執筆者：国民生活センター相談情報部

第20回

宅配便業者を装った「不在通知」の偽SMSに注意しましょう

相談事例

宅配便の不在通知のSMS（ショートメッセージサービス）を受け取り、記載されているURLにアクセスしたところ、ブラウザの更新をするよう表示されたので更新した。このときに不正アプリをインストールされたようで、知らない人から「いつ配達してもらえるか」といった内容の電話が多くかかってきた。その後、携帯電話会社からの請求書の明細を確認すると、海外宛てと国内宛てのSMSがそれぞれ100通ほど自分のスマートフォンから送られており、通信料が1万円以上となっている。

（30歳代、女性）

問題点とアドバイス

宅配便業者を装った「不在通知」の偽SMSに関する相談が寄せられています。消費者に送られてくるSMSには偽サイトに誘導するためのURLが記載されており、相談事例のように、偽サイトにアクセスして不正なアプリをインストールした結果、同じ内容のSMSが自身のスマートフォンから自動的に多数の宛先に送信されてしまい、身に覚えのない通信料を請求されるケースがみられます。また、アクセスした偽サイトに入力したID・パスワード、暗証番号、認証コード等が携帯電話会社のキャリア決済などで不正に利用されて、身に覚えのない請求を受けるケースもみられます。

(1) URLにはアクセスせず、ID・パスワード等を入力しないようにしましょう

スマートフォンや携帯電話に届いたSMSやメールが宅配便業者からの正式なものかどうか見分けることは困難です。自分で調べた宅配便業者の電話窓口や公式ホームページ等で真偽を確認し、もし「不在通知」を内容とするSMSやメールが届いても、記載されたURLに安易にアクセスしないようにしましょう。

万が一アクセスしてしまうと、提供元不明の不正なアプリをダウンロードするよう誘導されるケースがあります。公式マーケットにあるもの以外の「提供元不明のアプリ」はダウンロードやインストールをしないようにしましょう。

また、宅配便業者のほかに銀行などを装った偽サイト（フィッシングサイト）に誘導されてID・パスワード、暗証番号や認証コード等の入力を求められるケースもあります。銀行の場合は口座から預金を不正に引き出されるおそれがあるため、こうした情報を入力しないようにしましょう。

(2) 不正なアプリはアンインストールしましょう

万が一不正なアプリをインストールしてしまった場合には、スマートフォンなどを機内モードに設定し、不正なアプリをアンインストールしましょう。また、より安全な対応策としてスマートフォンの初期化も検討しましょう。

参考：国民生活センター「宅配便業者を装った「不在通知」の偽SMSに注意しましょう－URLにはアクセスしない、ID・パスワードを入力しない！－」（2020年11月26日公表） http://www.kokusen.go.jp/news/data/n-20201126_2.html