

サイバーセキュリティ パートナーシップだより



No.12

令和3年8月2日 山口県警察本部生活環境課

ヤマト運輸をかたる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、ヤマト運輸をかたった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。

〈実際に届いたメッセージ内容〉

+8180 〇〇〇〇 〇〇〇〇
SMS

やまと運輸よりお荷物を発送しましたが、宛先不明です、下記よりご確認ください。

<http://〇〇〇〇.duckdns.org>

送信元は、登録外の携帯電話番号や「ヤマト」「クロネコ」等で送られてくる。

【iPhoneの場合】

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

【Androidの場合】

ヤマト運輸の偽サイトへ誘導され、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たり、携帯電話番号の入力を求められる。

被害に遭わないためには、SMS内のURL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、Apple IDの乗っ取り等の被害につながります。

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。送り主に返信、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