知らぬ間に被害に遭っている「フィッシング詐欺」。家計を守るために知っておきたい最新の傾向と対策とは？

POINT

偽メッセージや偽サイトを用いてユーザーを騙し、IDやパスワードを盗むフィッシング詐欺による被害が急増。巧妙化する手口への対処法は、「２要素認証」「強固なパスワード」「安易にクリックしない」が基本。

皆さんがお使いのスマートフォン。Ｓｕｉｃａやクレジットカード、○○Ｐａｙのようなｑｒコード決済。マイナポイントのアプリなど、もはや中身はお財布と変わりません。そして、オンラインショッピングなら、皆さんのお財布とお店が直結していると言っても過言ではないでしょう。また、オンライン銀行口座での振込み、株取引などの投資なども、いつでもどこでもスマホで手軽にできてしまいます。

そんな便利さの反面、一般ユーザーを狙うネット犯罪が急増しているのをご存知でしょうか？　この記事では、皆さんのスマホに届く不審なメッセージやそこから始まるネット犯罪被害の最新事情をお伝えし、皆さんの資産を守るための対策について説明していきたいと思います。

フィッシング詐欺急増！一般ユーザーの金銭被害も拡大中

皆さんがお使いのクレジットカード、最近、**不正利用による被害金額が急増している**のはご存知でしょうか。日本クレジット協会の発表によると、２０２１年度では被害総額３３０億円を超え、過去最悪となっています。その原因の一つとなっているのが**「フィッシング詐欺」による、カード番号、パスワードの窃取**なのです。フィッシング詐欺の報告件数は２０２１年度には合計約56万件と過去最高を記録しています**【図１】**。ＮＨＫの番組「あさイチ」（２０２２年９月７日放送）の中でも特集が組まれるなど、社会問題化しています。

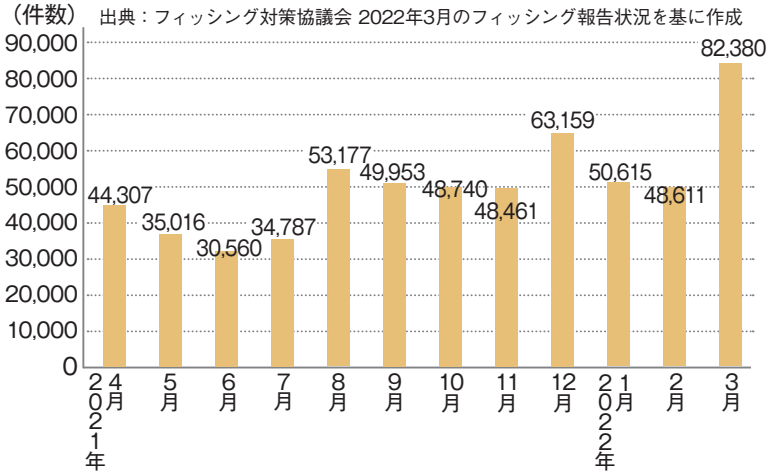
フィッシング詐欺とはどんなもの？

フィッシング詐欺は、本物そっくりの偽メッセージや偽サイトを用いてユーザーを騙し、ＩＤやパスワードを盗むネット詐欺の手口です。ルアーなど偽の餌で行う魚釣りと似ているため「Fishing」の頭の「Ｆ」を「Ｐ」に変え「Phishing」という造語が作られたと言われています。

「私なんか狙われないから関係ない」「詐欺は見抜けるから大丈夫」と考えられる方も多いかも知れません。

【図１】フィッシング詐欺の報告件数

出典：フィッシング対策協議会 2022年3月のフィッシング報告状況を基に作成



株式会社ラック
コーポレートコミュニケーション部
部長
山本 和輝
［やまもと・かずき］
外資系ソフトウェア企業数社を経て2000年よりセキュリティ業界へ。2020年にラックへ入社、広報責任者を担う。業務の傍ら一般消費者のサイバー犯罪被害防止の啓発活動、記事執筆、講演など積極的に行っている。

でも、最近の実際の手口をご覧になると、そうも言っていられなくなるかと思います。いくつか実例を紹介しましょう。

ショートメッセージ(SMS)は犯罪者にとって都合が良い

最近のフィッシング詐欺は、電子メールだけでなく、スマホのSMS（ショートメッセージ）に送られてくるものも増加しています。電話番号を指定するだけで送信できるSMSは、詐欺サイトへ誘導するメッセージを大量に送信するのに都合が良いのです。またSMSで送られてくるメッセージ文は字数が少なく、受け手が内容を判断しようとしても十分な情報がありません。そのため、表示されるリンクをタップ（クリック）してその先の詳しい情報を確認することが多いと思います。この日常の行動習慣を利用できるのも、犯罪者にとってはメリットがあるのです。

電子メールやSMSに自分が使っている有名企業の名前があれば「何かあったかな?」とメッセージのリンクを押してしまうかも知れません。そして誘導された先のログイン画面が、本物と寸分たがわないものだったら、ID、パスワードを入力してログインするのではないでしょうか。

あなたは大丈夫だったとしても、家族や友人はどうでしょうか。**自分が偽サイトにアクセスしていることに気づかないまま、ID、パスワードなど重要な情報を入力してしまっている方がとても多い**のです。

今すぐにご自分やご家族のスマホを開いてチェックしてみてください。AmazonやApple、運送会社を装ったSMSや電子メール、本人確認やパスワード変更を促すメッセージがありませんか？それは、犯罪者が無作為に大量送信した、フィッシング詐欺メッセージなのです【図2】。

フィッシング詐欺に騙されるとどうなる?

