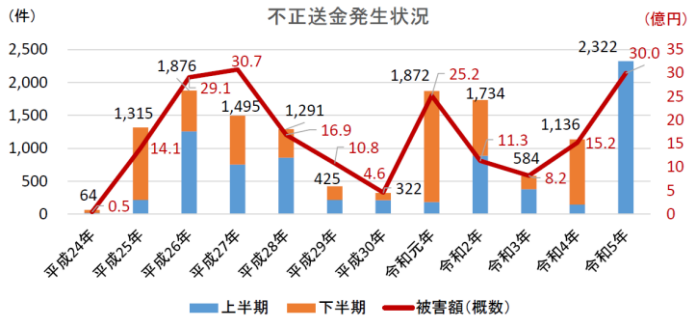
ASAMA あさまセキュリティニュースレター
Security Newsletter
2023年10月16日
Vol.101

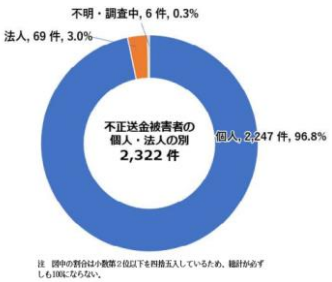
不正送金被害が急増中！

メールやSMS等経由のフィッシング手口で、インターネットバンキング利用者の
ＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発中！
令和５年上半期における被害件数は過去最多の2,322件、被害額も約30億円
被害者の大部分は個人（2247件）ですが、法人での被害も69件確認されています

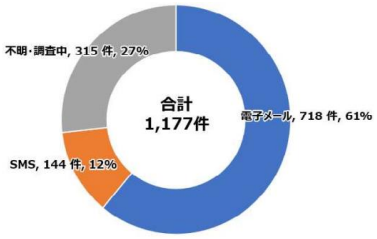


出典　金融庁　WEBサイト
https://www.fsa.go.jp/ordinary/internet-bank_2.html

図表11：インターネットバンキングに係る不正送金被害者の個人・法人の別



【図表13：フィッシングサイトへ誘導する手口別割合】



出典　警視庁
令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について

POINT

攻撃の6割を占めるメール経由のフィッシングは、メール文面やリンク先の偽のHPサイトも本物そっくり、見た目では判断つかなくなってきています。
電子証明書を利用したネットバンキングでも、パソコンを乗っ取られての被害も出ているため、セキュリティ対策も定期的に確認、見直しを！

サイバー攻撃のパターン

- **メール経由**　差出人を偽装、巧妙な文面で本文のURL（フィッシングサイトや不正なサイト）から不正サイトへ誘導するため、メール本文のリンクからではなく、WEBブラウザから正規サイトを開いて確認をメール経由の攻撃が多いため、**日ごろからどのようなフィッシングメールがあるか確認**を！
- **SMS経由**　携帯電話・スマートフォンの電話番号宛に、銀行を騙ったショートメッセージを送り、偽のログインサイトへ誘導、IDやパスワード、ワンタイムパスワード等入力させ不正送金
  メールよりも見られやすく、なりすましも容易、簡単に送れるため、個人被害が多発

対策

- **フィッシングメールは本物と見分けにくいため、最新の情報を確認**　・・・　参考URL　迷惑メール相談センター
  https://www.dekyo.or.jp/soudan/index.html
- **ID・パスワード等使い回ししていると、攻撃者は様々なサービスへ**
  不正にログイン・不正利用を試みます。パスワードの使いまわしは避けましょう
  ウイルス感染すると、入力情報の搾取だけでなく遠隔で悪用されるケースも。セキュリティ対策は怠らずに。

ビジネスでパソコンを利用する上での注意点

サポート切れのパソコンやソフト、古いネットワーク機器は使用をやめ定期的に見直しを
フリーWiFiや、公衆WiFiの利用はしない。デバイスやサービスは公私を分けて利用する。
使いまわしのUSBメモリは使用を避ける。出所不明のフリーソフトやクラウドサービスは利用しない。

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414