

AWAJI POLICE STATION NEWS

淡路警察署だより 1月号

偽メッセージについて

ショートメッセージサービス（SMS）、電子メール、SNSのダイレクトメッセージを利用し、偽サイトにつながるURLを送りつけるものが多く発生しています。

URLをタップしてリンク先に接続すると、個人情報の入力やアプリのインストールを促されます。

指示に従うと、IDやパスワード、カード情報などを盗まれ悪用される場合や、悪意のあるアプリをインストールすることで、アドレス帳などの情報が盗まれ悪用される場合があります。

官公庁や金融機関、宅配業者、通信事業者など、生活に密着した事業者等を装うものから、知人や取引先に成りすましたものまで様々です。

「支払情報に変更された」「1年以上利用がないためアカウントを停止する」等といって確認や再設定を促すもの、「セキュリティ上の理由でブロックされている」と不安をあおるもの、「お荷物をお届けにあがりましたが不在のため持ち帰りました」と日常生活で利用する宅配業者を装うものなど、信用してもおかしくない内容で届きます。

気を付けなければ、周りの人にまで迷惑がかかる場合もあります。

【対策】

- 知らない相手からのメッセージを開かない
- 知人からのメッセージでも安全性が確認できるまでリンク先を開かない
- 個人情報を入力するときは、正規サイトであることを確認する
- 事業者等からの連絡は公式ホームページやアプリで確認する

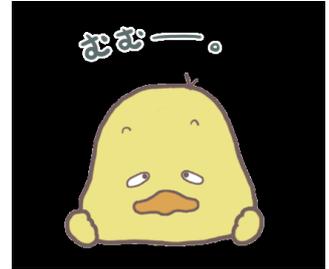
偽サイト・詐欺サイトについて

インターネットショッピングにおいて、「代金を支払ったが商品が届かない」、「別の商品が届いた」等、偽サイトや詐欺サイトによる相談も多く寄せられています。

これらの相談は「商品名で検索をかけた結果、偽サイト・詐欺サイトにたどり着いた」というケースが多くみられます。

【対策】

- 価格の安さや入手困難な商品に惑わされず、信頼できるお店を利用する
- 会社名・サイト名等を検索し、正規サイトが別に存在しないか確認する
- 検索エンジンから直接ショッピングサイトに移動するのではなく、
正規サイトのリンクからショッピングサイトに移動する
- 会社情報を確認する
 - (例) 実在の会社かどうか
 - (例) 連絡先がフリーメールアドレスになっていないか
- 決済方法を確認する
 - (例) 決済方法が「銀行振り込みのみ」になっていないか
 - (例) 決済方法を「銀行振り込み」に変更するよう依頼されていないか
 - (例) 振込先は法人名かどうか



個人名の場合は、代表者、責任者、運営者以外の個人名になっていないか

上の(例)に該当しない場合でも、偽サイトや詐欺サイトである場合がありますので十分に注意してください。