

広報とうや湖掲載8月号

宅配便をかたる偽SMS「不在通知」といった新たな手口が出現！フィッシングサイトでの情報入力に注意しよう！

去年の7月頃から全国で宅配便をかたる偽SMS（ショートメッセージ）が届き、消費者被害が多数発生しております。町内でも実際にメッセージが届いたという相談が複数寄せられており、被害がいつおきてもおかしくない状況です。

その手口は次のとおりです。

佐川急便をかたる偽SMS「不在通知」の文面「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。下記よりご確認ください。<http://sagawa-●●●●.com>」（●は2～4文字の英字）というもので、記載のURLを開くと、佐川急便の公式サイトを模した偽サイトへ誘導され、その偽サイトを介してフィッシングサイトへ誘導されます。フィッシングサイトでは「セキュリティの許可が必要」等のもっともらしいうたい文句で、「電話番号と認証コード」等を必須入力に見せかけます。ついつい「電話番号と認証コード」等を入力してしまい、キャリア決済サービスを不正使用され、スマホの通信料とあわせて高額の請求書が届きだまされたことに気づきます。

だまされないように次の点に注意しましょう！

- ・佐川急便やヤマト運輸ではSMSによる不在通知の案内は行っていません。
- ・偽SMS「不在通知」が入ったり、偽サイトやフィッシングサイトが表示された場合は、画面を閉じてください。フィッシングサイトに「電話番号・認証コード」等を入力していなければ、被害にはつながりません。

もし、入力した場合、機内モードにしてインストールされたアプリを削除しましょう。

その後、利用している携帯電話会社に不正なキャリア決済が発生していないか確認しましょう。

キャリア決済サービス：電話番号等を入力することによって、商品代金を携帯の通信料金とまとめてお支払する決済サービスです。