

サイバーセキュリティ パートナーシップだより



R6-15

JAバンク
をかたる

フィッシング  **に注意**

JAバンクは本年9月以降、JAバンク等を装ったフィッシングメールや偽サイトが確認されていると注意喚起しています。県内においても、フィッシングによりJAバンクのインターネットバンキングから不正に残高を送金される被害を確認しているため、注意をお願いします。

こんなメールやSMSに注意！！



✉ MAIL ✉

差出人：JA ネットバンク

件名 お客様情報等の
確認について

本文

お客様の直近の取引
についていくつかの
ご質問があります。
リンクをアクセス
し、ご回答ください。

<https://zh●x.com>

(一例)



アクセスすると

本物そっくりの
偽サイト

JAバンク

インターネットバンキング

ログイン ID

ログインパスワード

ログイン

ID やパスワード等を入力した場合
口座残高全額を不正送金される
被害に遭う可能性があります！！

被害に遭わないためのポイント

1 電子メールやSMSに記載されている
リンクやURLをクリックしない

2 リンクやURLを開いてしまっても
ID・パスワード・口座情報を入力しない

3 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

4 携帯電話会社などが提供する
セキュリティ設定を活用する

偽サイトにIDやパスワード等を入力したり、身に覚えのない取引に気が付いたら、①ログインパスワードをすぐに変更、
②サービス提供会社、警察に相談をお願いします。



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QRコード参照)

