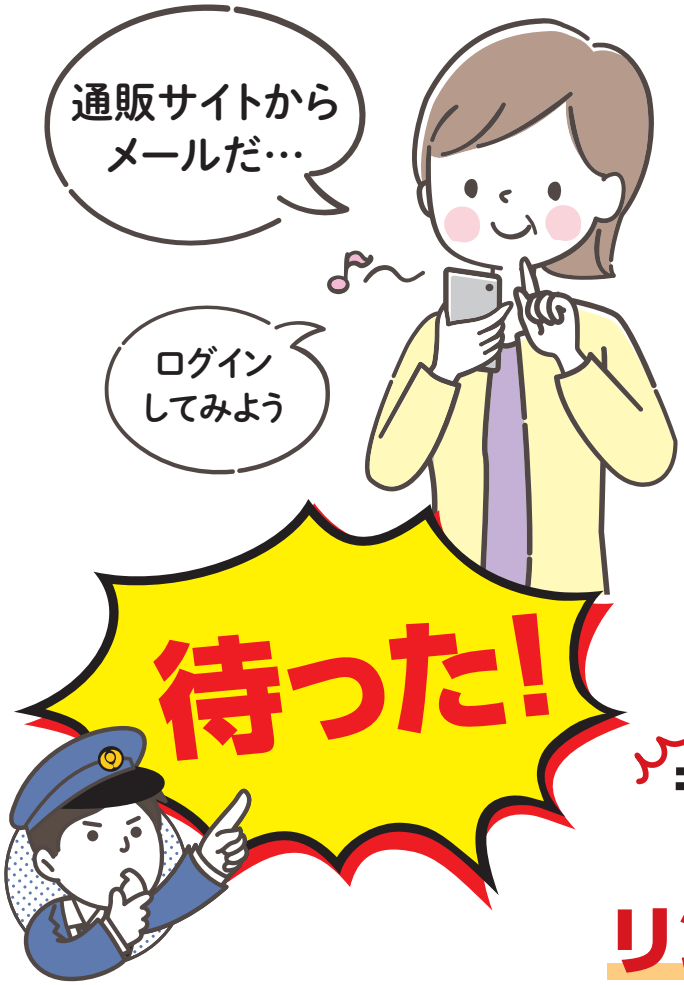
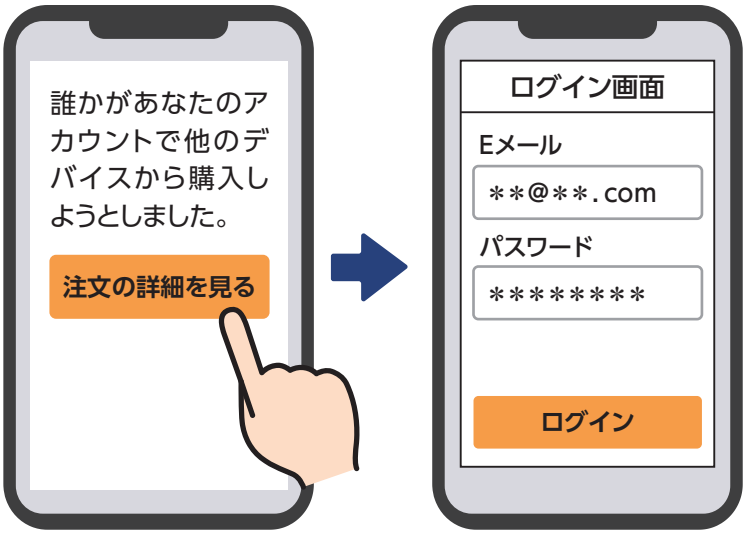
大手通販サイトのふりをした
偽メールに注意！





そのメール、信じても大丈夫?

もしかしたら、アカウント情報が盗まれるかも!?!

リンクは絶対に開かないで!

「通販サイトから『アカウントが不正利用されている』とメールが来た」という相談が警察に寄せられていますが、これは**偽のメール**です。
身に覚えのない注文や請求なら、

⚠ **メールのリンクは開かないようにする。**

⚠ **公式アプリやブックマークなどを使い公式サイトへログインして注文履歴などを確認するようにしましょう。**

北海道警察サイバーセキュリティ対策本部

通信事業者・金融機関・宅配業者を装った
偽SMSにご注意ください!

※SMS（ショート メッセージ サービス）：携帯電話番号を用いて、短いメッセージを送受信する機能

SMSを利用しフィッシングサイトに誘導する手口に関する**北海道警察への相談が増加**しております。

通信事業者を装ったSMSの例

●●お客様センターです。ご利用料金のお支払い確認が取れておりません。下記リンクより確認が必要です。
https://bit.aaa.▲▲.xyz

金融機関を装ったSMSの例

お客様がご利用の口座に対して第三者からの不正なアクセスを検知しました。セキュリティ強化のため更新手続きをお願いします。
http://www.××○□○○△.com

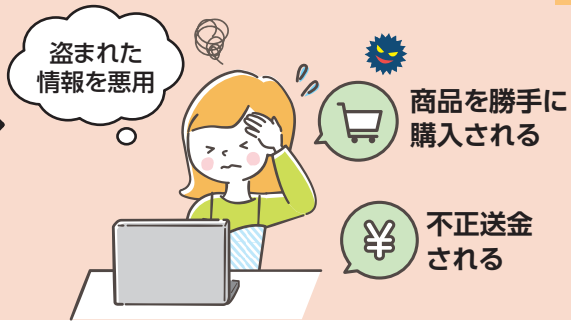
宅配業者を装ったSMSの例

お荷物のお届けに上がりましたが、不在のため持ち帰りました。下記リンクより再配達の手続きをお願いします。
http://www.○□△.org

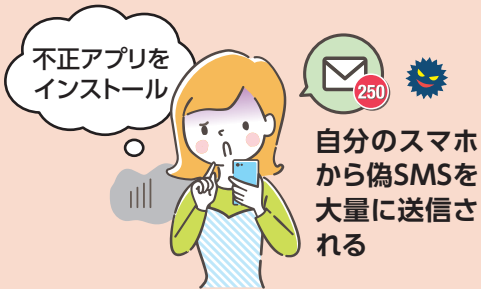
リンクをクリックしてしまうと…

<被害例>

ID・パスワード等の情報が盗み取られる



フィッシングサイトに誘導されて…



対策

被害にあわないために、注意しましょう

- ⚠ リンクを安易に開かない。
- ⚠ リンクを開いてしまっても、ID・パスワード等を絶対に入力しない。
- ⚠ サイトへのログインは、公式アプリや登録したブックマークからアクセスする。
- ⚠ 迷惑SMSブロック機能やセキュリティソフトを利用する。

北海道警察サイバーセキュリティ対策本部
警察相談ダイヤル【#9110】※通話料金がかかります
協力：トレンドマイクロ株式会社