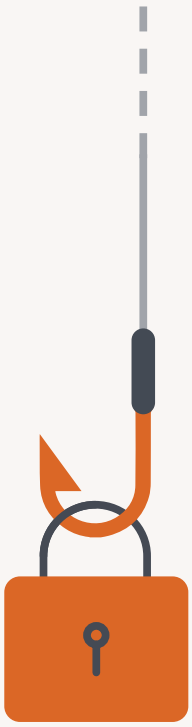
2021年版 フィッシング詐欺の傾向に関する調査結果

フィッシングの脅威は仕事や個人のメール、SMS、ソーシャルメディア、さらには広告まで、あらゆる形態のコミュニケーションに及んでいます

かつては社内メールに限られていたソーシャルエンジニアリングですが、今日ではモバイルやデスクトップなど、すべてのプラットフォームにおいて企業が直面する最大のサイバーセキュリティ上の脅威となっています。

その理由は、フィッシング攻撃によってユーザのデータを盗むほうが堅牢なデバイスのオペレーションシステムを攻撃するより簡単だからです。実際、組織がクラウドに対応した時代において、ユーザ認証情報は攻撃者にとってはるかに価値のあるものとなっています。ユーザ認証情報が分かればデバイスを超えて、SaaSアプリケーション、オンライン上のファイルストレージリポジトリ、さらにデータセンターで保管管理されている機密情報へのアクセス権を手にすることができます。

フィッシング攻撃は「受け取り忘れている宝くじ当選金があります」といった、すぐに詐欺だと見分けることができるメールからはるかに進化しています。受け取る人ごとにカスタマイズされ信憑性がより高いものになっているだけではなく、今まで以上に多くの場所にアクセスし、消費者だけではなくビジネスの認証情報やデータを標的としたものになっています。これにはモバイルの導入が大きく影響しています



フィッシング攻撃に騙されるモバイルユーザの増加

現在、インターネットのトラフィックのほとんどは、モバイルユーザによるものです。そして、ハッカーがこれを逆手に取って、モバイルプラットフォームに特化した攻撃を行っているのは驚くことではありません。モバイルデバイスの画面は小さく、多くのビジュアルショートカット機能が混在しているため、疑わしいサイトのURLや悪意のある送信者を検知するのが、デスクトップよりもはるかに困難になっています。また、優れた携帯性と本質的に自分に帰属しているものという感覚を持つため、モバイルデバイスを使っている間ユーザの注意力も散漫になり攻撃を受けやすくなっています。

モバイルユーザを攻撃対象にした、より説得力のあるフィッシング詐欺サイトが作成され続けており、10人に1人のモバイルユーザが被害に合っていると言われています。単にメッセージを受信するのではなく、実際にモバイルユーザがクリックしていることを意味します。

下記のグラフは、過去12ヶ月間にモバイルユーザを標的にしたフィッシング攻撃の被害が、前年比160%増加したことを示しています。これは、オンライン上に存在するフィッシング攻撃の数を示しているのではなく、被害にあったユーザの割合を示しています。罠にはまる被害者が増えているのは、攻撃者がその攻撃のテクニックを進化させているためと考えられます。今では、信頼のあるアプリを利用した攻撃の配信、説得力のあるドメインの登録、さらによく知られた有名ブランドを模倣するなどして、より少ない投資でより多くのユーザに近づこうとします。

