Lookout®

研究レポート

モバイル フィッシングの現状

昨今のフィッシングの傾向を理解することは、モバイルやリモートで仕事を行う従業員のデバイスを効果的に保護するうえで必要不可欠です。

目次

本レポートの概要

今日のモバイル セキュリティは常に進化しています。モバイル デバイスは個人でもビジネスでもかつてないほど使用されるようになりました。世界中が、つながりを強化し生産性を高めるための「乗り物」として、モバイルによるアクセシビリティを捉えています。もちろん、モバイルに依存することには大きなリスクも伴います。しかし、*Verizon Mobile Security Index 2020* レポートによると、そのようなリスクがあるにもかかわらず、43% の組織がセキュリティ面に不備を抱えており、さらには 39% の組織がセキュリティ侵害の被害を被っています。

悪意のある攻撃者は、モバイル デバイスへの依存度の高まりに気付いています。攻撃者の観点からすると、モバイル フィッシングは最も安上がりに個人や組織を攻撃できる手段となっています。これまでの事例を踏まえて、このような攻撃はメールでのみ行われると思われがちですが、Verizon によれば、モバイル フィッシングの 85% はメール アプリ以外で発生しています。モバイル ユーザーの 96% 以上が自分のスマートフォンに通信アプリやソーシャル アプリを導入していることや、組織がモバイル セキュリティを軽んじていることを考え合わせると、誰もがリスクにさらされています。

モバイル フィッシングは世界的な問題です。地域や業種を問わず、消費者ユーザーと企業ユーザーの両方がモバイル フィッシング攻撃を受ける確率は着実に増大しています。小さめの画面や短縮された URL では、フィッシング攻撃を見分けることが一層困難です。攻撃者はより実物に近い偽ページを作成することに精通しています。ソーシャル エンジニアリングを利用し、攻撃者にとってはメリットとなる画面の小ささを利用し、フィッシング攻撃を見分けにくくしているので、リスクが劇的に増大しているのです。

フィッシング攻撃の被害にあった場合の財務リスクは、組織に壊滅的な影響をもたらしかねません。多国籍企業では、フィッシング攻撃を成功させてしまうと、何億ドルもの損失を生じさせる可能性があります。地域医療システムのような、そこまで大規模でない組織であっても、リスクはやはり数千万ドルに及びます。

世界のどの地域のどの業界の組織であっても、モバイル フィッシングはもはや無視できない問題になっています。モバイルを標的にしたフィッシング攻撃、そうした攻撃への遭遇率、標的になった人が実際にタップしてそのリンクをたどる割合が着実に増加している状況を鑑みると、組織は現状を理解し適切な措置を iOS と Android デバイスに導入して、会社と顧客を有害なデータ漏えいから保護する必要があります。

はじめに

フィッシングとは、知らないうちにログイン情報を渡したり、マルウェアをダウンロードしたりするように人々を誘導する、悪意のある手法です。これらは最終的に、攻撃者が組織のネットワークにアクセスして会社の機密情報を盗み出すことにもつながります。もはやフィッシング リンクは単にメールに隠されるものではなく、メッセージング プラットフォーム、ソーシャルメディア、マッチング アプリ等をはじめ、あらゆるところに潜んでいます。

今日に至るまでの業界の歩みはどのようなものだったでしょうか。本レポートは、フィッシングやその対策についてのこれまでの経緯について記し、新たな傾向にスポットライトを当て、モバイルや自宅で仕事をしている従業員を保護するための効果的な方法を紹介しています。

フィッシングの起源

フィッシングは長年の間、悪意のある攻撃者が無防備な被害者からデータを盗む、最も効果的な手段の 1 つでした。実際、企業に対するサイバー攻撃の 91% がスピアフィッシング メールに端を発しており、特定の個人を標的にして欺き、攻撃者による企業のインフラへのアクセスが認証されるように誘導するものでした。

フィッシングの起源はメールにありますが、これは元々マルウェアを被害者に届けるサイバー攻撃の手段の 1 つでした。2000 年に、悪名高い ILOVEYOU ウィルスが登場。大量にウィルスを配布する方法としてメールが使われた最初の例として記録に残されています。それから間もなくして、ドメイン スプーフィングが攻撃ベクトルとして現れました。悪意のある攻撃者はこれを使い、メールが特定の組織や個人から送られてきたもののように見せかけ、被害者に資金を移動させたり、ログイン情報を共有させたり、その他のデータを漏えいさせたり、今日のオンライン詐欺につながることができるようになりました。

数年後、これらの詐欺手段は、大規模な個人のグループを低コストで標的にできる有効な方法として、サイバー攻撃者に認識されました。2000 年代初頭、*PCWorld* などの商業誌がこれらのメール詐欺をフィッシング攻撃と呼称したことから、フィッシングは業界用語になりました。

2004 年までは、被害者が知識不足の上、保護されてもいなかったため、フィッシング攻撃を行う者たちは大きな成果をあげました。2004 年の 5 月から 2005 年の 5 月までの間に、米国の企業はフィッシング攻撃により約 20 億ドルの損失を被ったと推定されています。また消費者レベルでは、米国の 120 万人のコンピューター ユーザーがフィッシングにより約 9 億 3000 万ドルの損害を被ったと推定されています。大西洋の反対側でも、英国だけでフィッシング攻撃が 8,000% 上昇したとする金融サービス組織の防犯チームの報告があります。フィッシングを特徴とする初期の攻撃で主流だったのは、Visa クレジットの顧客や Citibank の顧客を標的にしたり、John Kerry の大統領選挙戦のサポーターを標的にしたりするなど、特定のグループを対象とするものでした。

兄弟から送られてきたように見えるメールはフィッシング メールで、金銭的支援を求め、偽の寄付ページに誘導するものでした。

セキュリティ ソリューションのフィッシング対応はかなり進歩しましたが、他方でフィッシング攻撃も進化しています。特定の個人や組織になりすますのは常套手段になり、本物の ID のメールと偽の ID のメールを見分けることはますます難しくなっています。

1 人の従業員がフィッシング被害にあっただけで、組織の内外に多大な損失を招くことに、サイバーセキュリティのリーダーはすぐに気付きました。最もリスクが高いのは、金融や医療など、厳しいコンプライアンス基準で規制されている業界です。二次被害として、ブランドの評判が悪くなり、ビジネスが継続できなくなる危険性もあります。

