「自分は大丈夫」、ではないフィッシングと不正送金による被害

不審なメールが増えたと感じている人が多いのではないでしょうか。私のところにも毎日、多いときには10 通以上の不審メールが送られてきます。うっかりクリックすると経済的な被害も発生しかねないので、どのような犯罪手口と対処法があるのか知っておく必要があります。

●なりすましによるフィッシング

不審メールは大手企業や金融機関になりすましているものが多く、一目で「怪しい！」と気づけるものが多いものの、中には一見してわからない精巧に作られたものもあるため、注意が必要です。メールに添付されているファイルを開いたり、メール本文内に記載されている URL をクリックしたりすると、個人情報が流出するなどの被害を起こすマルウェア（ウィルス、トロイの木馬、スパイウェアなど悪意のあるソフトウェアの総称）に感染させられます。html 形式で書かれたメールの中には、開封せずプレビューしただけで感染するマルウェアが仕込まれている場合もあるようです。

また、記載された URL をクリックすることにより、偽の銀行サイトや通販サイトなどに巧みにおびき寄せられ、偽のログイン画面によって個人情報、ユーザーID、パスワード、銀行の暗証番号、クレジットカード情報などが盗まれます。「フィッシング」という手口ですが、引っかかると盗まれた情報が使われて銀行預金が不正送金されたり、クレジットカードが不正利用されたりと、経済的な被害が発生してしまいます。

パソコンだけでなく、スマートフォンの SMS（ショートメッセージ）にもなりすましメールが送られています。平成 29 年版の『情報通信白書（総務省）』を見ても、2016 年にはインターネット利用者に限ったスマートフォン利用割合が 71%となっているように、特に 40 歳代以下の若い世代ほど、パソコンよりスマートフォンを使ってインターネットを利用する傾向にあります。

SMS での簡潔な文面にリンクが張られていたら、気づかずタップしてしまいかねないので、手軽なだけにスマートフォンの扱いにも慎重さが必要です。

●不正送金の最近の手口

インターネット専業銀行であるジャパンネット銀行のサイバーセキュリティ対策室の方から、お話を聞く機会がありました。ここ 2 年ほど多数の銀行で被害が発生しているのが「ヴィッシング（ボイスフィッシング）」という手口で、主に高額預金者や極度額上限の大きいローン利用者がお金を持っているとみなされ、ターゲットになっているとのことです。

ヴィッシングとは、不正入手したログイン情報を元に電話番号を調べ、コールセンターの担当者であることを疑わせない言葉遣いの電話の架け子が、たとえば顧客に配布されているトークンで随時更新されるワンタイムパスワードなどの情報を聞き出し、不正送金するという手の込んだ手口です。

犯罪者が役割分担し組織化しているのは、振り込め詐欺だけでないということで、今後もますます手口が巧妙化すると思われます。オンライン取引に慣れている人も騙されているようですから、「自分は大丈夫」と決して思わないことが大事です。

●セキュリティ対策と補償

もちろん銀行も不正送金対策を行っており、たとえばジャパンネット銀行の場合は、カード型トークンによるワンタイムパスワードを導入しているほか、顧客の端末のマルウェア感染を検知したら振込限度額を 0 円に更新、なりすましの不正ログインを検知したら不正 IP アドレスをブロック、といったシステム環境にしています。

一方、利用者も自分でできる対策を講じなければなりません。驚いたことに、オンライン取引を日常的に行う人のなかにも、ウィルス対策を全くしていない人もいるそうです。ウィルスソフトが最新状態であれば、マルウェアはまず駆除されるので、感染による被害も避けられます。

もし不正送金被害に遭った場合、銀行に 30 日以内に申し出るなどの要件をクリアしていることを前提に、過失がなければ全額補償してもらえます（銀行により年間上限額があるなどの規定があるので取引先の条件を要確認）。

また、ウィルスソフトを使っていないなど個人でやるべきセキュリティ対策が不十分だと、軽度の過失ありとして補償の減額対象になるケースもあります。今一度セキュリティ対策を見直しましょう。

（クルー　浅田里花）

【パソコン・スマートフォンの個人でできるセキュリティ対策】

- ウィルスソフトをインストールし、いつも最新状態にアップデートする。
- OS やアプリの更新プログラムをいつも最新状態にアップデートし、脆弱性を突かれないようにする。
- 不審なメールに添付されているファイルを開いたり、本文内の URL をクリックしない。
- html 形式で書かれたメールがテキスト形式に変換されて受信するよう設定しておく。
- ログインする場合は、必ずそのネット銀行、ネット証券、通販会社などが運営するサイトから行う。
- 重要な情報の入力画面が「SSL 通信（URL の頭が https）」で、鍵マークがついているか確認する。
- ポップアップ画面に入力する場合は、いつもより入力項目が増えているなど不審な点がないか注意する。

クルーレポート 第747号 2018年10月20日

生活設計塾 CLUE
発行 生活設計塾クルー http://www.fp-clue.com/ 〒112-0001東京都文京区白山5-1-3 東京富山会館7F TEL:03-5805-2050 FAX:03-3815-3755