10人に1人

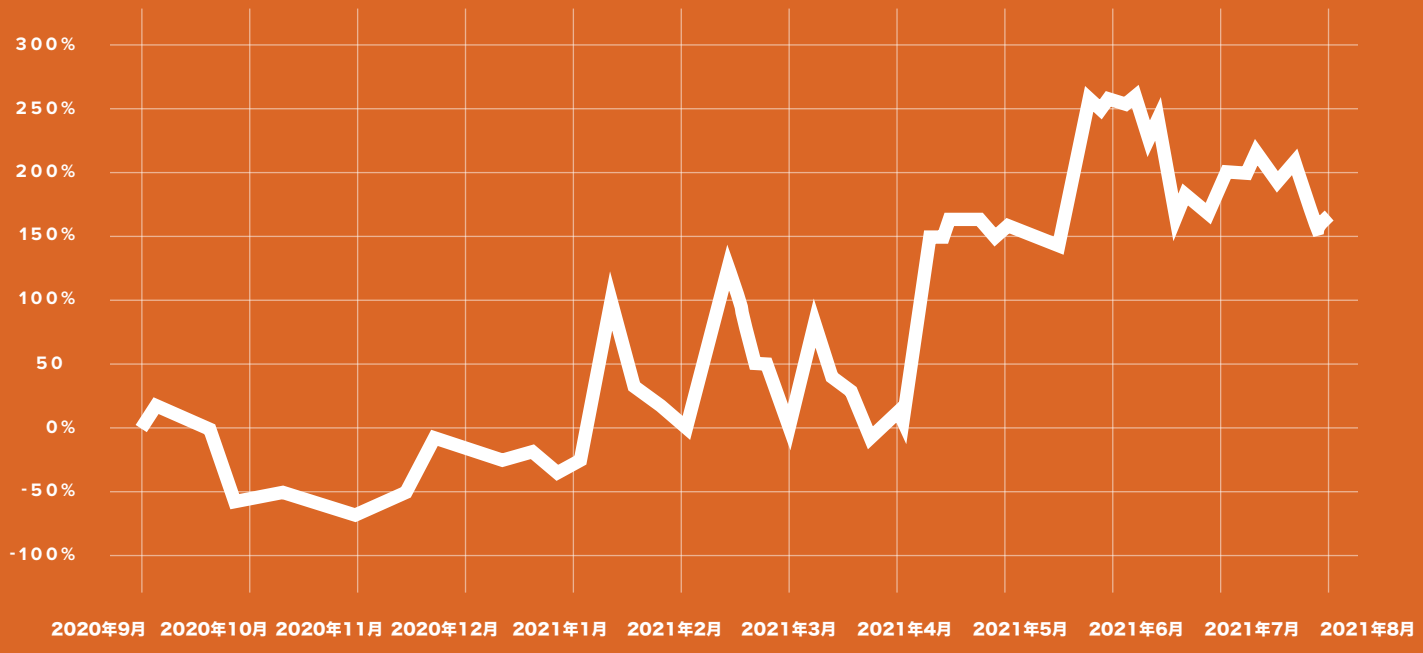
モバイルデバイスを使用中にフィッシング詐欺のリンクをクリックしています

資料：Wandera, a Jamf Company

フィッシング攻撃の犠牲になったモバイルユーザ数は前年比160%増加

資料：Wandera, a Jamf Company

フィッシング攻撃の成功率の推移



出典：Wandera, a Jamf Company

モバイルデバイスへのフィッシング攻撃を見分けるのは困難

今日、リモート勤務に使われるモバイルデバイスにおいて、フィッシングを見分けるのはより困難になっています。

- モバイルデバイスでは、画面サイズが小さく、ウェブサイトを正当に評価することが難しい
- ユーザインタフェースデザインの向上により、多くのコンテンツをページに表示できるようにするため、すでに小さいアドレスバーが隠れるようなデザインが一般的になった
- ユーザは、複数のデバイス上で、幅広い種類のアプリでコミュニケーションをとり、共同作業をするため、気が散りがちで、さまざまなページや通知を急いで見てしまいがち。加えて、アプリ開発者の多くがプロンプト内で「Accept（承認）」または「OK」ボタンを強調して表示するデザインを採用しているため、ユーザは内容を確認することなく自動的にプロンプトを受け入れる道を歩むことになっている
- メタデータではなくコンテンツを中心に構成され、合理化されたビジュアルにより、ユーザは、クリックする前にリンク先がどこなのかを判断できない
- テキストメッセージで一般的に使用されているBitlyやOwlyなどでURLが短縮化され、完全なドメインが表示されない

メールだけでなくユーザが予想しない場所にフィッシング攻撃は広がっています

従来のセキュリティでは、フィッシングを企業のメールに関する問題として扱ってきました。そのため、解決策をデバイスではなく、メールのアプライアンス自体に取り込んできました。しかし、モバイル化に伴いユーザは、より多数のアプリを使用し始めたにもかかわらず、その保護がされておらず、また、境界線の外へと移行したために、物理的環境を想定して構築されたセキュリティ保護による恩恵を受けられません。

