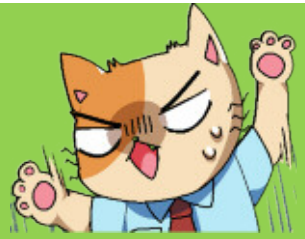


# 宅配事業者の不在通知を騙る フィッシングが **再び増化!!**



## 不在通知SMSは無視!

お客様宛にお荷物のお届けに  
上がりましたが不在の為持ち  
帰りました。下記よりご確認  
ください。

<http://takuhai.xx.com>

**STOP!**

**URLのリンク先は  
偽のサイトにゃ!**



最近、宅配を利用する人が多いから、  
ついURLを押してしまいそうね。



タレントの平松可奈子さんと、サイバ課長が  
「フィッシング」について、動画で紹介して  
います。(再生時間：1分)

サイバ課長 フィッシング



大学生サイバーボランティア  
による動画のご紹介

あなたの個人情報を守るのはあなただけ!セキュリティ意識を高めて防犯対策!

## あなたのお金・アカウント(ID・パスワード)が盗まれる… フィッシング被害**激増!!**

### フィッシング被害が激増!

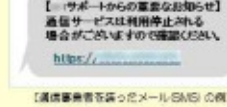
フィッシング対策協議会によると、  
令和3年中のフィッシング報告件数は  
52万6,504件で、4年前の約5.4倍、  
前年と比べても約2倍以上に激増して  
います。  
現在も愛知県警察にはフィッシング  
に関する相談が多数寄せられています。



### フィッシングとは

有名企業を装ったメールを送り、受信者を本物サイトに見せかけた偽サイトへ誘導し、  
クレジットカード番号やID・パスワード等を入力させ、不正に個人情報を入手する手口です。

#### ◇ フィッシングメールの例 ◇



【迷惑メール等対策課で調べたメール(SMS)の例】



【スマホ決済事業者を装った電子メールの例】

#### ◇ フィッシングメールの特徴 ◇

- ・「サービスの利用停止」「料金未払い」等と不安を煽る、緊急を装うメールの内容
- ・SMS(ショートメッセージ)、電子メール等さまざま
- ・URL等のリンクを押すと、公式サイトにそっくりなサイトが表示される

### 見た目でも偽メール・偽サイトを見分けるのは困難!

#### ・メールのリンクは押しちゃダメ!!

URL等のリンクを押してしまうと、巧みに不正アプリをインストールさせられたり、  
ID・パスワードやクレジットカード情報等の個人情報の入力求められる場合があります。  
不明な点がある場合は、公式ホームページに直接アクセスして確認しましょう。

#### ・パスワード使い回しの禁止!!

ID・パスワードの使い回しは大変危険です。  
流出してしまうと、使い回しているすべてのサービスで不正利用されるおそれがあります。

# 不在通知SMSは無視! メールのリンクは押しちゃダメ!!