令和４年５月発行

Kagawa Cyber Security Information

香川県サイバーセキュリティ連絡ネットワーク通信Vol.75

通信業者などを装った不審メッセージに注意!!

ある日、突然に
「【利用停止予告】未払い料金お支払いのお願い。」
「【重要なお知らせ】通信サービスは利用停止される場合がございますので、必ずご確認下さい。」
等と記載されたメールやＳＭＳが届いた・・・**待ってください！**
それ「**フィッシング詐欺**」かもしれません！！
安易に記載されている**ＵＲＬにアクセスしない**ように注意して下さい。

「フィッシング」とは？？

悪意を持った人が、実在する企業等を装って電子メールを送り付け、不正サイトに接続させたりするなどの方法で、クレジットカード番号やアカウント情報（ＩＤ・パスワード等）を盗むことです。
フィッシング手口としては、
① 不正サイトに繋がるＵＲＬを添付した、メールやＳＭＳを送付してくる。
② メールやＳＭＳに記載のＵＲＬをクリックするように誘導する。
③ 不正サイトのログイン画面が表示され、ＩＤ・パスワード等の個人情報を入力させる。
といった流れで犯行が行われます。

過去の実例紹介

下記以外の文面も多数存在するので注意！！

「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。https://●●haisou.com/●●」（＊配送業者を装っています。）

「お客様のアカウント情報に異常ログインの可能性がございます。下記ＵＲＬでご確認ください。https://●●tuusin.com/●●」（＊通信事業者を装っています。）

「通信量の制限を超えたので解除するにはここをクリック。
https://●●tuusin.com/●●」
（＊通信事業者を装っています。）

「通信サービスは利用停止される場合があるので必ずご確認を。
https://●●tuusin.com/●●」
（＊通信事業者を装っています。）

CHECK!!

被害に遭わないための６ヶ条

1 「重要」「緊急」といった件名や本文に惑わされない！
2 不用意にメールやＳＭＳに記載のＵＲＬにアクセスしない！
3 安易に個人情報を入力しない！
4 ＵＲＬの末尾が「.xyz」「.shop」などの見慣れないものは要注意！
5 メールやＳＭＳに記載のＵＲＬではなく、正規サイトからログインをする！
6 フィッシング詐欺などの犯罪の特徴や手口を普段から意識して知る！

香川県警察本部生活環境課 サイバー犯罪対策室　　TEL:０８７－８３３－０１１０