エンドユーザのコンピューティングデバイスでは、アプリ内にダイレクトメッセージ機能を持つ多くのメッセージングやソーシャルメディアアプリを統合したコミュニケーションプラットフォームを提供しています。Appleシリコンを使用したMacBookはmacOSアプリだけでなく、iOSアプリやWindowsなども実行させることができ、完全なコンピュータ体験を提供することができます。メッセージングアプリは組織の防御において見落とされがちな領域であるため、攻撃者にとって格好の標的となっています。

モバイルに焦点を絞ったことでハッカーは、信頼されたメールドメインからSMS、WhatsApp、Messenger、Instagram、LinkedInなどユーザが信頼する多数の新しいサービスを利用した配信へ移ることができます。

さらに、ユーザを騙すために南京錠(暗号化)が、使用されています

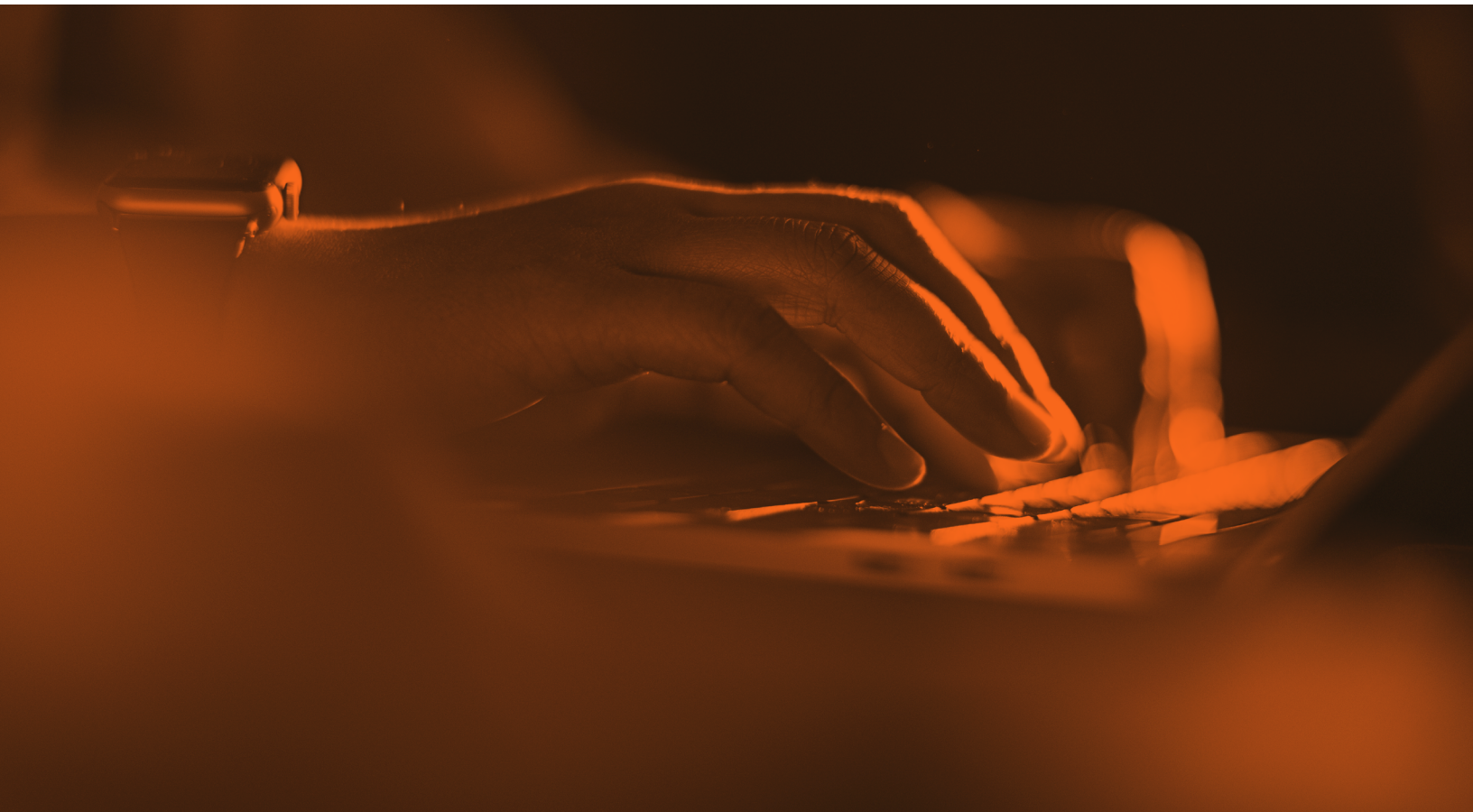
かつては悪質なドメインを見分けるのに、アドレスバーに南京錠のマークがあるかを確認するという簡単な方法がありました。しかし現在では、ハッカーは数ある無料オンラインサービスからSSL認証を簡単に手に入れて、悪意あるフィッシングサイト用に使うことができます。ユーザは、アドレスの前に南京錠マークがあればそのウェブサイトは安全だと信じているため、残念ながら、攻撃者にとって効果的な方法です。コスト面での壁が取り払われれば、攻撃者が悪質なサイトを暗号化しない理由はありません。

