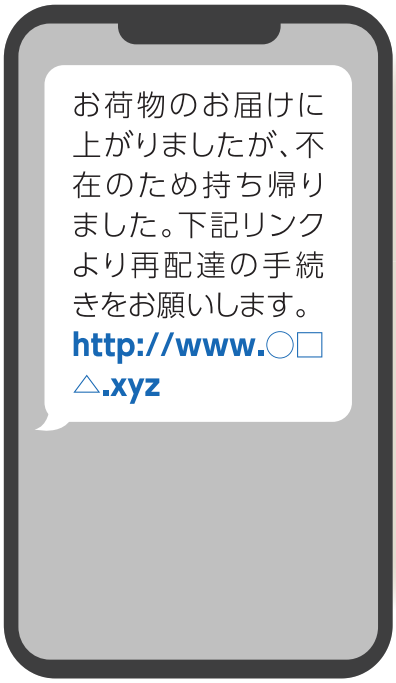
宅配業者を装った偽SMSにご注意ください

※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を使用したフィッシングサイトに関する相談が増加しています。



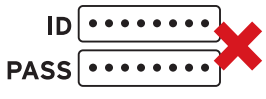
宅配業者を装ったSMSの例

リンクをクリックしてしまうと、フィッシングサイトに誘導されてID・パスワードなどの情報が盗み取られる

対策

1. リンクを不用意に開かない

2. リンクを開いてしまっても、ID・パスワードなどを絶対に入力しない



3. サイトへのログインは、公式アプリや公式サイトからアクセスする

4. 迷惑SMSブロック機能やセキュリティ対策ソフトを利用する

熊本県警察本部サイバー犯罪対策課　協力：トレンドマイクロ株式会社

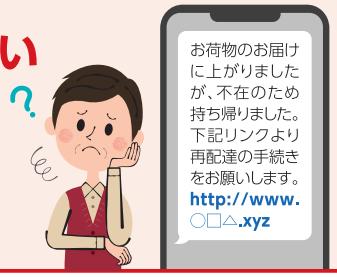
スマホを安全に使うためには

スマホでのキャッシュレス決済アプリの利用が年々増えています。
お財布のような存在になっているスマホですが、そのため不正利用の被害も…

スマホを使用する際には以下に気をつけましょう

メールや、SMS内のURL・リンクを不用意に開かない

大手企業などをかたる**偽メッセージ**から、**フィッシング詐欺の被害**にあわないよう、アクセスはブックマークに登録した**正規サイト**や、**公式アプリ**から行いましょう。



ご自身のアカウントを厳重に管理する

サービスごとに異なる、第三者に**推測されにくいIDとパスワード**を使用し、**二要素認証**※などを設定できる場合は必ず有効にしましょう。

※二要素認証とは2つの要素を組み合わせて認証することでセキュリティの強化を図る手法のこと。

スマホの画面ロックを設定する

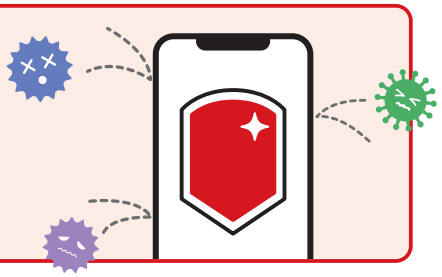
スマホの盗難、紛失時に**第三者に不正操作されないように、**パスワードや生体認証ロックを設定しておきましょう。

盗難紛失対策を設定しておく

盗難紛失時にスマホの捜索やロック、端末内の情報削除などができるよう、**盗難紛失対策機能**を設定しておきましょう。

セキュリティ対策ソフトを活用する

巧妙な詐欺サイトや**不正なリンクの判別**を行うセキュリティ対策ソフトを活用しましょう。



熊本県警察本部サイバー犯罪対策課　協力:トレンドマイクロ株式会社