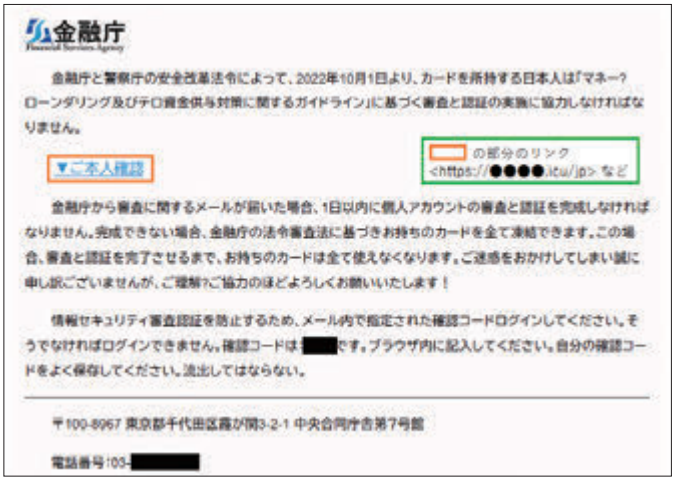
偽サイトにID、パスワード、クレジットカード番号などの重要な情報を入力してしまった場合、どんな被害が起きるのでしょうか。

ここで今一度、冒頭のクレジットカードの不正利用被害の話を思い出してください。名前とクレジットカード番号や有効期限、カード裏側の確認コードを窃取されたら、勝手に買い物をされてしまうことは容易に想像できるでしょう。

また、AmazonやRakutenなどのショッピングモールのID、パスワードであれば、本人に成りすましてログインされ、換金しや

【図2】フィッシング詐欺の例
（フィッシング対策協議会ホームページより抜粋）

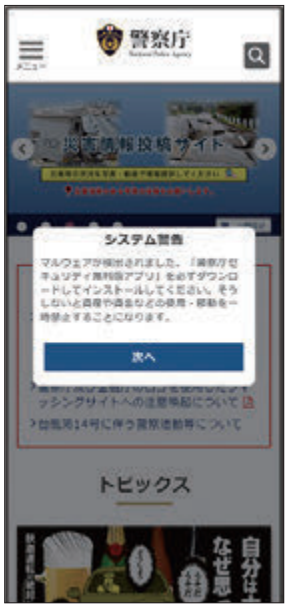
■ 金融庁を騙るフィッシング詐欺の例



■ 警察庁を装い不正アプリのインストールを誘導するSMSの例

■ 国税庁を騙りフィッシングサイトへ誘導する例

■ 警察庁を装い不正アプリのインストールを誘導する例



【図3】フィッシング対策協議会のホームページ（https://www.antiphishing.jp/）

「緊急情報」には、フィッシングメールやフィッシングサイトの実例が掲載されている。こまめにチェックしておきたい

すい高価な商品を購入されてしまうこともあります。カードの利用限度額まで、高級カメラや高額なスマートフォンなど換金しやすい商品を購入され、気づいた時には、商品は犯人の手元に配送され換金されてしまいます。

銀行のオンライン口座に不正にアクセスされたら、犯人の銀行口座へ勝手に送金されることもあります。スマホのバーコード決済なども油断はできません。犯人のスマホにアカウントを移して、お金を勝手にチャージされるなどの被害も過去に発生しました。このようなネット犯罪が本当に身近に発生し、日頃スマホを使う皆さんがターゲットになっているということが実感いただけたでしょうか。

フィッシング詐欺は儲かるのか。ネット犯罪者の実態とは？

ネット犯罪の手口で流行っているフィッシング詐欺。犯罪行為をする人たちが、どうしてフィッシング詐欺に集中しているのでしょうか。その理由の一つに、敷居の低さがあるようです。あるセキュリティ企業の調査によると、フィッシング詐欺の実行犯は1回に約300万通のフィッシングメッセージを送信していたそうです。

仮に、そのうちのわずか1%の人がID、パスワードを入力してしまった場合、3万人分の認証情報を獲得できるわけです。さらにその中の1%の人のアカウントで10万円分の不正な買い物ができた場合、単純計算で3000万円分相当の換金可能な商品を騙し取ることができます。