フィッシングドメインの93%がアドレスバーに南京錠がある「安全」なサイトによってホストされている

資料:Wandera, a Jamf Company

今日、93%のフィッシングサイトがHTTPS検証を利用し、その悪質性を隠しています。当社のデータでは、その数は2018年の65%からはるかに増加しています

資料:Wandera, a Jamf Company



Punycodeが悪質なドメインの識別を困難にしています

攻撃者はPunycodeを利用してフィッシングドメインを見分けにくくしています。Punycodeは、Unicodeを使用した文字（例えば、キリル語、ギリシャ語、ヘブライ語など）をASCII文字に変換して、コンピュータが理解できるようにします。

Punycodeを使った攻撃の始まりは、ブラウザがUnicodeに対応しておらず、アドレス表示のためにASCIIのみを使用していた時にさかのぼります。Punycodeは既知、または信頼できるドメインに極めて似通ったドメインに登録することが可能で、最終的にブラウザは実際には別のサイトにアクセスしているのに、あるサイトにアクセスしているかのごとくユーザを思わせることができるため、攻撃者はPunycodeを使い始めたのです。Unicodeでは一見すると見慣れたドメインでも、実際には別のサーバを指していたり見知らぬドメインにリンクされていたりします。

当社データによると、過去12ヶ月間、成功したゼロデイフィッシング攻撃の2%がPunycodeを含んでいました。以下はその例です。次のドメインで Unicode 文字を見つけてみましょう。

