

サイバーセキュリティ パートナーシップだより



令和3年5月25日 山口県警察本部生活環境課

宅配業者をかたる SMS(ショートメール) による「フィッシング被害」が急増中!!

現在、佐川急便をかたった SMS を受信し、メッセージ中の URL から誘導された偽サイトにおいて個人情報を入力した等のフィッシング被害相談が急増しています。

確認されている手口や SMS の特徴について紹介しますので、被害に遭わないよう十分注意してください。また、周りの方々にも注意を呼びかけてください。

事例 1

佐川急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。<http://〇〇〇〇〇〇.duckdns.org>

送信元は、登録外の携帯電話番号や「sagawa」、「佐川急便」等で送られてくる。

iPhone の場合、**Apple の偽サイトへ誘導**され、ID パスワードの入力を求められる。

Android の場合、**佐川急便の偽サイトが表示**されたり、提供元不明アプリをインストールさせるようなポップが表示される。

事例 2

ご本人様不在通知為お荷物を持ち帰りました。ご確認ください。

<https://sagawa-〇〇〇.icu>

iPhone、Android 共通～**佐川急便の偽サイト(再配達受付)に誘導**される。

入力項目として、電話番号、メールアドレス、本人確認書類として**運転免許証やマイナンバーカード等の身分証を写真で送信するよう求められる。**

被害に遭わないための大原則：SMS のリンクにアクセスしない!

上記のとおり、リンクにアクセスし、情報を送信してしまうと、**AppleID の乗っ取りや身分証の悪用被害**につながります。

また、機種や端末の設定によっては不正アプリをインストールしてしまい、自分の電話番号から同様の SMS が大量に発信されてしまいます。

リンク付きの SMS を受信した場合は、フィッシングを疑い、偽サイトにアクセスしないようにしましょう。また、送り主に返信したり、個人情報を入力することは避けましょう。



サイバー犯罪相談窓口

TEL 083-922-8983

mail cyber.soudan@police.pref.yamaguchi.lg.jp

～研修会の依頼は警察署又は警察本部生活環境課まで～

サイバー
防犯広報



https://www.police.pref.yamaguchi.lg.jp/kurashi/page_b001_000003.html