より多くの個人や組織がモバイル デバイスを使用するようになり、攻撃者がフィッシングをメールからサードパーティーのメッセージング プラットフォーム、個人向けアプリ、生産性スイートに拡大させるに伴い、フィッシングの戦場は多様性を極めています。ここ数年間で、より多くの従業員が自分のモバイル デバイスを使って職場と同じように効率的に業務を行える環境を望むようになり、2014 年から 2019 年の間にリモートで仕事をする人は 44% 増加しました。組織からすれば、モビリティを可能にすることは賢明な選択です。これにより、出張中の従業員やリモートの従業員は、オフィス外から業務を行うのに必要な内部リソースにアクセスすることができ、高い生産性を保つことができるようになります。さらに最近では、COVID-19 パンデミック対策として、ソーシャル ディスタンスを保たなければならない期間中も業務を遂行するため、自宅で仕事することを選ぶ人がかつてないほど増えています。しかしこれは、これまで自宅勤務の経験が無い多くの従業員に利便性を与えると同時に、組織にとってはリスクの増大を意味します。

近年のリモート環境の普及に伴い、多くの組織はモビリティの実現をセキュリティの確保より優先しています。脅威という側面から見るとモバイルは比較的新しいベクトルのため、ほとんどの IT チームとセキュリティ チームはモバイル化に関するプロジェクトに参加していません。これは、会社全体のセキュリティに対する姿勢に多大なマイナス影響を与えています。悪意のある攻撃者はこのことを知っており、モバイル攻撃をどのように回避するかを知らない、知識不足のモバイル ユーザーを餌食にしています。

モバイル デバイス上の操作で本物と偽物を見分けることは非常に難しくなってきており、一般ユーザーがフィッシングに気付くことは難しく、世界中でモバイルを標的にしたフィッシング攻撃が増加することにつながっています。

モバイル フィッシングとは何か

初期のフィッシング対策ツールはメールを主な対象にしていました。悪意のある攻撃者がフィッシング メッセージをインターネットに接続している大勢の人にばらまく方法はメールだけだったため、これは妥当な方法で、メールは多種多様な攻撃を行うための下地となりました。サイバー攻撃者にとって簡単なフィッシング攻撃を一律に多数に向けて行うことは、費用と時間の両面において最低限の投資でハイ リターンを期待できるものでした。

メール セキュリティ ソリューションのフィッシング攻撃の検出能力は高まってきており、悪意のある攻撃者は攻撃を成功させるための新たな手法を生み出すことにやっきになっています。近年のフィッシング戦争の高まりと同時進行的に起きているスマートフォンの高性能化を考えると、フィッシングを行う者たちの次の標的がモバイルとなることは簡単に想像できます。攻撃者たちの標的がモバイルに推移する中、SMS (スミッシング) やソーシャル メディア プラットフォーム などの新たなチャンネルを利用したソーシャル エンジニアリングにより、フィッシング攻撃は日々進化を遂げています。

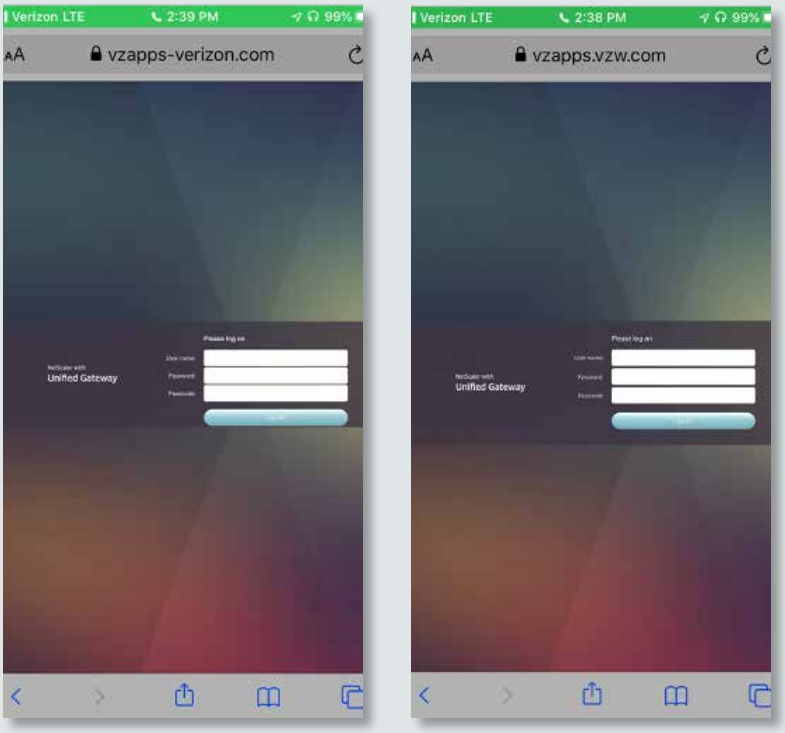
メッセージングによるフィッシング。銀行から送られてきたと見せかけたセキュリティに関する偽のメッセージ。
標的の名前を使用した無料のデータ提供。Facebook Messenger のソーシャル エンジニアリング攻撃。

モバイル フィッシングの成功率

モバイル デバイスへのフィッシング攻撃の成功率は非常に高くなってきています。その一因としては、ノート PC やデスクトップ PC の画面では認識できていたフィッシング攻撃の兆候を、モバイル デバイスで見分けることがとても難しいという点にあります。小さい画面、 デバイスを操作する速度、そしてモバイルではリンクを開ける前に内容を確認する方法をほとんどのユーザーが知らないという事実。これらはモバイル フィッシング攻撃に気付くことを大幅に難しくします。

さらに、ビジネスの分野では Bring Your Own Device (BYOD: 個人所有の機器の持ち込み) モデルが採用され、従業員が個人デバイスを業務に使用して、会社のあらゆるデータにアクセスできるようになってきています。Gartner は「2022 年までに、企業で使用されるスマートフォンの 75% が個人所有の機器の持ち込み (BYOD) になる (2018 年の 35% から上昇)」と予測しています。この動きは、さらに多くの従業員が個人デバイスを使って会社のデータにアクセスすることを意味しています。適切なセキュリティ対策を実施しない場合、データを今まで以上に危険にさらすことになったり、意図せずに過剰なアクセス許可が与えられたりすることにより、重大な事故につながりかねません。