ユーザが犠牲になったフィッシング攻撃の2%はPunycodeを含む

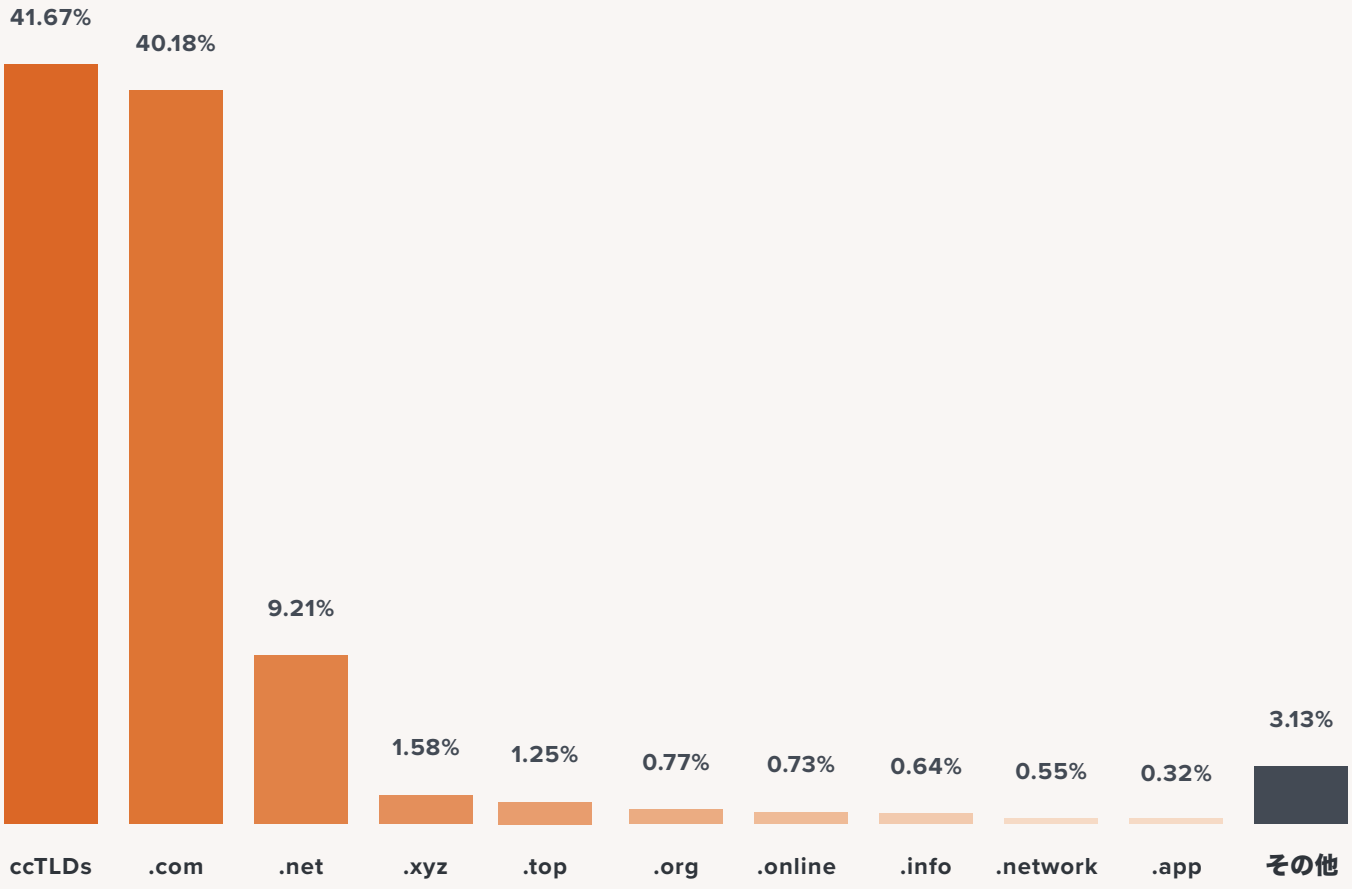
資料：Wandera, a Jamf Company

ブランド	ユーザに表示されるもの（UNICODE）	「デコード」されたPUNYCODE
Google	https://googĺe.com	xn--googe-95a.com
Starbucks	https://starbucks.com	xn--starucks-hpd.com
Rolex	https://rolẹx.com	xn--rolx-nu5a.com
Paypal	https://t.paypal.com	t.xn--ayal-9ndc.com
Facebook	https://www.facebook.com⁄login.en.do	www.facebook.xn--comlogin-g03d.en.do

曖昧なトップレベルドメインが事態を悪化させています

これまで、トップレベルドメイン（TLD）は、主に「.com」、「.net」、「.org」などでした。近年、さまざまな国コードトップレベルドメイン（ccTLD）や企業固有のTLDを使用したドメインが増加しています。（例「.attorney」、「.technology」、「.airline」など）以下は、これまでに成功したフィッシング攻撃に見られたトップレベルドメインの割合です。ここで危険なのは、知っているブランド名がユーザには表示されていても、フィッシングに使われるTLDが真のブランドのサイトのものではないことです。例えば、ハッカーは「microsoft.xyz」をドメインとして登録してMicrosoftをテーマにしたフィッシング攻撃をします。発見されると「microsoft.info」または「microsoft.network」などにすり替わります。

もう一度、過去12ヶ月間に当社のプラットフォームで検知したフィッシング攻撃の成功例に使われたTLDの割合（下記）を確認すると、「.com」と「.net」 が最もよく使われているトップレベルドメインで、「.as」、「.ru」、「.uk」などの国コードをまとめたものも使用されていることが分かります。



出典：Wandera, a Jamf Company

主要なポイント：暗号化、Punycode、そして、従来とは異なるTLDが加わり、有名ブランドを偽った説得力のあるフィッシングドメインを作るのがいかに容易であるか納得いただけるでしょう。

