source=Ads&utm_content=NewAd3&gclid=CjwKCAjw6fCCBhBNEiwAem5SO8oIgjFVtVzMA5pg-uSkRAho6S356pspA4bY3FBFk9FXCKW0Ksq-ExoCsHEQAvD_BwE

[8] https://www.yubico.com/resources/glossary/spear-phishing/

[9] https://www.helpnetsecurity.com/2021/06/14/phishing-levels-2021/

[10] https://www.agari.com/email-security-blog/ancient-tortoise-bec-attack-chain/

[11] https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/

[12] https://www.yubico.com/resources/reference-customers/city-of-mission-viejo/

[13] https://www.ftc.gov/coronavirus/scams-consumer-advice

[14] https://www.reuters.com/article/us-health-coronavirus-technology/permanently-remote-workers-seen-doubling-in-2021-due-to-pandemic-productivity-survey-idUSKBN2772P0

[15] https://www.verizon.com/business/en-gb/resources/reports/dbir/

[16] https://www.yubico.com/resources/reference-customers/datadog-leads-in-authentication-best-practices-deploys-yubikeys-to-all-employees-enterprise-wide/

[17] https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

[18] https://datareportal.com/global-digital-overview

[19] https://www.sans.org/webcasts/dont-bait-steps-avoid-phishing-attacks-120005/

[20] https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

[21] https://www.brighttalk.com/webcast/15793/479907

[22] https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/

[23] https://www.yubico.com/resources/reference-customers/atlassian/

yubico

Yubicoについて

Yubicoはコンピューター、モバイルデバイス、サーバー、インターネットアカウントにシンプルでセキュアにアクセスするための新しいグローバルスタンダードを創造しています。

中核となる製品は、タッチひとつで数多くのITシステムやオンラインサービスへのアクセスをセキュアにする物理デバイスのYubiKeyと、サーバーに保存されている機微なデータを保護する極小ハードウェアセキュリティーモジュールのYubiHSMです。

YubicoはFIDO2、WebAuthn、FIDO U2Fなどの認証標準化にも大きく貢献しており、わたしたちのテクノロジーは大手インターネット・ブランドの10社中9社や、160か国数百万のユーザーに利用され愛されています。

2007年に創立され非上場企業として活動しており、スウェーデン、UK、ドイツ、アメリカ、オーストラリア、シンガポールにオフィスがあります。さらに詳しい情報はこちらへ