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。

R４年度 No.４

サイバー犯罪相談増加
特に気を付けて欲しい4つの事例

フィッシング

フィッシングは、メールやSMSを使ってユーザーを偽サイトに誘導し、**ID・パスワード**や**クレジットカード情報**等を入力させて、それらの情報を盗み取る手口です。

ID・パスワードを盗み取られたら・・・
- ショッピングサイトで**無断で買い物**をされる。
- クレジットカードを無断で使用される。
- **闇サイト**で個人情報を売られる。
- パスワードを変更される。

「口座設定による本人確認手続き」
下記URLでご確認が必要です。
http://www.●●●.com

【被害防止】
- メール等に記載されたリンク（URL）をクリックしない。
- ID・パスワードは、必ず**公式サイト**から入力しましょう。

偽ショッピングサイト詐欺

偽ショッピングサイトは、**本物のサイトをコピー**したり、実在する会社名や代表者名を使用するため、見分けることが難しくなっています。会社が存在するか、連絡先が正しいかを確認してください。

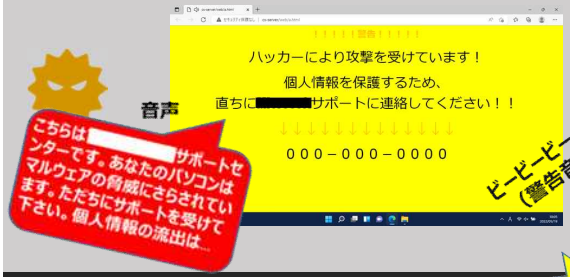
特に**要注意なドメイン**
「**.top**」「**.xyz**」
「**.site**」「**.online**」
これらのドメインがついたURLは
偽サイトの可能性が高いです。

STOP!振込

【偽サイト見分けるポイント】
- **商品の支払い方法が銀行振込だけでないか。**
  偽ショッピングサイトの多くは、銀行振込しか利用できません。（入金後すぐに出金が可能であるため）
  会社が経営しているのに個人名義であったり外国人名義の口座も要注意です。

サポート詐欺

サポート詐欺は、画面に突然、**偽のセキュリティ警告**等のメッセージを表示させたり、偽のウイルス感染を音声で知らせたりするなどして、ユーザの**不安を煽り**、画面に表示された電話番号に電話をかけさせ、パソコンを遠隔操作するソフトウェアをインストールするように促し、有償のサービス契約や**サポート料金を請求**する手口です。



【被害防止】
- 警告は偽物です。**電話しないでください。**
- 偽警告画面は、「×」ボタン等で消すことができます。

STOP!電話

投資や副業を装った詐欺

SNSや**マッチングアプリ**等を通じて、知り合った人から、**投資**や**副業**等の話を持ち掛けられて、金銭（暗号資産）を**だまし取られる**ケースが発生しています。

- ◆ SNSで異性と知り合って、投資を勧められた。
- ◆ 外国人から資金を送る協力を依頼された。
- ◆ 余命宣告を受けた人から遺産を譲りたいと言われた。
- ◆ 話を聞くだけで**稼げる**と言われた。
- ◆「〇〇を評価するだけの仕事」を紹介された。

【ロマンス詐欺】
外国人などを名乗り、ネットで知り合った相手に恋愛感情を抱かせて現金をだましとる手口。

【被害防止】
- 「**儲かる話**」は信用しないでください。
- 投資や金銭（暗号資産）の送金は**慎重**に行ってください。

STOP!送金

これらの事案で現金等を請求・要求されたら家族や警察等にご相談ください。

«サイバーコネクトSHIG@»定期的にソフトウェアの脆弱性情報をチェックしましょう。

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→