知らぬ間にあなたの名前でお買い物

事例 クレジットカード会社から最近使っていなかった通販サイトの請求があったので、マイページで購入履歴を確認した。すると、注文していないのに複数の商品を買ったことになっていた。思い返すと、そのサイトから「支払方法の更新」というメールが届き、案内に従って情報を再登録したことがある。

実在する通販サイトやカード会社を装うメールを送りつけ、偽サイトへ誘導し、ログイン情報（メールアドレスとパスワード）やカード情報を盗み取るフィッシング詐欺が増えています。

盗まれた情報は不正ログインに使われ、本人の知らない間に勝手に買い物をされ、後日、カード会社から代金の請求だけが届きます。覚えのない注文や請求に気付いたら、早急に通販サイトとカード会社へ連絡し、利用停止を申し出ましょう。ただし、不正利用と認められても、各社の規約や判断により、必ず返金されるとは限りません。被害を最小限に抑えるために、利用明細などをこまめに確認する習慣をつけておきましょう。

フィッシングメールには「至急」「要確認」など不安をあおる文面のほか、「規約変更のお知らせ」など通常の案内に見えるものもあります。表示される送信元も通販サイトやカード会社、携帯電話会社など多種多様なうえ、最近はAIが生成した本物そっくりのメールやサイトも多く、真偽の見分けが非常に難しくなっています。カード会社などからのメールが届いた場合は、メールのリンクからはアクセスせず、自分で公式サイトの問い合せ先を検索して連絡するか、公式アプリ内の通知をチェックしましょう。

知っている業者名で届いても、メールやSNS内にあるURLや、青字の「こちら」のようなリンクは偽サイトへつながる可能性があるため、絶対に押さないことが重要です。

問消費生活センター
TEL 6319・1000
FAX 6319・1500