サイバーセキュリティパートナーシップだより

R5-11

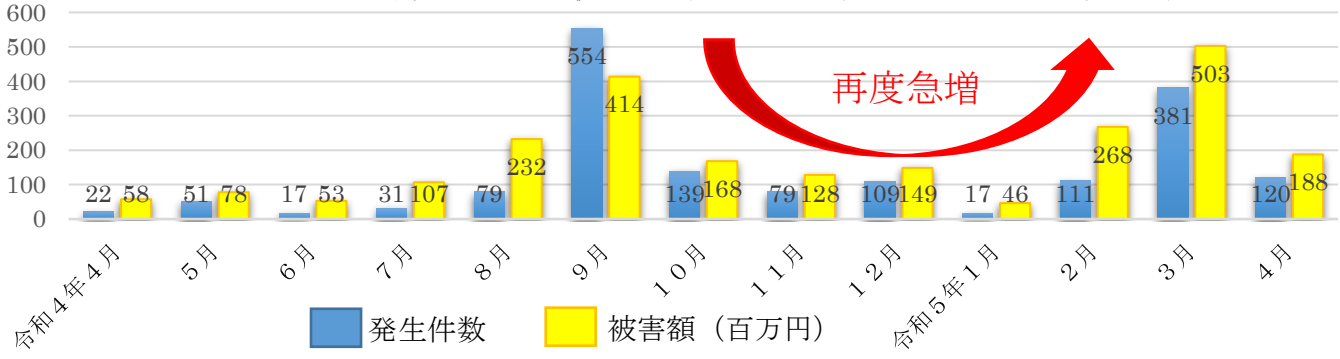
フィッシングに要注意！

インターネットバンキングの不正送金被害、急増中

全国のインターネットバンキングの不正送金被害は、昨年８月下旬から９月に急増し、以降、一旦被害が減少したものの、今年に入り、

・２月 ➡【発生数】１１１件、【被害額】約２億6,800万円
・３月 ➡【発生数】３８１件、【被害額】約５億３００万円
・４月１日から１４日までの間
➡【発生数】１２０件、【被害額】約１億8,800万円

と、再度急増している状況で、被害の多くはフィッシングによるものとみられます。



被害に遭わないために

日々の心がけとして、

- ☑ 心当たりのないSMS等は開かない（金融機関が、IDやパスワードをSMSで問い合わせることはありません）
- ☑ インターネットバンキングの利用状況を通知する機能を有効に設定し、不審な取引（ログイン、パスワード変更、送金等）に注意する
- ☑ 金融機関のウェブサイトへのアクセスに際しては、SMS等に記載されたURLにアクセスしないようにする

ことに気をつけましょう。

さらに＋α（スマホやパソコン、アプリの設定）

① 迷惑メールフィルターの強度を上げて設定する
② 金融機関が推奨する多要素認証等の認証方式を利用する
③ ウイルス対策ソフトが無償で提供されている場合は、導入を検討する
④ スマホやパソコン、アプリのウイルスセキュリティソフトを最新にする

などの設定をすれば、さらに安心です。

✉フィッシングメールの例✉
（金融機関騙りで実際に送られたもの）

⚠ 特徴及び注意点 ⚠

法律名を記載

法律に則っているように記載し、アクセスを促します。

また、「犯罪に加担している」、「裁判の手続きになる」等不安をあおり、アクセスを促す場合もあります。

不自然なリンク、URL の添付

アクセスすると、ID・パスワードクレジットカード情報等の入力フォームが用意されており、入力してしまった場合、情報を窃取されます。

正規サイトの URL を混載

受信者を信用させるために、正規サイトの URL を織り交ぜています。

メール本文

From [redacted]銀行 <[redacted].jp>

重要：[redacted]銀行お客様のお取引目的等のご確認

2023/04/22 土曜日 11:21

※いつも[redacted]銀行をご利用いただき、ありがとうございます
当社では、犯罪収益移転防止法に基づき、お取引を行う目的等を確認させていただいております。
また、この度のご案内は、当社ご利用規約第 4 条 5 項 9 に基づくご依頼となります。
お客様お客様の直近の取引についていくつかのご質問がございます、下記のリンクをアクセスし、ご回答ください。

お取引確認

文字が変わっているリンクに要注意！！

※当社サイトの一部において旧社名のドメイン「[redacted].jp」を使用しています。
※本メールは重要なお知らせのため、配信を希望されていないお客さまにもお送りしています。
【メールに関するお問い合わせ】
個人のお客さま
https://www.[redacted].jp/support/customer.html
法人・個人事業主のお客さま
https://login.

[redacted]銀行株式会社
東京都
https://www.[redacted]jp/
Copyright All rights reserved.

ページトップへ

※　フィッシングメールは金融機関のほか、公的機関、携帯電話会社、宅配便、通販サイトを騙るなど、多岐にわたり、巧妙につくられています。**メール本文中の URL に絶対にアクセスしないでください。**

山口県警察本部サイバー犯罪相談窓口
TEL　０８３－９２２－８９８３

県警ホームページにて広報資料や動画を公開中です。
（詳しくは QR コード参照）