緊急レポート

コロナ禍の今、フィッシング詐欺激増中!

フィッシング対策協議会に聞く、その手口と対策

フィッシング対策協議会

コロナ禍で外出を控える人が増えたことで、インターネット通販やオンラインバンキングなど、自宅で使えるインターネット上のサービスを利用する人が増えています。その一方で、そうした利用者を狙った「フィッシング詐欺」が広がっています。その手口と被害に遭わないための対策を、フィッシング対策協議会の吉岡 道明氏に聞きました。

Part1 フィッシング詐欺とは?

―貴協議会の役割について教えてください。

「私たちはフィッシング詐欺に関する事例の情報収集と提供を通じ、国内のフィッシング詐欺の抑制を目指し活動する任意団体です。会員はセキュリティ関係企業、またそうした詐欺にブランドを使われている企業などで構成されています」

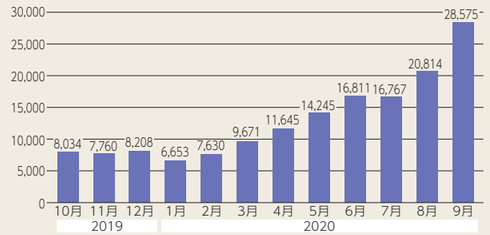
―フィッシング詐欺とはどういった詐欺なのでしょう。

「私たちは『不正アクセス禁止法』に照らし、フィッシングを定義しています。つまり実在の事業者を装って利用者にメールやSMS※1を送り、本物のサイトと誤認させてIDやパスワード、個人情報を盗み取る行為です」

―現在のフィッシング詐欺の傾向を教えてください。

「私たちは2013年から報告件数の統計を取っていますが、2015~2017年はほぼ横ばいという状況でした。ところが2018~2019年にかけて増加ペースが上がり、2020年は9月末時点でも昨年の報告件数の2.5倍近くになっています(図1参照)。これはコロナ禍により在宅勤務を行う人、ECサイト(オンラインショッピングサイト)を使う人が多くなり、そうした人がターゲットとして狙われるのではないかと推測しています」

【図1:過去1年間のフィッシング報告件数】

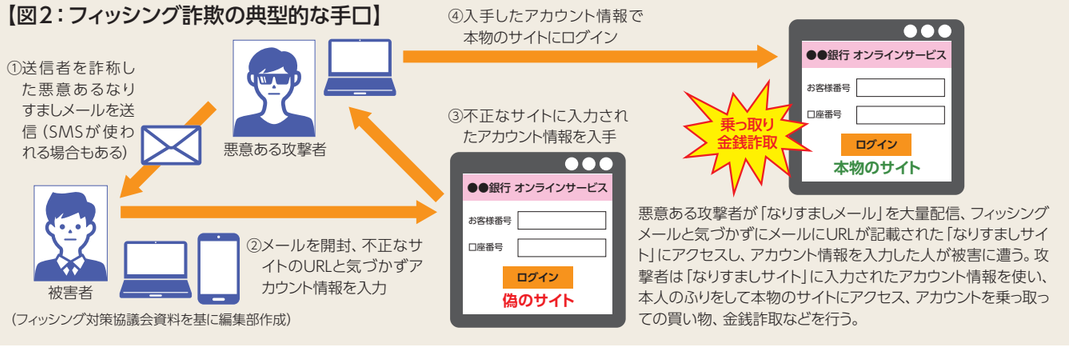


フィッシング対策協議会への報告件数は右肩上がりに伸びている。また年ごとの集計でも2017年の9,812件が2018年には1万9,960件、2019年には5万5,787件。今年は9月までに13万2,811件とさらに激増している。(出典:フィッシング対策協議会)

―具体的な手口にはどのようなものがありますか。

「ECサイトや金融機関、カード会社を騙るメールで偽サイトに誘導し、IDやパスワード、個人情報(氏名、住所、電話番号)、クレジットカード情報などを盗み取る手口がほとんどです(図2参照)。また宅配便を装い、不在通知のSMSをスマートフォンに送信し、不正なアプリをインストールさせる手口もあります」

【図2:フィッシング詐欺の典型的な手口】



(フィッシング対策協議会資料を基に編集部作成)

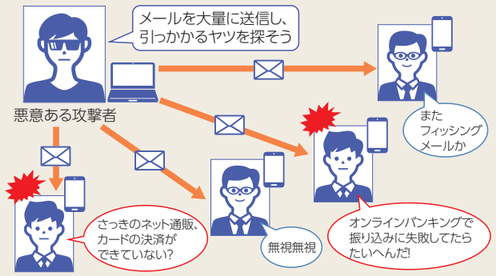
悪意ある攻撃者は膨大な数のフィッシングメールを送信する。そのメールを受信した人の中に一定数含まれる「オンラインバンキングで仕事関係の入金をしたばかり」とか、「ネット通販でカードを使い買い物した」といった人が、あまりのタイミングのよさに本物と信じてクリックしてしまい、被害に遭うケースが多い。

Part2 なぜ騙されてしまうの?

