令和5年号外　兵庫県警察サイバーセンターサイバー情報発信室

サイバー防犯通信

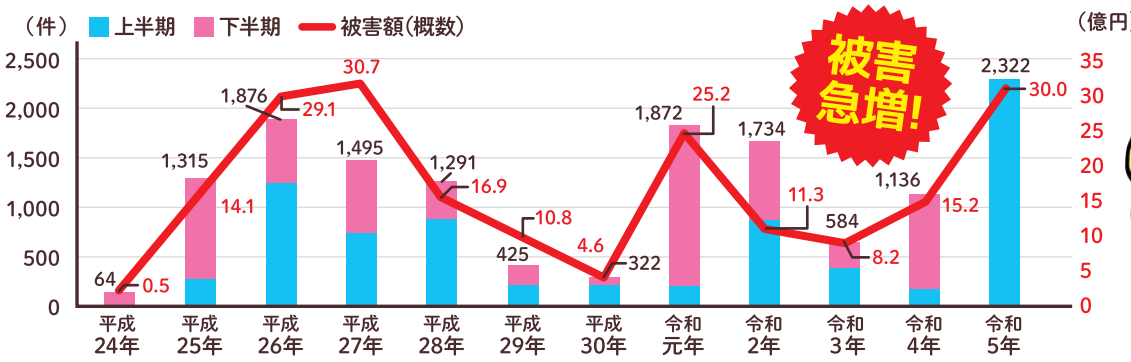
\Check/

https://www.police.pref.hyogo.lg.jp/

インターネットバンキングの不正送金

不正送金発生状況（令和5年8月4日現在）

警察庁広報資料：「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」



これらの被害の多くは、フィッシングから！

金融機関を装ったフィッシングサイト（偽ログインサイト）に誘導するメール（SMS）を多数確認しています！

そもそもフィッシングってなに？

実在のサービスや企業をかたり、偽のメールやSMS（携帯電話のショートメッセージ）で偽サイトに誘導し、IDやパスワードなどの情報を盗んだり、マルウェアに感染させたりする手口です。情報を盗まれると、アカウントを乗っ取られてお金を奪われたり、インターネット通信販売サイトで勝手に買物をされたりします。

フィッシングサイトへの誘導方法、手口

携帯電話の電話番号宛てに送信可能なSMSを悪用し、携帯電話会社、宅配業者、金融機関（銀行など）をかたって本物そっくりの偽サイトに誘導する事例を多数確認しています。そのほか、企業の本物のメールアドレスになりすました電子メールを送信する方法や、官公庁を名乗る電子メールを送信する方法、検索サイトの広告から誘引する方法など様々な誘導方法が確認されています。SMSの場合、携帯電話会社などの正規スレッドに偽メッセージが表示されたり、メールの場合、実在する企業のロゴが貼り付けられるなど、様々な手口がありますのでご注意ください。

怪しいメールを受信した！

フィッシングサイトを発見した！

フィッシングサイトに情報を入力してしまった！

通報！

最寄りの警察署
または
兵庫県警察本部
（代）078−341−7441

サイバーセンター公式SNS
（旧ツイッター）

兵庫県警察サイバーセンターでは公式SNS（旧ツイッター）で、サイバー犯罪やサイバーセキュリティの情報をいちはやくお届けしています。

https://twitter.com/HPP_c3division

金融機関などを装った

偽SMSに ご注意ください！

※SMS（ショートメッセージ サービス）：携帯電話番号を用いて、短いメッセージを送受信する機能

SMSを使用したフィッシングサイトに関する相談が増加しています。

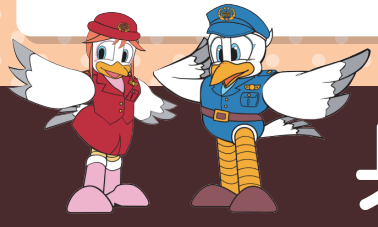
銀行を装ったSMSの例

盗まれた**ID・パスワード**などで、犯人に**本物のサイトにログイン**される。

預金を**犯人の口座に送金され**
盗まれることも…！

対策

- **リンクを不用意に開かない**
- リンクを開いてしまっても**ID・パスワード**などを**絶対に入力しない**
- サイトへのログインは、**公式アプリ**や**公式サイト**からアクセスする
- **迷惑SMSブロック機能**や**セキュリティ対策ソフト**を利用する



兵庫県警察

協力：トレンドマイクロ株式会社