下に Verizon の従業員を標的にしたモバイル フィッシング攻撃の例と、サイバー攻撃者が模倣した本物のモバイル画面を並べて示しています。従業員を標的にするのは会社内部のデータやインフラへのアクセス権を入手するかなり効果的な方法であり、この攻撃者は 1 人が引っかかるだけで十分であることを知っています。この攻撃は単なる共有 URL なので、攻撃者はさまざまな方法で配ることができます。標的が内部従業員であることを考慮すると、攻撃者が用いる配布手段は、経営幹部になりすましたメッセージ、Verizon の従業員がかなりの割合を占める地域の市外局番の電話番号に SMS をばらまいて送る、個人のプラットフォームのソーシャル エンジニアリングで特定の個人を標的にするなどが考えられます。



偽の Verizon 従業員ログイン ポータル (左) と本物 (右)。出典:Lookout

攻撃者は Web ページのユーザー インタフェース (UI) をかなり精巧に偽装しており、少ない要素で構成されるシンプルなログイン ページを意図的に選んでいるようです。さらに攻撃者は、本物のように見える URL を使用し、被害者にほとんど警戒心を抱かせません。

モバイル デバイスへのログイン情報の入力という日常的な行為を考えると、いつもログインしているページのようにみえるページを、被害者がその都度くまなく観察することは皆無に等しいと言えます。

これは、攻撃者が企業のアカウント情報を入手するためにフィッシングを使用する場合の典型的な攻撃例です。企業を対象としたフィッシング攻撃の主な標的の 1 つに、高いレベルのアクセス特権 (財務記録、研究データ、顧客データなどの資産へのアクセス権) を持つ従業員のアカウント情報があります。これは、企業レベルでの悪影響を及ぼす危険性があります。

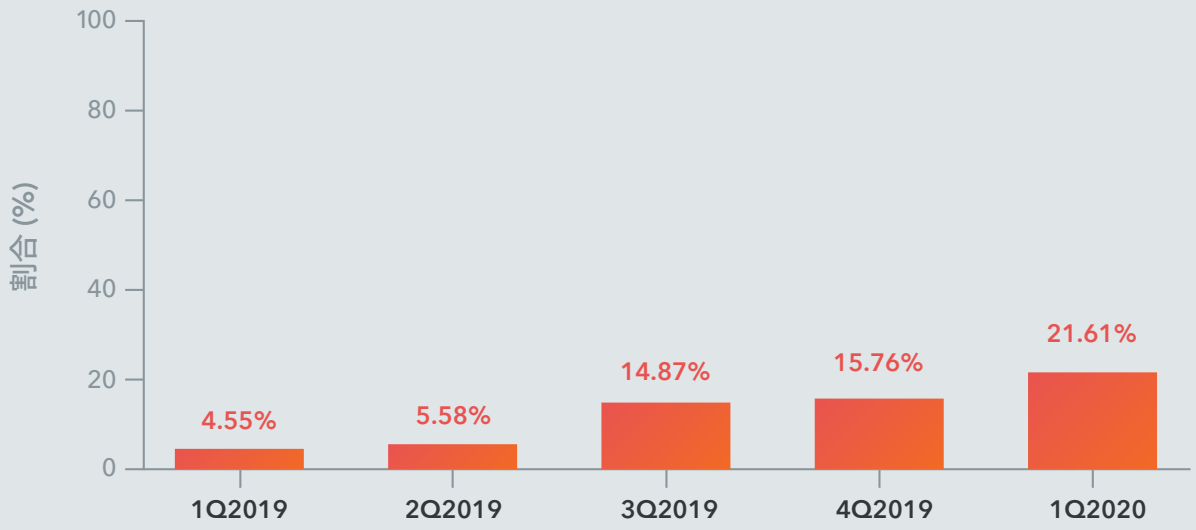
モバイル フィッシングの成功率が上がっているのは、従業員が個人デバイスを業務で使用することを許可されていたり、特定の市外局番の電話番号を用いて 1 回で大人数からなるグループを標的にできたり、攻撃者が UI をピクセル単位でほぼ完全に複製できたり、モバイルデバイスがコンピュータと比べてフィッシング攻撃を認識する方法に乏しいことが原因となっています。

フィッシング攻撃は世界中で起きている

モバイル フィッシング攻撃は世界中で発生しています。下の地図に示すように、世界中のあらゆる地域の国々がこの問題に取り組んでいます。この地図の元データは、Lookoutでモバイル デバイスのフィッシング対策をしている全ての国のお客様の、2019 年のフィッシング攻撃遭遇率を示しています。

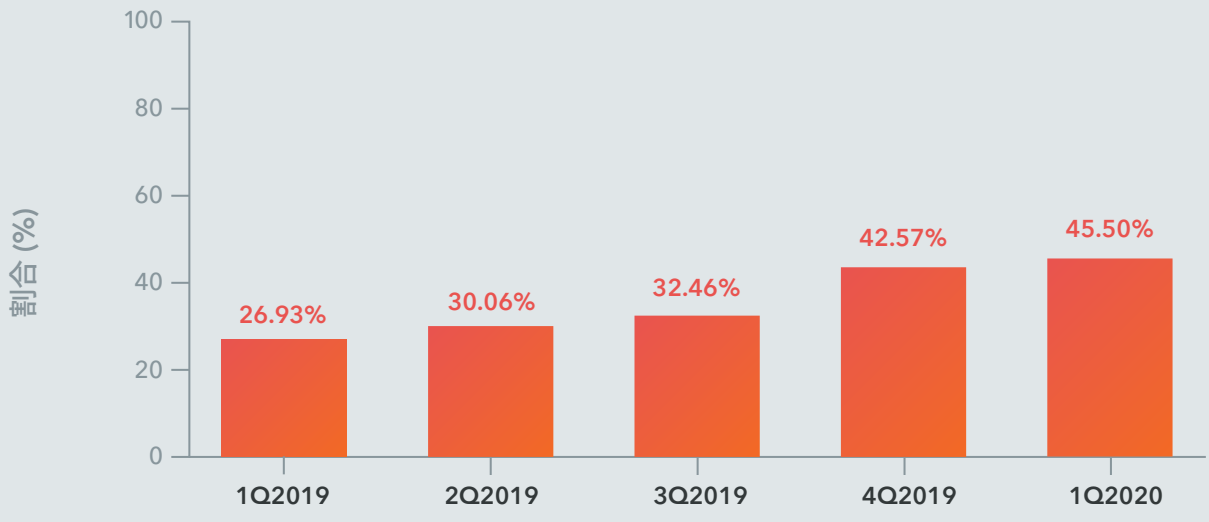
2019 年の全世界におけるモバイル フィッシング攻撃遭遇率。出典:Lookout:

