サイバーセキュリティパートナーシップだより

No.31

令和2年12月11日　山口県警察本部生活環境課

リンクへのアクセスを誘うSMS（ショートメール）は、フィッシングor不正アプリを疑え！！！

大手通販サイト、金融機関、クレジットカード会社、宅配事業者等をかたったフィッシングメールによる被害が後を絶ちません。

特に、スマホに受信したSMS（ショートメール）のメッセージに記載されたURLリンクへのアクセスを促され、フィッシングサイトへ誘導されたり、不正なアプリをインストールされてしまう手口が増加しています。

SMSで興味を引かせたり、異常を知らせて不安を煽ることでリンクへのアクセスを誘うものは、全て「悪意のある攻撃」と疑い、冷静に対処しましょう。

※フィッシングとは・・実在組織をかたり個人情報をだまし取る等の行為

フィッシングメールの一例

お荷物のお届けにあがりましたが不在のため持ち帰りました。ご確認ください。http://○○○.○○

○○でご購入ありがとうございます。商品発送状況はこちらにてご確認ください。https://○○○.○○

お客様の○○に対し、第三者からの不正なアクセスを検知しました。ご確認ください。https://○○○.○○

お客様の○○銀行口座がセキュリティ強化のため、一時利用停止しております。再開手続きをお願いします。https://○○○

○○使用制限ポリシーの違反が検出されました、ログインして確認してください。https://○○.○○

被害に遭わないために

大原則：ＳＭＳのリンクに安易にアクセスしない

- 正規のアプリや、ブックマークしたサイトURLからアクセスする癖をつける
- ID・パスワードは使い回さない
- スマホのポップアップ機能を使用して利用者の不安を煽り、誘導してくる手口にも注意

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