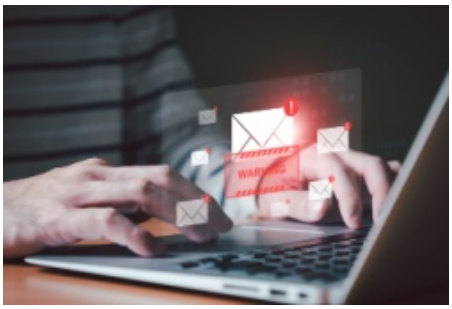
事例で学ぶセキュリティインシデント（第20回）

インシデントは思いがけないところから。偽メールに要注意

2025.01.14



関西で戸建て住宅などの建設業を営むT社。支店の女性社員から本社のIT担当者に電話がかかってきた。「取引先からのメールだと思い、添付ファイルを開いてしまったのですが、大丈夫でしょうか」。メールの内容は、取引先の事務所が移転したとの連絡で、移転先の住所や電話番号、URL、地図などは添付ファイルを参照するように書かれていた。女性は添付を開いたものの、心配になって本社に電話をしてきた。IT担当者はその取引先に電話連絡したところ、移転の予定もなく、メールも送っていない。IT担当者は役員に報告するとともに、全社員に不審なメールを開かないように注意喚起した。

フィッシングサイトにひっかかり誤って個人情報を入力

そもそも、本社の営業部門や管理部門ではなく、どうして支店の女性社員に取引先をかたる不審なメールが届いたのか。IT担当者は女性社員に思い当たることはないか尋ねた。女性社員が記憶をたどると1週間ほど前、おかしなことがあった。いつも、使っているショッピングサイトから顧客情報の更新の連絡がスマートフォンに届いた。女性社員は何の疑いもなく、記載されていたリンクにアクセスして住所や氏名、勤務先、クレジットカード情報などの個人情報を入力してしまったという。

近年、サイバー攻撃の中で増えているのがフィッシングだ。対象が主に個人であることから、企業・組織にとって直接的な攻撃であると認識されにくいが、フィッシングのメールやメッセージ、SNSを受け取ったことのある人は少なくないはずだ。

一般の人が取引していそうな金融機関や電力会社、通信会社、クレジットカード会社などの名をかたり、正規のWebサイトをまねた偽のサイトに誘導して個人情報やクレジットカード情報、認証情報などを入力させる。攻撃者はその情報を悪用して物品を購入、転売して金銭を得たり、個人情報をダークサイトで販売したりして利益を得る。かつて、フィッシングサイトに誘導する日本語もおかしな言い回しが目立ったが、近年はAIを使って流ちょうな日本語になり、本物そっくりの偽サイトをつくり、だまされやすくなる傾向にある。文中に記載されたURLをクリックしてフィッシングサイトに誘導する他、QRコードを悪用してサイトに誘導するものもあり、フィッシングの手口も巧妙化している。

IT担当者は女性社員の話を聞いて、おそらくフィッシングサイトに記載した勤務先名が攻撃者に悪用され、不審なメールが

送られてきたと推察した。ただ、女性社員は添付ファイルを開いたものの、記載されていたURLをクリックすることなく、IT担当者に連絡してきたため、ウイルス感染被害は免れた。そして、IT担当者は女性社員にクレジットカード会社へ連絡して、事情を説明するようにアドバイスした。

業務に関係のある内容に偽装し添付ファイルを開かせる… 続きを読む