―そうした手口にどうして騙されてしまうのでしょうか。

「一つはスマートフォンの普及です。スマートフォンは画面の表示エリアが狭く、送信者名やメールアドレス、偽サイトのURLが見分けづらくなっています。そのため本物のメールと誤認して、アクセスしてしまうのです。次に手口の巧妙化です。最近はフィッシングメールも偽サイトも本物をコピーして作られ、一目では見分けられないものも多くなっています。さらにもう一つ、理由として考えられるのは、『自分が行った操作』との関連づけです。例えばECサイトで買い物をした直後、オンラインバンキングで振り込みを行った直後にエラーメッセージを伝えるフィッシングメールが着信して、そのタイミングのよさからうっかり信じてしまうパターンです。特にECサイトでは、Amazonや楽天など、利用者が多いサービスが、こうした詐欺の主な標的になっています」

【図3:"偶然のタイミング"に罠がある】
～フィッシングメールに騙される理由とは～



―送信者は、そうした利用者の行為を知ってフィッシングメールを送るのですか。

「いいえ、そうではありません。詐欺を働く人物は、不正に得た大量のメールアドレスに同じ内容のメールを送信します。大手ECサイトは利用者も多いため、受信者のうち何人かにはそうした"絶妙なタイミング"で着信することになるわけです(図3参照)。またメールの多くには『アカウントをロックします』など行動を急かす文言が含まれ、受信者を慌てさせ、正常な判断を妨げる細工も行われています」

Part3 有効な対策とは?

―このようなフィッシングメールや偽サイトを見破る有効な手段はあるのでしょうか。

「かつては『メールのここを確認しましょう』といった"見破り方"が推奨されていた時期もありましたが、現在のフィッシングメールは、そうした方法では見分けがつかないものが多くなっています。また簡易なドメイン認証(DV)を取得し、ブラウザのアドレス部分の左に『錠前マーク(SSLサーバー証明書)※2』を表示させる偽サイトが当たり前のように登場しています。錠前マークをクリックすると『この接続は保護されています』というメッセージが出てきますが、偽サイトかどうか、それだけでは判断できないのです」

―では、騙されないためには、どのような対策が必要でしょうか。

「まずは慌ててメールにあるURLをクリックしないことです。ブックマークにある正しいURLからアクセスする、スマートフォンであれば正式なアプリからアクセスして状況を確認し、もし疑問点があったらそうした正しいサイトから問い合わせましょう。そしてほとんどの場合、正しいサイトが『本人確認のため』と称してカード情報、口座情報を入力させることはないということも覚えておくといいでしょう。また私たち協議会のウェブサイトでは『利用者向けフィッシング詐欺対策ガイドライン』を公開しています。ぜひこちらもご覧いただきたいと思います」

Point 騙されないための心得
「STOP.THINK.CONNECT.」

STOP:立ち止まる	THINK:考える	CONNECT:楽しむ
急かすようなメール、警告メールにも慌てず、いったん立ち止まる	クリックしたらどうなるか、何が起こるか、調べたり考えたりする	そして安全だと判断できたら、インターネットを楽しむ

フィッシング対策協議会も周知に力を入れる心得が、この「STOP.THINK.CONNECT.」という全世界共通のサイバーセキュリティキャンペーン。うっかりクリックしたことで取り返しのつかない被害を生み出さないよう、立ち止まり、何が起こるか考えてからインターネットを利用したい。キャンペーン内容について詳しくは公式サイト(https://stopthinkconnect.jp/)を参照。

※1 SMS:ショートメッセージサービスのことで、携帯端末間で「テキスト」をやり取りできる仕組みのこと。
※2 錠前マーク(SSLサーバー証明書):信頼できる第三者機関(認証局)が発行する電子証明書で、アクセスしているサイトが「認証局によって認められた正当なサイトである」ということを証明するもの。

吉岡 道明氏
フィッシング対策協議会事務局
一般社団法人JPCERTコーディネーションセンター
エンタープライズサポートグループ
リーダー
シニアアナリスト

フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシング詐欺に関する事例の情報収集と提供を通じ、国内のフィッシング詐欺の抑制を目指して活動する任意団体(2005 年4月発足)。会員はセキュリティ関係企業をはじめ、詐欺にブランドを利用されている企業などで構成されている。

ユーザ協会 D10005 検索