成功したフィッシング攻撃に使用されたブランドトップ10

攻撃の成功率を上げるために、悪意のある攻撃者はどの企業を偽装するかを吟味する必要があります。

攻撃者は攻撃を地域的なもの（例えば、地元の銀行ブランド）から、世界的でテクノロジーに携わるブランドを取り入れた攻撃に移行しています。ユーザは、実際に自身がアカウントを持つサイトを装ったフィッシング攻撃の犠牲になる可能性が高くなっています。シングルサインオン技術がより多くのアプリに取り込まれるにつれ、AppleやGoogle、Amazon、Microsoftなどの影響力のある大企業の認証情報は、単なる電子メール以上のものへのアクセスを提供します。それらは「魔法の鍵」となって、個人また企業データのさらなる層へと広がっていきます。責任は企業にあるのではなく、こういった組織は認知され貴重な情報源であるので攻撃者に利用されているに過ぎません。

悪意のある攻撃者は、Office 365やGoogle G Suiteアプリなど業務用アプリケーションにさらに標的を絞っています。組織がアクセスをクラウドに移行するにつれて、これは大きな懸念事項です。巧妙なフィッシング攻撃（例えば、Google Driveログイン認証情報を確認するなど）を受けた従業員が一度でも間違いを犯すと、ハッカーは一般的なクラウドアプリケーションに保管してある企業資産にアクセスできます。

当社調査によると、2021年にユーザを巧妙に騙したフィッシング詐欺のリンクに使われた3大ブランドは、Apple、PayPal、Amazonで、それぞれの割合は43%、27%、9%でした。

