フィッシング詐欺の現状と対策とは？

フィッシング―インターネット版「振り込め詐欺」「おれおれ詐欺」

Q このたび、いつも利用している銀行からメールが送られてきました。「セキュリティのため、パスワードを更新してください」と書かれており、メールに書かれていたURLをクリックすると、いつも見ている銀行のURLと違うサイトであることに気がつきました。どのように対処したらよいのでしょうか。

A 警視庁ハイテク犯罪対策総合センターによると、本年五月二十九日、中学三年生（一四歳）がゲーム会社の偽サイトを作成し、他人のIDやパスワード、メールアドレスを盗み取っていたことが判明しました。フィッシング詐欺事件では最年少の摘発者であり、同センターは、著作権法違反と不正アクセス禁止法違反の容疑で書類送検します。

以下では、フィッシング詐欺の手口と対策について説明します。単純な仕組みであり、前述のように中学生でも行える技術ですが、巧妙に人を騙す手口はインターネット版「振り込め詐欺」「おれおれ詐欺」とも呼ばれます。

1 フィッシングとは

フィッシングは、銀行やクレジットカード会社などの金融機関や大手ISP事業者、ECサイトを装って、大量にメールを送りつけ、メール本文にURLを記してクリックさせ、偽のサイトへ誘導し、IDやパスワードなどの個人の金融情報等を盗み取る詐欺行為です。

フィッシングとは、もともと「釣り」を意味する「fishing」が語源ですが、偽装の手口が巧妙かつ洗練されている（sophisticated）ことから、「phishing」と呼ばれています。

2 フィッシング詐欺の手口

フィッシング詐欺の手口は、次のとおりです。

(1) 大量メールの送信

無差別に送りつけるスパムメールを大量に送付します。メール本文には個人情報を入力するよう促す案内文と、Webページへのリンクurlが記述されています。案内文には、「パスワードの有効期限切れのため」とか、「セキュリティのためID／パスワードの更新を行ってください」などと、人の心の隙間をついて、メールに書かれているURLをうっかりクリックさせます（ソーシャルエンジニアリング）。

聞き出そうとする個人情報は、クレジットカード番号、キャッシュカード番号、暗証番号、住所、氏名、電話番号、プロバイダ・電子メール等のID／パスワードです。

(2) 偽サイトへ誘導

メールの「送信者名」を金融機関窓口などの表記にし、メール本文に記述したURLをクリックさせ、偽のサイトへ誘導します。リンクURLをクリックすると、その金融機関の正規のWebサイト（本物）と、個人情報入力用のポップアップウィンドウ（偽物）が表示されます。

また、URLに使用される書式を利用して、あたかも本物のドメインにリンクしているかのように見せかけたり、ポップアップウィンドウのアドレスバーを非表示にしたりしている手口もあります（スプーフィング）。

近時はブログ内のトラックバック機能を用いて、偽サイトへ誘導する手口もあります。

(3) 個人の情報などを盗取

本物を見て安心したユーザーがポップアップに表示された入力フォームに暗証番号やパスワード、クレジットカード番号などの金融情報を入力し、送信すると、犯人に情報が送信されます。

3 対策

前述したように、フィッシング詐欺は、メールやブログなど、テキストで記述された普通のメールやトラックバックから忍び入ります。添付ファイルやHTMLメールで送付される場合ならウィルスソフトが検知してくれますが、そうはいきません。

これは人の心の隙間をつくソーシャルエンジニアリングによるものであり、利用者のより一層の注意が必要となります。

(1) 予防策

次の諸点に注意してください。

①メールヘッダの確認

メールヘッダには送信者名（自称）を示す「From」項目のほかに、経由したSMTPサーバーを示す「Received from」という項目があります。

完全ではありませんが、安易なフィッシングメールであれば、これで送信者を詐称しているか否かがわかります。

②本物サイトの「お知らせ」を確認

銀行・クレジットカード会社が、個人情報の登録・修正依頼をメールで行うことは皆無です。

そのようなメールが届いた場合は、ブックマークからいつも利用している銀行・クレジットカード会社のホームページのお知らせを確認するか、直接、問い合わせを行ってください。

③URLを確認

一般のホームページのURLは「http://～」から始まっています。しかし、銀行やクレジットカード会社のログイン画面、特に個人情報の入力を求めるメニューはSSLといって、暗号化がかけられています。

URLを確認し、「https://～」となっていることを確認してください。

④鍵マークの確認

銀行・クレジットカード会社のログインメニューやパスワードを求めるメニューには、ブラウザの画面の右下部分に「鍵マーク」がついています。このマークの存在を確認してください。

(2) 警察の取り組み

警察庁では、今後、増加が懸念されるフィッシング詐欺について、関係機関・団体と連携し、詐欺の被害が発生する前の段階でフィッシング行為の防止を図るとともに、フィッシング行為自体を業務妨害罪、著作権法違反などで検挙するよう努めています。

具体的な施策として、全国の都道府県警察において、フィッシング事案に関する情報提供を受け付ける「フィッシング一一〇番」を設置し、提供された情報をもとにフィッシング行為の取り締まりを強化しています。

次のような場合は、サイバー犯罪相談窓口（http://www.npa.go.jp/cyber/soudan.htm）にご連絡ください。

① フィッシングをしている偽のホームページを見つけた場合
→ホームページのアドレスを連絡する。

② フィッシングと思われるメールが送付された場合
→メールの題名、内容、リンク先などを連絡する。

③ フィッシングの被害に遭ってしまった場合
→被害の状況について連絡する。