サイバーセキュリティパートナーシップだより

R6-5

被害多数！！「フィッシング」に注意

「フィッシング」は、実在する組織を騙ったメールやSMSを使って、偽サイトに誘導し、アカウントID、パスワード、クレジットカード番号といった個人情報を盗み取る手口です。

令和５年中、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の不正送金事案は、全国で被害件数・被害額ともに過去最高を更新しており、特に注意が必要です。

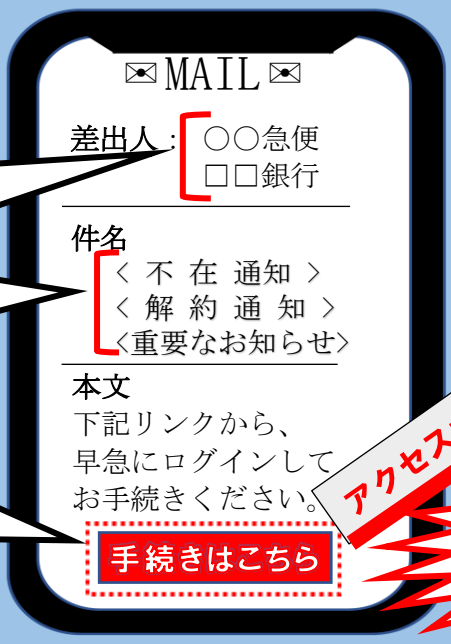
フィッシングのメール・SMSの特徴を知り、被害を防止しましょう。

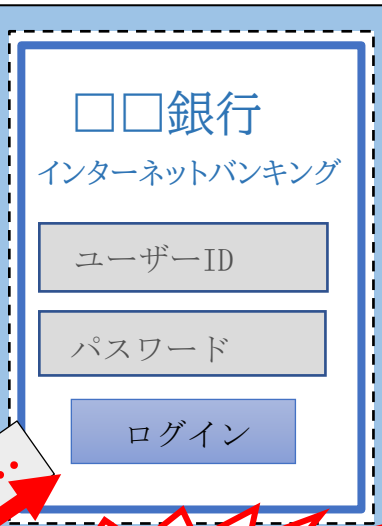
フィッシングメール・SMSの特徴

① **差出人名**
銀行、クレジットカード会社
宅配業者、通販サイト等の
実在する組織

② **件　名**
思わず「確認しなければ！」
と思わせる内容

③ **本　文**
本文中のリンクやURLへの
アクセスを促してくる





アクセスすると・・・

本物そっくりな偽サイトが出現！
入力した情報を窃取されるので、
アクセスしてはいけません！！

習慣づけで被害を予防しましょう

フィッシングサイトは本物のサイトにそっくりで、見た目では偽物のサイトと判断することが困難です。

日頃から利用しているサービスへログインする際は、メールやSMSのリンクをクリックせず、いつも使っている公式アプリ・公式サイトから開くように習慣づけましょう。

これを習慣づければ、フィッシングサイトを開く可能性が減るため、被害を防止することができます。

「いつもの」
公式アプリから
アクセス！

「いつもの」
公式サイトから
アクセス！

山口県警察
サイバー犯罪相談窓口

県警ホームページにて広報資料や動画を公開中です。
（詳しくはQRコード参照）

山口県警察本部サイバー犯罪対策課