滋賀県警察

サイバーセキュリティ情報SHIG@

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R５年度 No.1

大手金融機関を装ったフィッシングに注意

大手金融機関を装ったフィッシングメールが確認されています。
金融機関や通信事業者、ショッピングサイトからを装ったメール（ショートメッセージを含む）によるフィッシングサイトへの誘導が、多数発生していますので、ご注意ください。

メール文面の例

［メッセージ］
〇〇バンキングをご利用いただき、誠に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。

お客様の直近の取引についてご質問があります。
下記のリンクにアクセスし、ご回答ください。

https://www.●●●.jp.■■■.com

URLをクリックしないでください

STOP クリック！

※一定期間ご確認いただけない場合、口座取引を一部制限させていただきます。
※回答が完了しますと、通常通りログイン後のお手続きが可能になります。

ーーーーーーーー
【お問い合わせ先】
●●インフォメーションデスク
□□□□
（受付時間）平日・土・日・祝9時～17時

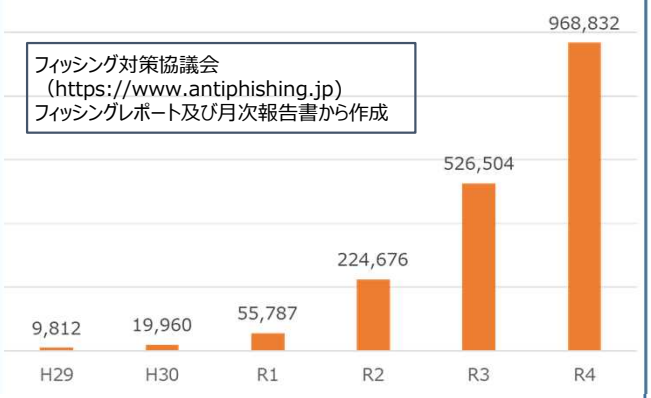
ID/パスワード、口座情報等が盗まれて、インターネットバンキングを悪用した不正送金に利用されるおそれがあります。

フィッシングメールの特徴

- **口座情報等を確認させる内容が多い。**
- **他のサイトに誘導するURLが記載されている。**
- **URLにアクセスすると、金融機関等のログイン画面となり、IP･パスワードを入力するように表示される。**
- **ID/パスワードのほか、個人情報、口座番号、クレジットカード番号の入力を求められる。**

フィッシングメールの件名
【〇〇銀行】取引目的開示のお願い
【〇〇銀行】お取引目的等の確認のお願い
【重要】振込･振替サービスの制限のお知らせ
【〇〇銀行】必ずご回答ください
※上記以外の件名も使われている可能性があります。

フィッシング報告件数の推移



フィッシング対策協議会によりますと、令和4年のフィッシング報告件数は、96万8,832件（前年比+44万2,328件で右肩上がりで増加しています。

参照：フィッシング対策協議会｜緊急情報（https://www.antiphishing.jp/news/alert/smtb_20230322.html）

- **フィッシングサイトは本物そっくりです。**
- **メール（ショートメッセージ）の本文のURLからアクセスしないでください。**
- **サービスにログインするときは、公式アプリやWebサイトのブックマークを利用してください。**

«サイバーコネクトSHIG@»Fortinet社製品の脆弱性にご注意願います。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　県警Webページ→

https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html