

サイバーセキュリティ パートナーシップだより



R7-22

～あなたの銀行口座（ネットバンク）がねらわれています～
フィッシングによる不正送金被害に注意！

～被害事例～

〇〇銀行から「重要」「本人確認」といったメールが届き、メール内のリンクからサイトに飛んで、インターネットバンキングのログインIDやパスワード、口座情報等を入力したところ、知らないうちにネットバンクの口座から100万円が勝手に送金されていた。

～フィッシングメールの例～

From : ●●ネット銀行
(▲▲▲@com)

【重要なお知らせ】

お客様の口座において、×月△日
までに確認が必要な事項がございます。

確認手続きはこちら

<https://▲▲▲.example.com/> (偽サイトのURL)

●●ネット銀行

ログインID

パスワード

ログイン

ニセ
偽

ログイン情報を入力してしまう
と不正送金被害に！

※ニセサイトは本物そっくりに
作られているため見分けが困難！

銀行が口座情報や個人情報を
メールで確認することはありません！

被害に遭わないための対策

- ☐ 不安を煽るような件名・内容のメール・SMSを受信した際は要注意！
- ☐ 登録情報などの確認は「公式アプリ」や「公式サイト」から行う！
- ☐ メールやSMSの文中のリンクをクリックして内容確認しない！
- ☐ セキュリティ対策ソフト（アプリ）や迷惑メールブロック設定を活用！
- ☐ ログイン設定における「パスキー」や「多要素認証」の利用！
- ☐ 振込限度額の引き下げ

SMS
メール

URL



サイバー犯罪相談事例
対処法と対策・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。
(詳しくは二次元バーコード参照)



山口県警察本部
サイバー犯罪対策課