

JAバンクを装った フィッシングメールにご注意ください

日本国内で発生している詐欺の件数や被害金額は年々増加しています。また、その手口も多様化しており、より巧妙で詐欺と気づきにくいケースも存在します。JAバンクをかたってフィッシングメールを送りつけ、JAバンク利用者の貯金を狙う事例も発生しています。フィッシングの対策を知り、しっかりと自分の身を守りましょう。



「フィッシング」って何？

銀行などを装ったメールやショートメッセージサービス(SMS)から偽サイトに誘導し、金融情報や個人情報を不正に入手する手口を「フィッシング」と呼びます。

●フィッシングにだまされると…

- ・銀行口座を操作され、勝手に送金される！
- ・ECサイトで勝手に買い物をする！
- ・アカウントを乗っ取られる！

こんなメールに注意！

①

From: XYZ銀行
件名: 【重要】取引停止のお知らせ
本人かどうか確認できない取引がありましたので停止いたしました。
下記URLから確認してください。
<http://xyz-bank.com>

取引の停止

②

From: XYZカード
件名: 【緊急】不正アクセスを検知しました
第三者からの不正なアクセスを検知しました。
下記URLから確認してください。
<http://xyz-card.com>

不正アクセス

③

050-XXXX-XXXX
お荷物のお届けがありました、不在のため持ち帰りました。
<http://xyz.com>

不在持ち帰り

有効なフィッシング対策

- メールやSMSに記載されたリンクを**クリックしない** → 内容の確認は、公式サイトやアプリを使い行う
- 携帯電話会社等の**迷惑メッセージブロック機能**を活用する
- 生体認証を活用する (**パスワードを入力しない**)

警察庁ホームページではフィッシング対策をさらに詳しく、また、岩手県警察本部サイバー犯罪対策課の公式X(旧Twitter)では、サイバー空間を悪用した犯罪手口やその対策などを発信しています。



岩手県警察
サイバー犯罪対策課
公式 X



警察庁
ホームページ

お問い合わせ先

JA金融課 ☎23-3007 または JA各支店