ニューノーマル処方箋（第35回）

被害拡大中「フィッシング詐欺」の防ぎ方

2024.02.27

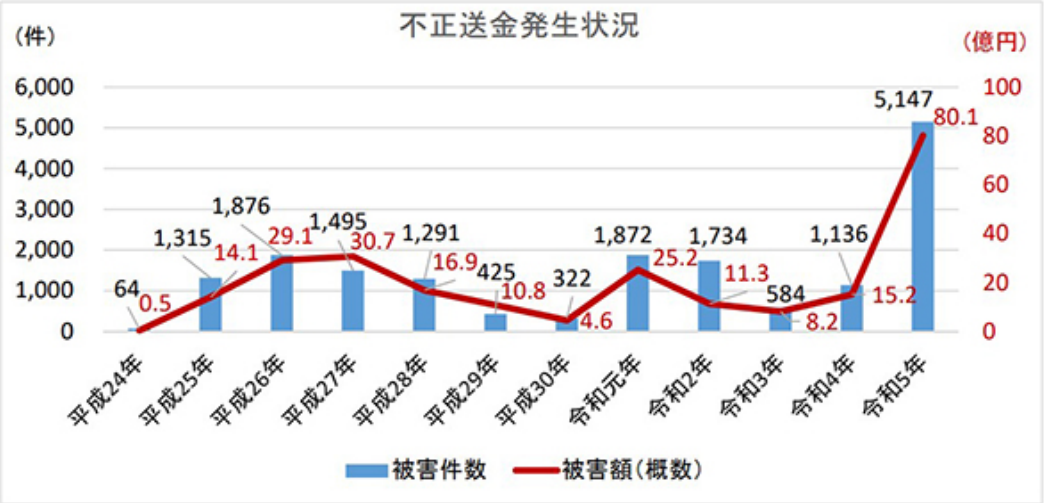
＜目次＞

2023年のフィッシング被害額は80億円を突破

「フィッシング詐欺」とは、偽のメールや偽のサイトを利用したサイバー犯罪です。有名な企業や通販サイトをかたったメールでユーザーを偽サイトに誘導し、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、データを盗み取る詐欺のことをさします。

フィッシング詐欺の被害抑制を目的とした組織「フィッシング対策協議会」の調べによると、2023年に同組織に寄せられたフィッシングの報告件数は合計119万6390件で、これは2022年の96万8832件よりも20万件以上高い数値です（数値は海外含む）。

金融庁の調査によると、最近は特にインターネットバンキングの利用者のID・パスワードがフィッシングによって盗まれ、預金が不正に送金される手口が多発。2023年の被害件数は5147件で、被害額は約80.1億円に及んでいます。この数値は11月末時点のものですが、いずれも過去最多を更新しているといいます。



なおフィッシング詐欺の「フィッシング(Phishing)」とは、「釣り(Fishing)」と「Sophisticated(洗練された)」を組み合わせた造語であると言われています(総務省のサイトより)。

フィッシング詐欺は、どのような手口で個人情報を盗むのか？

フィッシング詐欺の手口は、基本的にはユーザーに個人情報を入力させる「フィッシングサイト(偽サイト)」と、フィッシングサイトへユーザーを誘導する「フィッシングメール(なりすましメール)」がセットとなっています。

多くのフィッシングメールには、タイトルや本文に「重要なお知らせ」「あなたのアカウントに不正アクセスがありました」といった、クレジットカード会社や銀行からの通知メールを装い、フィッシングサイトへのURLが記載されているケースが多く見られます。

Eメールのフィッシングメールの場合、送信元のアドレスをよく確認すると、アドレスがデタラメな表記であることが多く、なりすましであることは比較的判別しやすいです。しかし、携帯電話の番号だけでメールが送れるSMS(ショートメッセージサービス)のフィッシングメールの場合、偽物か否かを見分けるのは困難です。こうしたSMSを活用したフィッシング詐欺は「スミッシング」と呼ばれます。

フィッシングメール内のURLを誤ってクリックすると、フィッシングサイトへ遷移します。たとえフィッシングサイトを訪問したとしても、基本的にはIDやパスワードなどを入力しない限り、大きな問題はありません。すぐにブラウザーを閉じれば、個人情報が盗み取られる可能性は低いようです。

ただし、フィッシングサイトは本物のサイトをそのままコピーしたものが多いため、場合によっては本物のサイトと勘違いすることも十分に考えられます。ここでフィッシングサイトに個人情報を入力してしまうと、その情報は悪意のある第三者の手に渡り、悪用される恐れがあります。

フィッシング詐欺を防ぐために必要なこととは… 続きを読む