

## 地域見守り情報



第249号

### その URL のクリック、ちょっと待って！ ～SMS やメールでの“フィッシング詐欺”に注意～

事業者や公的機関などの実在する組織をかたる SMS(ショートメッセージサービス)やメールを送信し、パスワードや ID、暗証番号、クレジットカード番号などの個人情報を詐取したうえ、クレジットカード等を不正利用するフィッシングに関する相談が後を絶ちません。

#### 事業者や公的機関などの SMS やメールを見るときは

- ・通販サイトや銀行など、日頃利用している事業者からでも、まずフィッシングを疑う。
- ・記載されている URL にはアクセスせず、事前にブックマークした正規のサイトの URL や、正規のアプリからアクセスする。
- ・事前のブックマークがない場合や、少しでも不安に思う点があれば、事業者等の正規のサイトでフィッシングに関する情報がないか確認する。

#### フィッシングサイトにアクセスしたと気づいたら

- ・ID やパスワード、クレジットカード番号等は入力しない。
- ・フィッシングサイト上のアプリをダウンロードしない。



#### フィッシングサイトに情報を入力してしまったら

- ・同じ ID やパスワードを使い回しているサービスはすぐに変更する。
- ・クレジットカード会社や金融機関などにも連絡する。

#### 日ごろからの事前対策は

- ・セキュリティソフトや携帯電話会社の対策サービス等を活用する。
- ・ID やパスワード等の使い回しをしない。
- ・クレジットカードやキャリア決済、インターネットバンキングの利用明細はこまめに確認する。

※困ったときはすぐに消費生活センターや市町村の消費生活相談窓口に相談してください。

消費者ホットライン「188(いやや)」番で最寄りの消費生活センター等につながります。