小さな会社のトラブル抑止（第5回）

偽サイトにご用心。インターネットの落とし穴

2018.03.12

ユーザーが簡単に見分けられないほど巧妙に作られた「偽サイト」が、社会問題になっている。オンラインショップや銀行の偽サイトにアクセスしてしまい、不正送金や詐欺の被害に遭うケースも急増中だ。インターネットの利便性を逆手に取った犯罪からいかにして身を守るか、対策の抜本的な見直しが求められている。

銀行、通販、保険。偽サイトの最新手口



2017年7月、ウイルス対策ソフト大手のトレンドマイクロから、警察庁のサイトを偽装したサイトを確認したという発表があった。その偽サイトには「違法なコンテンツを閲覧したことを確認したのでパソコンをロックした。違反金として50000円支払え」などと記載されていた。

支払い方法が電子マネーのみであることや「違反金」という表現など、冷静に考えれば疑わしい部分は多いのだが、Webブラウザーの全画面表示機能を悪用してURLも偽装し、一見すると正規サイトかと勘違いしてしまう。また、慌ててブラウザーの「閉じる」ボタンをクリックしても、偽装されたボタンなので反応はなく、画面は表示されたまま。ユーザーの心理を突いた巧妙な詐欺サイトだ。

このような偽サイトを使った犯罪は「フィッシング（Phishing）」と呼ばれる。この名前は英語の「釣り（Fishing）」と「洗練（Sophisticated）」を合わせた造語だ。インターネットの利用が本格化した2000年代に急増し、現在もその勢いは止まらない。

フィッシング詐欺の手口は、文字通り釣りと似ている。犯人はまずメールという「まき餌」を大量に送信。魚（被害者）はまき餌を食べて（メール記載のURLをクリックして）仕掛け（偽サイト）に近づき、釣り上げられる。手法自体は広く知られているにもかかわらず、いまだに被害が後を絶たないのはなぜか。そこには仕掛けとなる偽サイトの進化が関係する。

ユーザーを誘い込む方法も巧妙化している。「アカウントの有効期限が切れています。更新してください」といったメールを送り、本文に記載されたURLをクリックさせる事例では、メールの発信元に実在する企業、組織名を明記し、画面も実在のサイトに酷似したものが多い。実際に、ある大手銀行の偽サイトは本物とほとんど見分けがつかず、銀行側の発表でも「入力欄が2つのサイトは本物で、3つ以上のものは偽物」というありさまだった。

さらに最近は、スマートフォンのSMS（ショートメッセージサービス）を使って偽サイトへ誘導する「スニッシング」と呼ばれる手口も現れた。2017年7月には日本でもGoogleを装ったSMSを送り、ウイルス対策費と称し金銭をだまし取ったとして容疑者が逮捕された。

お金も顧客情報も失う… 続きを読む