犯罪者にとって、パソコン1台の操作で始められる、とても効率の良いお金儲けとなります。つまり「儲かるビジネス」だからフィッシング詐欺が急激に増加しているということなのです。

フィッシング詐欺サイトの進化には目を見張るものがあります。大手銀行などのログイン画面は、フィッシング詐欺で模倣されるので、銀行は対策のためにデザイン変更を頻繁にしています。しかし、犯罪者側はすぐに最新のログイン画面のデザインを取り入れるなど、いたちごっこが続いています。

その結果、今では変な日本語表現などもほとんど見なくなり、偽メッセージや偽サイトは一見して本物と区別がつかないほどの品質になっているのです。

犯罪者は常に、私たちの一歩先の手口を用意している

「フィッシング詐欺の見抜き方をわかりやすく教えてくれないか？」

情報技術に詳しくない人向けのニュース番組を作るテレビ局などの方々からの取材では、わかりやすくポイントを教えてほしいとよく言われます。

しかし、はっきり言っておきたいことは、「見抜こうとするな！」ということです。

フィッシング対策協議会で長年啓発をやってきている専門家でさえ、「一見するだけでは偽サイトかどうかの判断はできない」と口にします【図3】。フィッシング詐欺の誘導メール、SMSも、犯罪とは関係の無いものと区別しにくいものになっているのです。

昔は「URLを確認すればわかる」「日本語が変だから騙されない」などと言われた時期もありましたが、今はもう状況がまるっきり違います。スマホのブラウザアプリ

の小さな画面で確認できるURLの文字列（ドメイン名）の最初の方を本物とまったく同じにしておき、異なる部分を見えなくしておくなど、誤認しやすいテクニックが駆使され、**犯罪者は常に私たちの一歩先の手口を用意**しているのです。

私達はどうやって対策したらよいのか？

対策については、まず、最初に次の2点を必ず押さえてください。

①2要素認証（2段階認証）を設定する

普段使わないパソコンやスマホからのアクセスがあった場合、そのアクセスが本人のものかどうかを確認するために、スマホのSMSに4桁～6桁の数字のコードが送られてくる仕組みがあります。

これは、**ID、パスワードという1つ目の要素、本人しか所持していないスマホの電話番号という2つ目の要素を使って成りすましアクセスを防ぐ仕組みで「2要素認証」**と言われています。GoogleやAppleID、Yahoo!Japan、Amazon、Facebookなど、主要なネットサービス、オンライン銀行口座などで用いられています。これだけで完璧というわけではありませんが、不正を防ぐには有効性の高い方法です。お使いの各サービスのアカウントの設定を確認して、2要素認証をONにしておきましょう。

②サービスごとに異なったパスワードを設定する

同じパスワードを複数のサービスで使いまわしていると、そのうちの1つのサービスでパスワードを盗まれたり漏えいしたりすれば、他のサービスアカウントにも不正ログインを許してしまうことになります。

これを防ぐため、IPA（情報処理通信機構）のガイドでは、以下のような条件を満たすパスワードを推奨しています。

- **最低でも10文字以上の文字数で構成されている。**
- **パスワードの中に数字や「@」「%」「“」などの記号も混ぜている。**
- **パスワード内のアルファベットに大文字と小文字の両方を入れている。**
- **サービスごとに違うパスワードを設定している。**

昔よく言われていたパスワードの定期的な変更は、対策として有効でないため必要ありません。ただし、**利用するサービスで個人情報漏えいが発生した場合には速やかにパスワードを変更**するようにします。

特に、**お金に関わる金融系のサービスは**、深刻な金銭被害に遭うリスクがありますので、**入出金、利用履歴は頻繁に確認すると良い**でしょう。

これら基本的な2つの対策を施したうえで、次の行動習慣を心がけてください。

③電子メールやSMSのメッセージ上のURLをタップしない

大手企業のおなじみの会社名、サービス名が書いてあっても、それは偽物かも知れません。書いてあるURLリンクをタップ（クリック）せず、あらかじめブックマークしておいた本物のサイトへアクセスし、ログインを行って自分のアカウント宛てのメッセージを確認しましょう。

スマホであれば、**本物のサイトへのショートカットをホーム画面上に追加**する、もしくは**専用アプリを使ってサービスへアクセス**するのが、最も安全です。

銀行や主要なネットサービス事業者は、SMSで認証コード（数字）をスマホに送ることはあっても、URL付きのSMSは送信しなくなってきています。

あらためて強調しますが、SMSのメッセージや、アクセス先の偽サイトを、URLやデザイン、日本語表記などで見分けようとしても判別がつきません。

「偽メッセージ、偽サイトを見分けようとするな！」

「SMS、電子メールは全て怪しいと考え、URLをクリック、タップしない」

これを徹底すれば、現在起きているフィッシング詐欺やネット犯罪の騙しの手口に引っかかるリスクは劇的に低くなるとお考えください。