過去 15 カ月に渡り、四半期ごとにモバイル フィッシングは上昇傾向にあります。特に注目すべきは、2019 年の第 4 四半期から 2020 年の第 1 四半期にかけて、約 37% の大幅な増加が見られたことです。この大半は COVID-19 による状況を悪用したフィッシング攻撃によるもので、攻撃者は被害者をフィッシングの餌食にしています。



2019 年第 1 四半期から 2020 年第 1 四半期までの、四半期ごとの企業のフィッシング攻撃遭遇率。出典:Lookout:

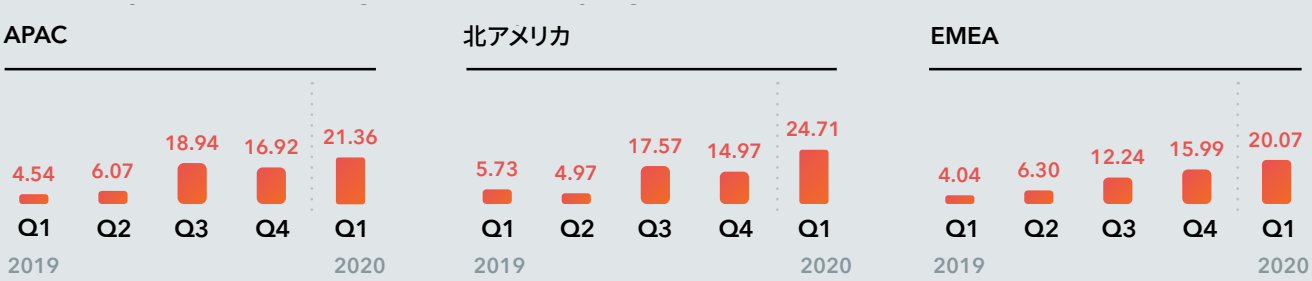
消費者のデバイスでは、より大きなスケールで同様の傾向が見られます。これらの 2 つの割合には大きな違いがありますが、Gartner は、個人のデバイスを使用して会社のデータにアクセスすることを許可した場合でも、BYOD ユーザー個人の習慣は変わらないため、企業における BYOD の増加に伴い企業に対する攻撃遭遇率も同じように増加すると予測しています。結論、今後数年の間に、企業リスクの増加は不可避であると言えます。



2019 年第 1 四半期から 2020 年第 1 四半期までの、四半期ごとの個人のフィッシング攻撃遭遇率。出典:Lookout:

地域別データを見ても、モバイル フィッシングが着実に世界的な脅威となっていることは明らかです。テクノロジーの進歩が比較的遅れている地域では、ユーザーが攻撃を見分ける訓練を受けておらず、悪意のある攻撃者に対抗し続けるためのテクノロジーも入手できないため、脅威がより大きくなっていると思われるかもしれません。しかし以下に示すように、誰もが同じようにモバイル フィッシング攻撃に遭遇する可能性があります。

2019 年 第1四半期から2020年 第1四半期にかけて、地域別の企業におけるモバイル フィッシング攻撃遭遇率(割合 %)



地域別、企業のモバイル フィッシング攻撃遭遇率。出典:Lookout:

企業については、すべての業種が何らかの手段でフィッシング攻撃の標的となっています。特に、2019 年の第 4 四半期にモバイル フィッシングの標的となって影響を受けた上位 5 つの業種は、高い企業価値や市場価値を持ち、厳格な規制を設ける業界となっています。

標的にされた上位の業種は、厳格に規制された業種でもある。
出典:Lookout:

あらゆる観点から、モバイル フィッシングはもはや無視できない世界的な問題となっています。個人であろうが大規模企業であろうが、モバイル デバイスを確実に保護するため、自分たちにできることしなければなりません。攻撃者から見ると、彼らは個人消費者と企業の両方を標的とすることに成功しています。以下に示す通り、企業ユーザーについては、最初に攻撃が成功した後は、成功率が急激に低下する傾向にあります。企業ユーザーが実際にフィッシング URL をタップする割合を見てみると、デバイスが会社所有であろうが個人所有であろうが初めてフィッシング リンクに関わった後、自分の間違いからすぐに学習していることが明白です。

かたや一般消費者は、企業ユーザーほどには注意していないように見えます。使用しているデバイスが会社のデータやインフラにつながっていないからかもしれませんし、例え悪意があろうと URL からブロックされた状態を不便に感じる気持ちが大きいからかもしれません。企業ユーザーと一般消費者がほぼ対極的な習慣を示していることが観察されるのは興味深いことです。

対象	プラットフォーム	1	2	3-5	6+
企業向け	Android	44.4%	18.2%	21.7%	15.7%
	iOS	46.5%	19.6%	20.4%	13.5%
	合計	45.8%	19.2%	20.8%	14.2%
消費者向け	Android	22.0%	13.7%	23.2%	41.1%
	iOS	20.4%	13.1%	22.3%	44.2%
	合計	21.6%	13.6%	23.0%	41.8%

2019 年、フィッシングで攻撃を受けた数のユーザー別詳細。出典:Lookout:

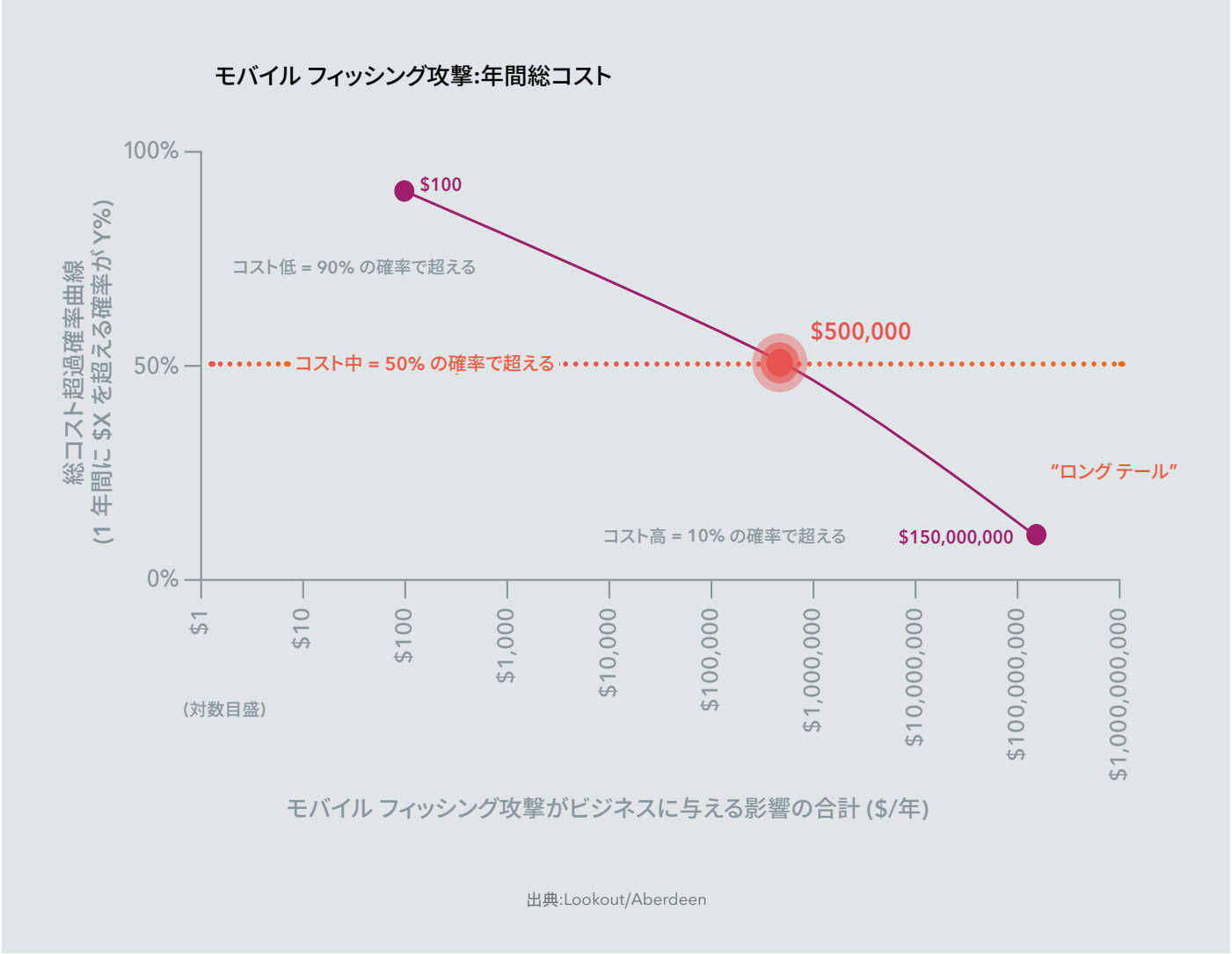
フィッシングによる潜在的な財務リスク

セキュリティ リスクは、いつの時代も規模を問わず、世界中の組織の課題となっています。そして組織にとっての最大の懸念は、セキュリティの不備が組織の財務に及ぼすリスクです。

以下に、Aberdeen の Phishing Risk Assessment ツールで見て取れる、フィッシング攻撃が様々な規模や業界の組織財務に与える可能性のある影響を示す 3 つの例を示します。組織に対するモバイル フィッシングのリスクを評価するにあたり、要因となるいくつかのデータ ポイントがあります。そうしたデータ ポイントには、モバイル デバイスの数、Android と iOS の割合、組織が Mobile Device Manager (MDM: モバイル デバイス マネージャ) を使用しているかどうか、そして最も重要な点として、組織が所有するデータ レコードの数が含まれます。

例 A:全国展開する医療システム

ここでは、50,000 台のデバイスを MDM で管理する大規模な企業組織を例として取り上げます。この企業には約 1 億のデータ レコードがあり、Android デバイスと iOS デバイスの割合は 50 対 50 です。このシナリオは、病院とケア センターを運営する全国的な医療組織特有のものです。