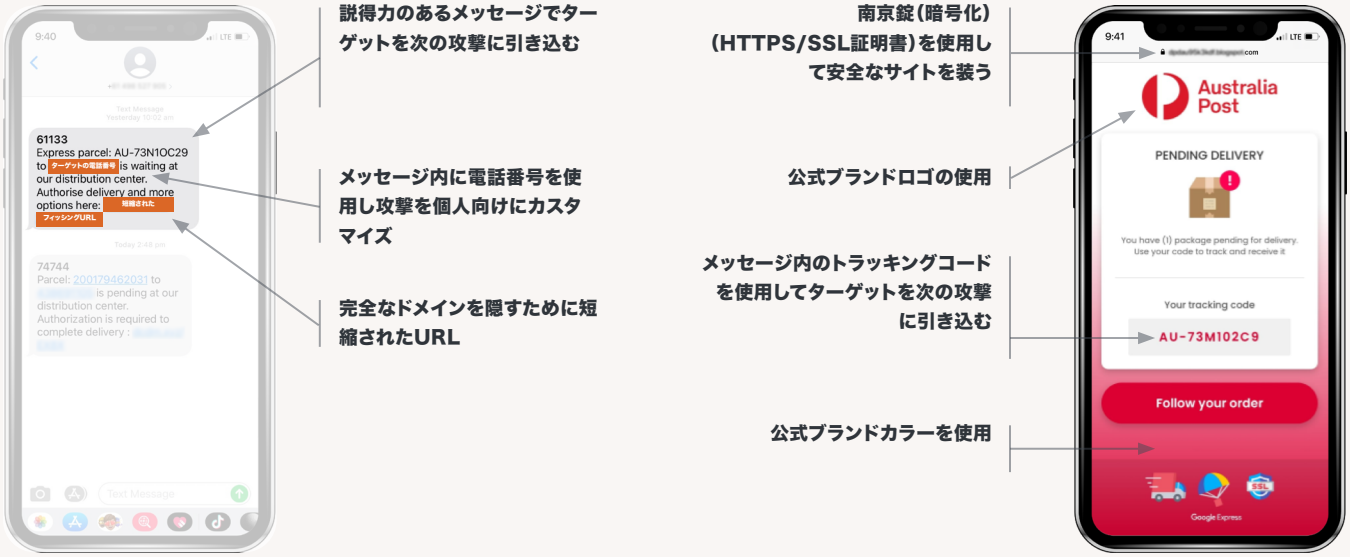
2021年にフィッシング攻撃キャンペーンに最もよく使われたブランド

1. Apple
2. PayPal
3. Amazon
4. Chase
5. Facebook
6. Google
7. Twitter
8. Netflix
9. Microsoft
10. Wells Fargo

出典：Wandera, a Jamf Company

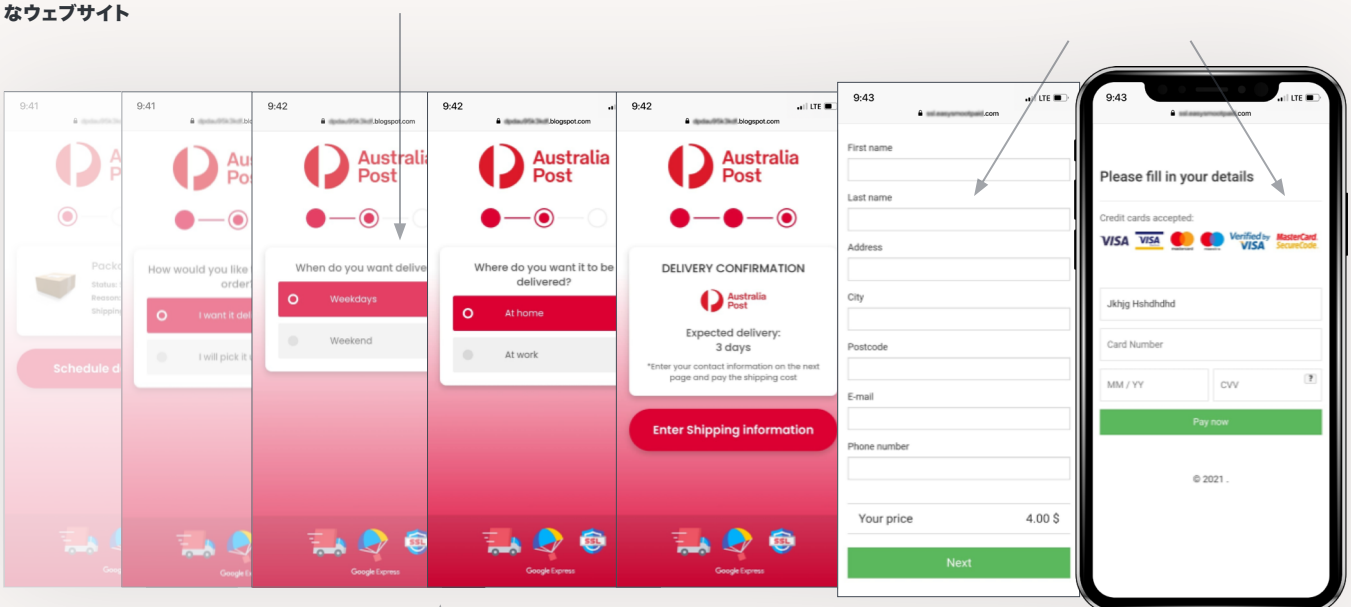
注意すべきフィッシング攻撃の例 — オーストラリアポスト

当社のリサーチャーは、疑わしいテキストメッセージが複数報告された際に、フィッシング攻撃キャンペーンを調査しました。メッセージは、広く知られるオーストラリアポストのブランドを騙った、郵便物配送を中心としたものでした。（オーストラリアポストは米国ではUSPS、また英国ではRoyal Mailに相当するブランドで、オーストラリアに居住し郵便物を受け取る人なら誰でも潜在的に攻撃の的となります）コロナ禍の下、オーストラリアでは厳重な封鎖が何度も繰り返され、市民は郵便配送に依存した生活を送っていた中での攻撃です。他の主要ブランドと同様に、オーストラリアポストには何も不手際はありません。ただ認識されるブランドなので利用されたのです。



一貫したアイコン、フォント、ブランドなどを持つインタラクティブなウェブサイト

認証情報、財務データ、およびその他個人情報の送信



ソーシャルエンジニアリング攻撃が進んでいく

出典：Wandera, a Jamf Company

お粗末なフィッシング攻撃キャンペーンは数多くあります。時にはメッセージがページの内容に関連していなかったり、ページの内容が非常に一般的な詐欺である場合があります。オーストラリアポストのフィッシング攻撃は、メッセージとページの内容に連続性があり、被害者に荷物の配達を承認する必要があると思わせるような、巧妙なものになっています。

オーストラリアポストのフィッシング攻撃はよく出来ていますが、フィッシングと見破られる点がいくつかあります。まず、URLに「auspost」ドメインを使用していません。次に、ブランディングは説得力のあるものですが、正規のオーストラリアポストのウェブサイトと完璧に一致していません。さらに、ユーザは別のブランドドメインに転送され、配達を承認する場合、通常は必要とされない支払いを請求されます。最後に、オーストラリアでは「センター」を「center」ではなく「centre」と綴ります。このような細かい点がフィッシング攻撃を見破るポイントとなることもあるので、気をつけてください。

