

## そのメール、フィッシングかも！

## こんなメールやSMSに要注意！

From：XYZ銀行

件名：【重要】取引停止のお知らせ

本人かどうか確認が取れない取引がありましたので停止しました。確認してください。

<http://xyz-bank.com>

取引の停止



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。確認してください。

<http://xyz-card.com>

不正アクセス



050xxxxxxx

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://xxx.com>

不在持ち帰り



メールやSMSによるフィッシング被害が発生中！！

## フィッシングに騙されるとどうなるの？

銀行等を装ったメールやSMSから偽のウェブサイトに誘導し、**金融情報や個人情報**を不正に入手する手口、それがフィッシングです！

- 銀行口座を操作されて勝手に送金される
- ECサイトで勝手に買物をされる
- アカウントを乗っ取られる

## フィッシングに対してできること



- 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利用する
- 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（パスワードを利用しない。）

※詳細なフィッシング対策はこちら⇒ <https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>

「サイバーコネクトSHIG@」定期的にソフトウェアの脆弱性情報をチェックしましょう。

←公式X

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表）

県警Webページ→