日頃利用している事業者からのメールもフィッシングを疑って

実在する事業者をかたるメールや SMS を送信し、そこに記載された URL をクリック等させ、偽のウェブサイトに誘導することで、パスワードやクレジットカード番号などを詐取するフィッシング詐欺に関する相談が依然として寄せられています。日頃利用している事業者や公的機関などのメールや SMS であっても、まずはフィッシングを疑いましょう。

事例を紹介します

・ 普段から利用しているアプリの名前でスマホにメールが届いた。「登録している支払い方法に確認が必要な状態」「更新が遅れるとストアでアプリが購入できなくなる」などと書いてあったので、記載の URL からアクセスして、クレジットカード番号等を入力し支払い情報を更新した。ところがその後、ネットショッピングで約 20 万円の利用を知らせるメールが届いた。どうしたらよいか。（80 歳代）

記載されている URL にはアクセスせず、事前にブックマークした正規サイトの URL や、正規のアプリからアクセスしましょう。リンク先にアクセスしてしまっても、クレジットカード番号などは入力せず、そのサイト上にあるアプリもダウンロードしないことが大切です。

不正利用に早く気づけるように、クレジットカード等の明細は、こまめに確認しましょう。

困ったときは、お住まいの自治体の消費生活相談窓口にご相談ください（消費者ホットライン 188）。

（参考：国民生活センターウエブサイト）