簡単にできるリアリティチェック

フィッシングサイトの多くはインターネットに数時間だけ公開され、ハッカーはその後全く新しいホストサーバに移行します。検知を避けブロックされることもなく、フィッシング攻撃キャンペーンを続けていられるのはこのためです。固定リストベースの脅威インテリジェンスがアップデートされる前のユーザへのリスクは最も深刻です。

上記のオーストラリアポストの攻撃では、フィッシングドメインが報告されて削除されると、攻撃者は新たなドメインを登録して攻撃を再開し、その新たなドメインも報告されるまで繰り返します。トップレベルドメインの数と、現在正規のURLに見られるたくさんのサブドメイン（「login.」、「mobile.」、「en.」など）を考慮すると、攻撃者がこのようなフィッシング攻撃キャンペーンを続けていられる理由がお分かりでしょう。下記の例で、独自のフィッシングURLを組み合わせて、もし、ご自身が目にしたら、その罠に引っかかる可能性があるかを試してみてください。

気をつけてください！

説得力のあるメッセージを受信した場合は、届いたメールまたはメッセージをクリックするのではなく、直接そのサービスのアプリやウェブサイトへ移動することを推奨します。

サブドメイン	ブランド	トップレベルドメイン
tracking.	aus-post	.com
feedback.	auspost	.net
mobile.	australiapost	.review

推奨事項

フィッシング攻撃は、企業の中で最も脆弱性の危険性がある、従業員を狙います。従業員は、企業にとって最も価値のある資産ですが、データを安全に保護するという点では最大のセキュリティの弱点でもあります。

だからこそ単にメールだけでなく、全てのコミュニケーションアプリで動作するゼロデイフィッシングソリューションは、一般的な攻撃、またビジネスに特化したさらに巧妙な攻撃の両方を阻止するには重要です。

フィッシング攻撃の被害にあった後、対処策として何をすべきでしょうか。

- 漏えいしたアカウントのパスワード、それらと同じまたは類似したパスワードを持つアカウントのパスワードを全て変更する
- フィッシングページにクレジットカード情報を入力した場合、カードをキャンセルする
- コンピュータをオフラインにする、あるいはメールアカウントを削除して、フィッシングリンクが連絡先リストに広がるのを防ぐ
- 攻撃で装われた組織または個人に連絡する。最高経営責任者や同僚、または銀行担当者である可能性があります。メッセージに返信するのではなく、電話など別の連絡方法を用いて相手が情報の送信先であるかを確認する
- ID盗難の警告に注意し、クレジット口座に詐欺警告を提出する

最良の改善策は防止することです。以下のアドバイスに従ってフィッシング被害を防止してください

- 疑わしいリンクをクリックしない
- URLの文字を慎重に観察する疑わしい場合、Punycode攻撃でないかをより効果的に見極めるため、ブラウザからURLをUnicode対応のエディタにコピーしてみる
- 大手テクノロジー企業ブランドからのメッセージには注意するメッセージが
  口調、語句、地域の方言などと一致しているかを確認
- クレジットカード情報を無名または信頼できないサービスに入力しない
- リンクがお使いの銀行のウェブサイトに転送される場合、別のウィンドウで銀行名を入力し銀行サイトを開くか、公式アプリを使用する
- 賞金を獲得したことを知らせる明らかな詐欺に引っかからない
- アドレスバーに「my.apple.pay.com」などの不審なURLや模倣されたURLが表示されていないか確認する

この調査について

当社ではモバイルフィッシングの実態と、最も危険にさらされている情報についてより理解を深めたいと考えていました。本ホワイトペーパーと統計では、Jamfの一部であるWanderaのお客様をベースに、90か国50万台の保護されたデバイスを対象とし、発見されたフィッシング攻撃の動向を2021年第3四半期に分析しました。本調査において分析されたメタデータは、個人または企業特定の情報を含まない集計ログを使用しています。

この分析は脅威に対する不安をあおろうとしたものではなく、お客様自身、またお客様のユーザに与えられている選択肢を示し、デバイス、ユーザ、そして組織のデータをあらゆる面で安全に維持する方法をアドバイスするためのものです。セーフガードを守りセキュリティポスチャを拡張する方法に関する詳細については、当社にお問い合わせください。