出典:Lookout/Aberdeen

前提:50,000 台のモバイル デバイス | 50% が iOS、50% が Android | 100,000,000 レコード

攻撃を受ける台数:最小:4,400 台のデバイス | 最大:23,760 | 中央値:13,570

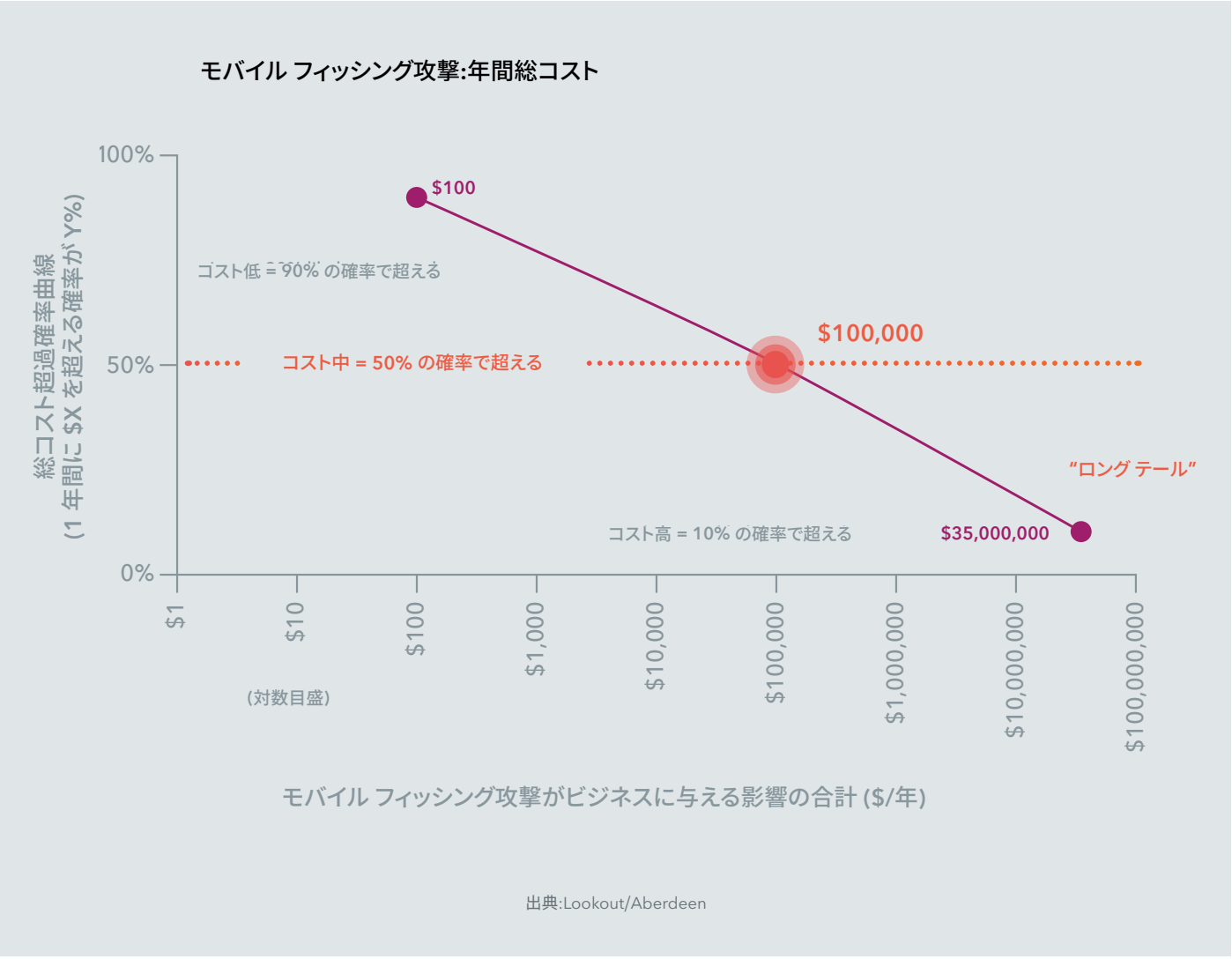
クリック数:最小: 1,760 | 最大:12,760 | 中央値:6,640

影響の中央値: $500,000/年

最大リスク: $150,000,000/年

例 B:多数の現場作業員を抱える大手メーカー

ここでは、10,000 台のデバイスを MDM で管理する組織を例に取り上げます。この企業には約 1,000 万のデータレコードがあり、80% が Android ユーザー、20% が iOS ユーザーです。このシナリオは、いくつかの工場を運営し、大規模な現場サービス チームを持つメーカーに当てはまります。工場、事務所、現場の従業員は、会社の製品の設計、製造、サービスを行うために、機密データと知的財産にアクセスする必要があります。



出典:Lookout/Aberdeen

前提:10,000 台のモバイル デバイス | 20% が iOS、80% が Android | 10,000,000 レコード

攻撃を受ける台数:最小:810 台のデバイス | 最大:5,220 | 中央値:2,670

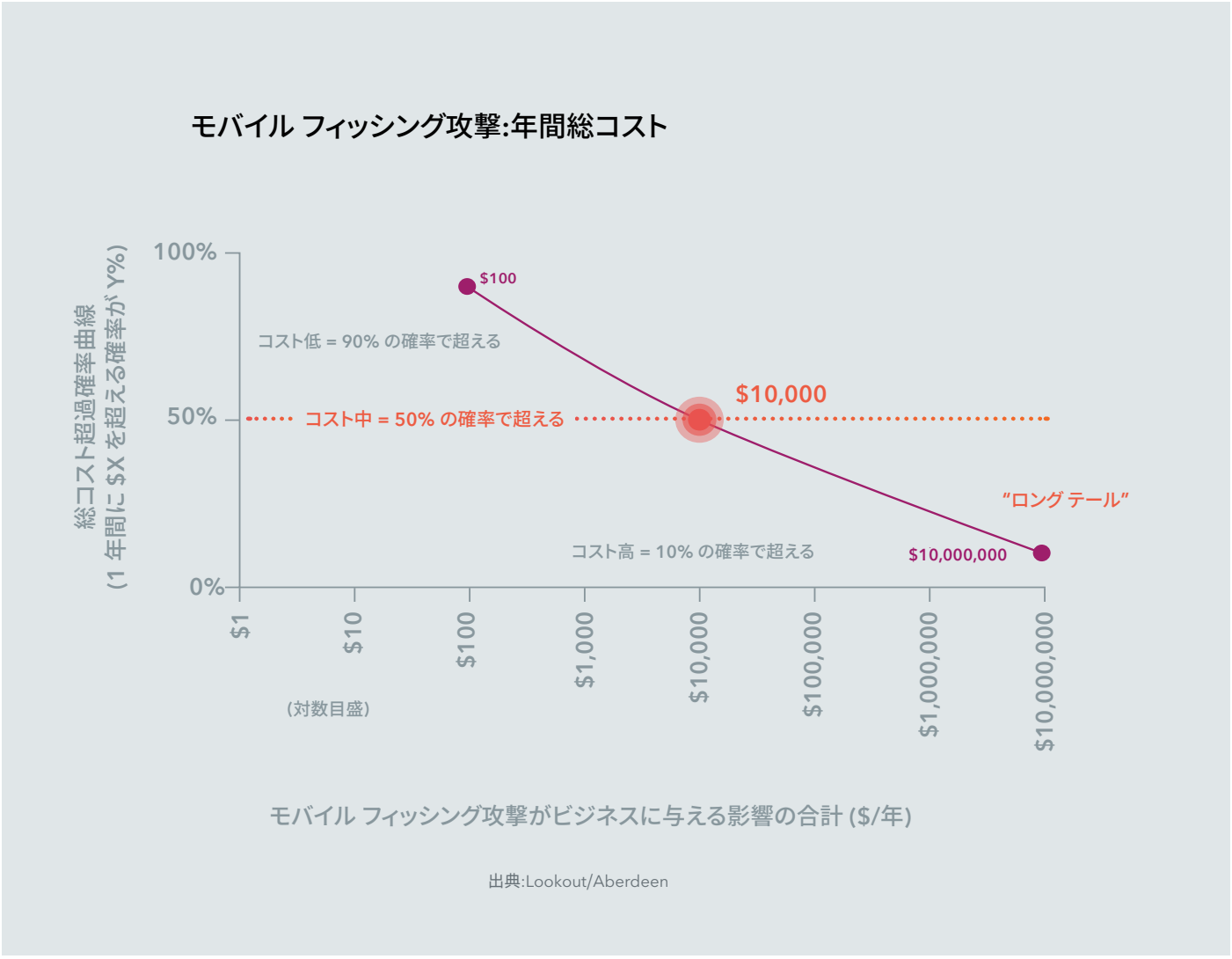
クリック数:最小: 270 | 最大:3,150 | 中央値:1,420

影響の中央値: $100,000/年

最大リスク: $35,000,000/年

例 C:中規模地域法律事務所

ここでは、1,000 台のデバイスを MDM を使わずに管理する組織を例に取り上げます。この企業には約 100 万のデータレコードがあり、100% がiOS ユーザーです。このタイプのシナリオの例は、法律事務所などの中規模のビジネスに当てはまります。従業員のほとんどはいくつかの都市を拠点としていますが、事務所、法廷、クライアントとの会議などで機密データにアクセスする必要があります。



