スミッシングに注意
～そのショートメッセージは大丈夫？～


和歌山県警察マスコット
きしゅう君

スミッシングについて

1 スミッシングとは？

スマートフォン等モバイル機器で使用されるSMS（ショートメッセージサービス）を利用して、**正規の金融機関やショッピングサイトなどを装いメッセージを送りフィッシングサイトへ誘導し**、ID、パスワード、クレジットカード番号、氏名・住所などの**個人情報を入力させて盗む方法です。**

被害者を欺くため、通信業者や運送会社を装ったり、またウイルスに感染させるために**偽アプリのインストールを求める**手口もあります。

2 スミッシング被害

その1　銀行を装ったスミッシング

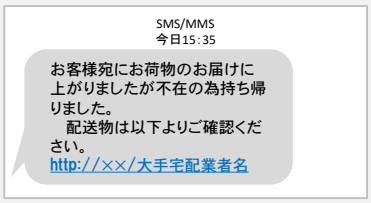
「お客様の口座が不正アクセスされました」等の**緊急対応を迫る内容でサイトにアクセスさせ、口座情報やパスワード等の入力を求める**ものが多くなっています。

この場合、口座番号やパスワードを入力してしまうと、たった数分でお使いの銀行口座からから見知らぬ口座へ不正に送金されてしまう被害に遭います。

●●銀行を装ったSMSの画面（イメージ）

たった数分で不正送金が！

その2　大手宅配業者を装ったスミッシング



←××運送を装ったSMSの画面（イメージ）

××運送を装った偽サイト画面（イメージ）

このようなショートメッセージが届き、**リンク先を開く**と右の画像のような**本物のサイトに似せた偽サイトにつながり、個人情報の入力を要求**されたりします。

被害としては、ギフトカード数万円分を勝手に購入されたという被害報告があります。

和歌山県内でも実際にショートメッセージが届き、個人情報を入力してしまったという相談があります。

怪しいメッセージを受信したとき

1 メッセージを受信したとき

送信先の名前は、相手の番号や企業名が表示されます。

身に覚えのない番号や名前の場合には気を付けてください。

また正規の企業から送信されたメッセージと同一のスレッド内に偽のメッセージが表示される場合も報告されていますので、**URLの確認**が必要です。

また相手への**折り返しの電話や返信は行わないようにしてください。**

正規のURLでない場合は、接続しないでください。

※ メッセージを開く前、URLに接続する前に一度よく考えてみましょう!

犯人側が勝手に設定した番号などが表示されます。

正規の企業名が表示される場合もあります。

正規のURLと同じでしょうか？

タップする前に確認してみましょう。

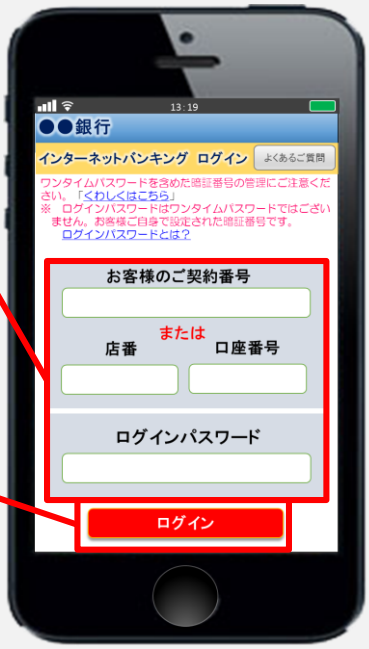
2 もしURLに接続してしまったとき

多くが本物のサイトに似せて作っている偽サイトにつながります。ID、パスワード、クレジットカード番号、氏名・住所などの**個人情報入力箇所がありますが、入力しないで通信を切ってください。**

入力してしまった場合も、「ログイン」や「次へ」の**ボタン類を押さずに通信を切ってください。**

また偽サイト上のページを押すと偽アプリのインストールが開始される場合がありますので**偽サイト上のページを押さずに通信を切ってください。**

※ 個人情報を入力しないようにしましょう!



ID、パスワード、クレジットカード番号、氏名・住所などの個人情報入力箇所がありますが入力しないでください。

「ログイン」や「次へ」などボタン類も押さないでください。

3 もし個人情報を入力してしまったとき

- パスワードを入力してしまった場合は、**サービスを提供している企業の正規のサイトから再度パスワードの変更**をしてください。
- クレジットカード番号や銀行口座の情報を入力してしまった場合は、**クレジットカードの停止や口座の停止などの措置**を行ってください。
- 実際にクレジットカードの不正利用などの被害にあった場合には、**お近くの警察署またはサイバー犯罪対策課にご相談ください。**

【発行元】 和歌山県警察本部サイバー犯罪対策課 073-423-0110㈹