令和５年４月27日

サイバーセキュリティ関連情報（５月号）

鳥取県警察本部サイバー犯罪対策課

YouTube公開中

鳥取県警察サイバー犯罪対策課
マスコットキャラクター

インターネットバンキングに係る不正送金被害の急増

インターネットバンキングは、銀行のサービスで、スマートフォン等で、口座の残高確認、振込等をすることができます。

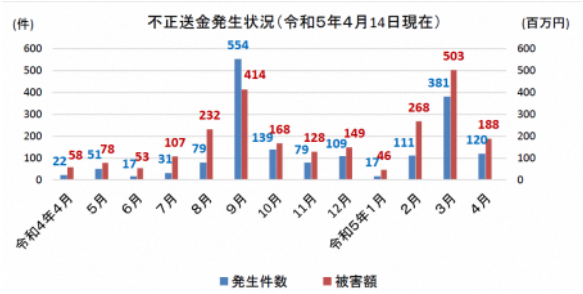
インターネットバンキングを使うには、「ＩＤ、パスワード」などが必要で、これらを専用のサイトで入力してログインを行います。

銀行やＡＴＭに行くことなく利用できて便利な一方、他人にＩＤ等が知られてしまうと、銀行口座を不正に操作し、所有者が気づかないうちに口座からお金を移動することが可能となります。

（※このお金の移動を「不正送金」と言います。）

不正送金は、令和５年２月から急増しており、被害の多くはフィッシングによるものと見られ、銀行を装った偽サイト（ログイン画面）へ誘導するメールが多数確認されています。

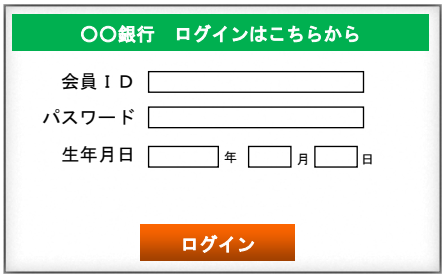
以下の手口に注意をお願いします。



（令和５年中の数値は暫定値）

【フッシングの手口】

① メールや、ＳＭＳ（ショートメッセージ）が届く
② ①には、ＵＲＬ「http://〇〇～」等が記載されている
③ ②のＵＲＬを押すと、偽サイトが表示される
④ **ＩＤ、パスワード等の入力**を求められる
⑤ 情報が盗み取られ不正送金に利用される



偽サイトのイメージ
（実在のサイトと見分けるのは困難です）

★参考★
【警察庁ウェブサイト】
「フィッシング対策」
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

長期休暇に向けてのセキュリティ対策

企業等の長期休暇では、

〇セキュリティ担当者の不在期間の発生
〇機器の脆弱性に対するアップデートの未実施
〇休暇中の在宅勤務で使用する端末の管理
〇連休中に蓄積されたメール確認の際
・機器の脆弱性を残した端末での開封は危険
・多数のメールを処理する際、意図せず添付ファイルを開封

等の問題があり、不正アクセス等を企図する者から絶好の攻撃機会となる期間です。

休暇前に必要な対策、休暇後の対策に関しては、右のとおり資料を公開していますので、参考としていただくようお願いします。

また、休暇中に関しては、企業等の従業員の方に対して、セキュリティ担当者への連絡方法を分かりやすく手配するなどして、早期対応・被害拡大の防止となるように準備をお願いします。

鳥取県サイバーセキュリティ対策ネットワーク
Webページ内で公開中