出典:Lookout/Aberdeen

前提:1,000 台のモバイル デバイス | 100% が iOS | 1,000,000 レコード

攻撃を受ける台数:最小:20 台のデバイス | 最大:570 | 中央値:230

クリック数:最小:0 | 最大:250 | 中央値:80

影響の中央値: $10,000/年

最大リスク: $10,000,000/年

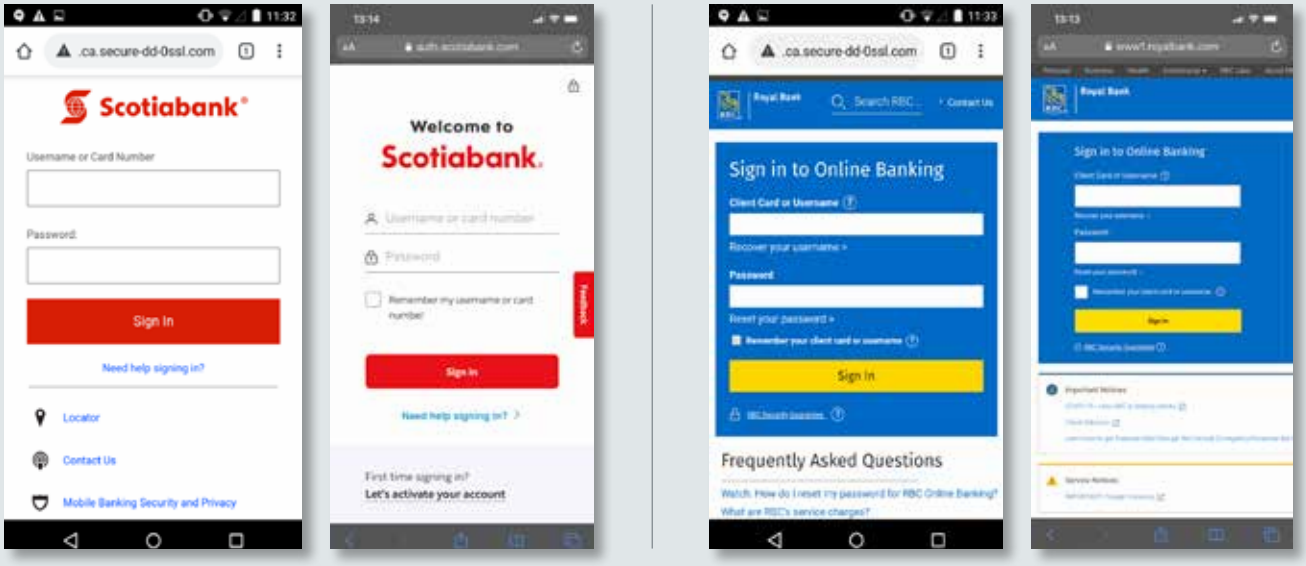
現実の世界におけるモバイル フィッシング攻撃の遭遇率に基づいたこれらの数字を見ると、たった 1 人の従業員が攻撃者に組織インフラへのアクセスを許してしまうだけで、かなりの財務的な損害が企業に及ぶ可能性があることが分かります。実際には無数のシナリオがありますが、このような攻撃の潜在的影響がどのようなものであれ、組織の成長と財務的な健全性に有害なものであることに変わりありません。

バンキング利用者を標的にしたモバイル フィッシング攻撃の実例

フィッシング攻撃は複雑さを増し、本物のメールやサイトとの見分けは年々難しくなっています。レポートの前半で説明したように、フィッシング攻撃は、初期のメールによる攻撃から長い道のりをたどって進化してきました。従業員がどこからでもデータにアクセスすることを可能にするクラウド サービスの世界的な普及により、攻撃者の手法も進化してきました。しかし、こうした悪意ある攻撃者の最終的な目的は変わっていません。それは、金銭的利得を得ることができる価値の高い情報を盗み、個人や会社に対してその情報を行使することです。

