第８００号
2019年11月23日
無許可転載禁

クルーレポート

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
毎月第1～4土曜日発行　月額1,650円(税込)

この秋急増している不正送金被害、その手口と対策は？

私たちの生活を大きく変えた IT。金融サービスでも IT を取り入れたフィンテックが広がりつつあります。ネットバンキングもそのひとつ。しかし、馴染みの薄いサービスを使うのに抵抗を感じる人が多いのも事実です。大事なお金に関することだけに、不正利用被害への不安もあります。不正利用を防げるのか、ジャパンネット銀行の話を聞く機会がありました。

●最近の手口は「スミッシング」

警察庁によると、この 9 月からインターネットバンキングにかかわる不正送金の被害が急増している模様。今年 1 月から 6 月までの半年で発生した件数が 183 件、被害額は約 1 億 6600 万円だったところ、9 月だけで発生件数 436 件、被害額は約 4 億 2600 万円にのぼっています。2012 年以降で最多の発生件数、被害額は 2 番目に多い水準とのこと。その原因として、2019 年に入ってからメガバンクを中心にフィッシングサイトが継続的に発生し、ネット銀行にも拡大していることが挙げられます。

「フィッシング」とは、あたかも釣りを行うように、実在する金融機関や企業になりすましてｅメールなどを送りつけ（餌をまく）、正規のウェブサイトそっくりに作成した偽サイトに誘導し（食いつきを待つ）、ID やパスワード、クレジットカード番号などの個人情報を入力させる（釣り上げる）犯罪行為のこと。ID やパスワードを犯罪者が知れば、本人同様にログインできますから、簡単に不正送金されてしまいます。

手口も多様化しており、「マルウェア」と呼ばれる悪意のあるプログラムやソフトウェアを感染させる手口、銀行員などを装って電話で認証情報などを聞き出す「ヴィッシング（ボイスフィッシング）」などがあり、最近では「スミッシング（SMS フィッシング）」と呼ばれる手口が急増しています。これは、スマートフォンの SMS（ショートメッセージサービス）になりすましてメールを送りつけ、不正サイトに誘導する手口。不在配達を連絡する宅配業者や、本人認証を求める携帯電話会社を装ってのショートメッセージを受け取ったことはないでしょうか。これらには手続き先として不正サイトの URL が記載されており、クリックさせて認証情報を入力するように誘導します。ネットバンキングを行う銀行を装ってのスミッシングも増えてきており、本人認証だけでなく、ワンタイムパスワードなどの二段階認証情報をも入力させるフィッシングサイトが用意されているという巧妙さ。そのため、不正送金の被害が拡大しているというわけです。

●ログインは常に正規サイトから

被害に遭うのを防ぐには、まず受信したショートメッセージの内容や URL をよく確認することです。日本語が不自然だったり、明らかに金融機関や企業のサイトと無関係の URL だったりすればスミッシングを疑いましょう。ショートメッセージが本物の金融機関・企業から送られてくる場合もありますが、慌ててクリックせず、常に正規のサイトからログインする慎重さが必要です。

不正サイトの URL をうっかりクリックしてしまった場合、スマホに登録してある電話番号へと SMS 送信するウィルスに感染するケースも出ています。知人からのショートメッセージなので油断してクリックすると、登録先に SMS 送信され被害の芽が増殖していきます。自分が被害を防がなかったことで、知人にも被害が広がっていくことになります。送信者が信頼できる人であっても、ショートメッセージに記載されている URL のクリックは慎重にしたほうがいいでしょう。思い当たることがあればスマホのアプリをチェックし、インストールした覚えのないアプリがあるようならアンインストールしておくことです。

●カード番号の流出に注意

なかなかキャッシュレス化が進まない日本ですが、10 月から消費増税に伴うポイント還元制度がスタートし、クレジットカードを使う機会が増えたという人も多いでしょう。しかし、（社）日本クレジット協会の調べによると、クレジットカード不正利用被害は年々増加しており、2014 年の被害総額 114.5 億円から、2019 年は1～6 月の半年で 137 億円となっています。そして、その 81.7%がクレジットカード番号盗用被害。フィッシング等で盗まれたカード番号が、闇サイトで取引されていることも被害を拡大しています。

残念ながら、カード番号の不正利用を完全に防ぐ対策はないとのこと。被害を最小限に防ぐためにできる対策として、まずは不審なサイトでカード番号の入力を行わないようにしましょう。ネットショッピングは信頼のおけるサイトでなければ止め、楽天など大手 EC サイトでも検索結果からリンクを辿るのは避けたほうが賢明。偽サイトに誘導される可能性がゼロではないからです。お店で使う際は、カードから目を離さないようにしましょう。目の届かないところや、うっかり目を離した隙に、小型スキャナ等でカード情報を盗まれるかもしれません。カードの利用限度額が高額であれば、適切な額に引き下げておくのも手です。海外旅行などで枠が必要な場合は、ちょっと面倒ですがそのとき引き上げればOK。月々の利用明細には必ず目をとおし、不正利用がないかチェックすべきなのは言うまでもありません。

（クルー　浅田里花）