令和３年１０月

【宅配業者かたるショートメッセージ】

【相　談】

スマートフォンに実在する宅配業者の不在通知がＳＭＳ（ショートメッセージサービス）で届いた。「ご確認ください」と記載されていたＵＲＬをタップし、現れた画面の指示でＩＤなどを入力した。数日後、スマホのキャリア決済が不正に利用されてしまった。

【アドバイス】

宅配業者をかたるＳＭＳによるフィッシング詐欺は、２年ほど前から急増しています。スマートフォンの種類で手口が異なり、開いた偽サイトからダウンロードしたアプリをインストールしたところ、１日100通以上のＳＭＳが勝手に送信され、通信料の高額請求を受けた事例もあります。

宅配業者をかたる偽サイトは、本物とほとんど区別がつきません。まずは「記載されたＵＲＬを安易に開かない」ことが重要です。実在する事業者名がメールやＳＭＳに記載されていても、問い合わせ窓口を公式サイトなどで調べましょう。多くの宅配業者のサイトで、不審なＳＭＳについて注意を呼びかけています。

万一、サイトを開けてしまっても「アプリのインストール」や「ＩＤ・パスワード等の入力」をしなければ被害は防げます。落ち着いて行動しましょう。

事前対策として「携帯電話会社の対策サービスやセキュリティーソフト等を活用」「ＩＤ・パスワード等の使い回しをしない」「キャリア決済の限度額を必要最小限または利用しない設定にする」なども有効です。

不安に思ったりトラブルに遭ったりした場合は最寄りの消費生活センターや警察署等に相談してください。手口など詳細は独立行政法人情報処理推進機構（IPA）安心相談窓口だよりが参考になります。

**消費者ホットライン　　☎局番なしの１８８（泣き寝入りはいやや！）・・・お近くの消費生活センター等につながります。**