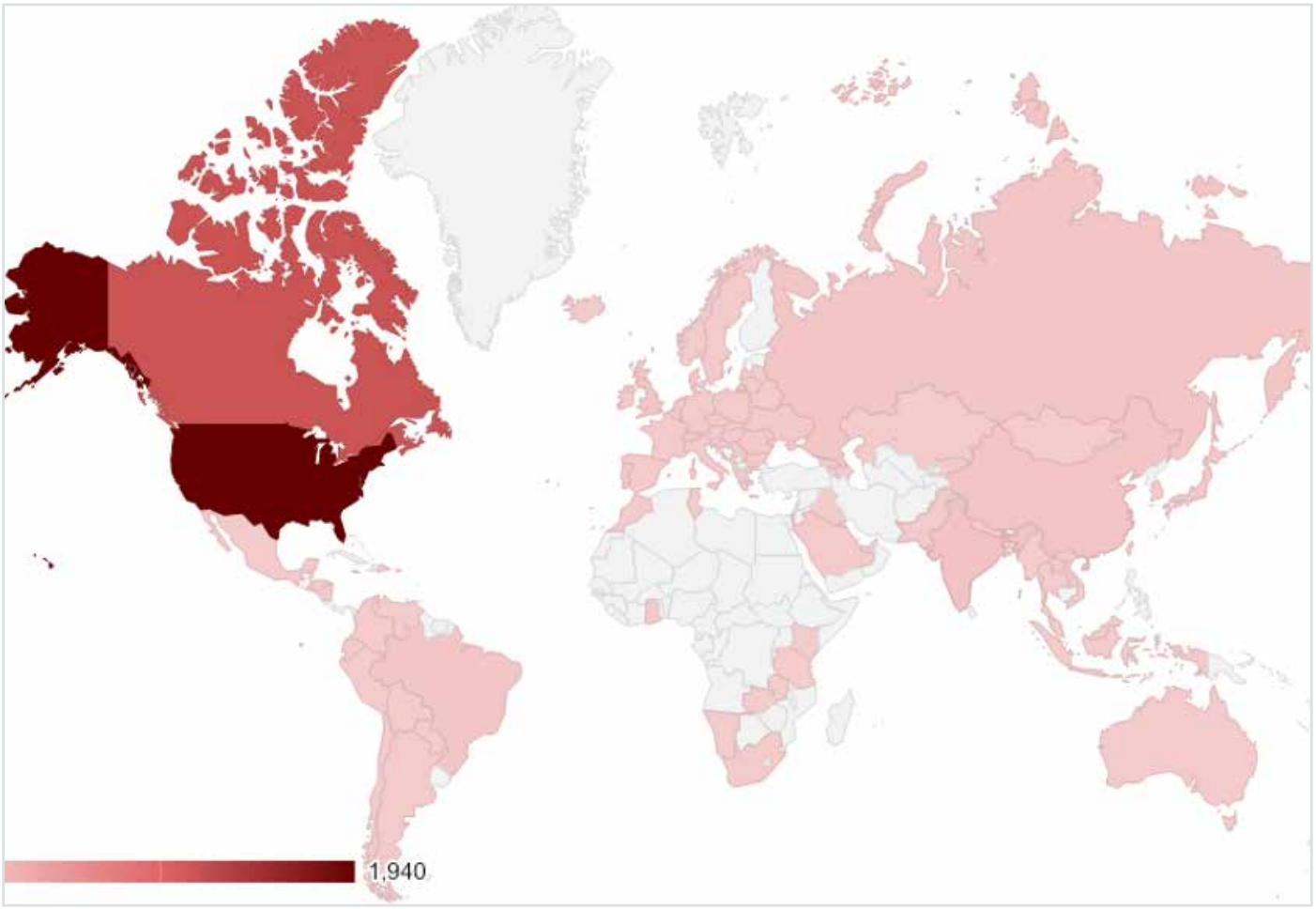
そのような中、巧妙に仕組まれた、モバイルを標的としたフィッシング攻撃の典型的な例が、2020 年 2 月に検知されました。この攻撃は、カナダの大手銀行の顧客を標的とし、受信者に自分のアカウントにログ インするためのリンクをクリックするよう求める大量の SMS を、カナダ国内の番号から大量配信しました。

受信者がそのリンクをクリックして移動したモバイル サイトは、受信者が本物のページに毎日アクセスでもしていない限り、本物のオンライン アカウント サービスの正真正銘のログイン ページのように見えました。



カナダの銀行の顧客用の、本物のログイン ページと偽物のログイン ページを並べて比較したもの。出典:Lookout

前述のスクリーンショットが示すように、顧客がこのログイン ページが偽物で詐欺を行おうとしていることに気付くことは非常に困難です。これらが偽ページであることを実際に見分けられる手段は、URL情報のみとなります。しかしログイン画面では慣れきった操作が行われることに加え、しばしばログインは煩わしい行為と見なされがちであるため、Web アドレスに注意が払われることはほとんどありません。



このフィッシング攻撃の被害者の IP ロケーションの広がりを示したヒート マップ。
7 カ月の間に、3,900 以上の異なる IP アドレスが確認された。出典:Lookout:

モバイル フィッシングを検出して保護するには

所属組織がモバイル デバイスを提供している場合であっても、BYOD を許可している場合であっても、すべての Android デバイスと iOS デバイスにフィッシング対策を実装するべきです。攻撃は誰からもたらされるか、どこで起きるかわかりません。残念ながら、攻撃がどのような形で行われるか予測する術はないため、すべての人が対策を備えておくべきです。

デバイスを監視する機能を導入していなければ、フィッシング攻撃を検出して対応することは不可能であり、まして保護することはできないでしょう。従業員の 1 人がフィッシング リンクを見つけてそれがフィッシングであると判断できた場合であっても、ほとんどの場合その従業員は単にそのメール、テキスト、もしくはソーシャル メディアのメッセージを削除して終わりでしょう。しかし代わりに、そのインシデントについて組織のセキュリティ チームに報告し、フィッシング対策戦略を強化するためにデータを提供すべきです。さらに悪いケースとして想定されるのが、実際に攻撃にひっかかってログイン情報、何らかの資金、または何であれ攻撃者が標的にしているものを彼らに与えてしまった場合、その影響が会社に損害を与えるような形で返されるまで、自分の行動の結果を認識できないということです。

モバイル フィッシング攻撃を成功させてしまうと、財務的な損失に留まらず、多大なマイナスの影響を会社に与えます。特に、金融サービス、法律、医療関係などの厳格に規制された業界では、顧客の高度な機密情報が漏洩した場合、ブランドに傷がつくことで壊滅的な影響がもたらされることもありえます。得意客の信頼を取り戻すまでには長い道のりが待っているでしょうし、規制当局から罰金が課されることもあります。その財務的損失だけでも、会社の今後の成長に致命的な影響を与える可能性があります。

組織全体を通して、目的に沿って作られたモバイル優先のセキュリティ ソリューションを導入することは、モバイル フィッシングを検出して保護する上で必要不可欠です。多くのソリューションは、伝統的なデスクトップ パソコン主体のメール フィッシング ソリューションをモバイルに持ち込んでいますが、このレポートの最初の方で考察したように、それらはモバイル フィッシング攻撃のすべてのベクトルをカバーするものではありません。さらに大切なことは、 iOS と Android を等しく保護することです。ほとんどの組織、特に BYOD を承認している組織では、両方のデバイスが混在しているからです。

また、ユーザーが監視されていると感じることを避けたいのであれば、「覗く」ことなく保護できるモバイル セキュリティのソリューションを選択する必要があります。コンテンツを検閲することなく、代わりに、悪意のあるリンクをクリックもしくは読み込んだ時にだけ警告を行ったり、悪意のある接続を自動的にブロックしたりするソリューションであれば理想的です。これらの警告によって、ユーザーは自分の閲覧習慣を自ら調整することを学び、最終的には組織全体のリスク プロファイルを抑えることにつながります。

こちらのビデオで、 Lookout Phishing and Content Protection の動作する様子をご覧ください。

詳細については、lookout.com/jp をご覧ください。