

ショッピングサイト・
金融機関・宅配業者

を装う**偽SMS**に**注意!**

そのメッセージ**本物**ですか?

ショッピングサイトを 装う偽SMSの例

- ・アカウント情報を入力させたり、偽のカスタマーセンターに電話するように仕向ける。

商品発送状況はこちら
でご確認ください。

<http://www.〇□△>

未納料金があるため
連絡してください。

01-2345-xxxx

金融機関を装う 偽SMSの例

- ・口座情報を入力させる。

口座への不正アクセス
を感知しました。

[http://www.xx〇□
〇〇△〇x](http://www.xx〇□〇〇△〇x)



宅配業者を装う 偽SMSの例

- ・アカウント情報を入力させたり、偽のアプリをダウンロードさせる。

不在のため持ち帰りま
した。配達物をご確認
ください。

[http://www.△x□x
□△□〇](http://www.△x□x□△□〇)



↓
**アカウント情報や個人情報、
クレジットカード情報などを入力してしまうと
情報が犯罪者の手に…**

対策

- ・SMSに記載のURLへアクセスしたり、問い合わせ先に連絡したりしない。
- ・企業やサービスの公式サイトやアプリからアクセスするようにする。
- ・セキュリティソフトを最新の状態で利用する。
- ・企業などが偽SMSに関する注意喚起を出していないか確認する。



そのワンクリック大丈夫?

メール内のURLや、Webサイト内のボタン・画像などをクリックした際に、「**入会登録が完了しました。料金をお支払いください**」などのメッセージを表示し、金銭を支払わせる手口が流行!

あたかも個人を特定したかのように見せかけるケースもあり、不安をあおって支払いに応じさせようとしています。



請求画面のイメージ



- こんな画面が出てきても、あわてず「無視」する。
- 連絡などは、絶対にしない。



もしも支払ってしまったら...

**愛媛県警察サイバー犯罪対策課 /
最寄りの警察署 / 消費者ホットライン188
等に相談しましょう!**

