見守り新鮮情報



©Kurosaki Gen

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）

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

ひとこと助言



- 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。
- 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**消費生活センター**等にご相談ください（消費者ホットライン188）。

本文イラスト：黒崎 玄

見守り新鮮情報　第550号（2026年9月3日）発行：独立行政法人国民生活センター