# スミッシングに注意

## ~そのショートメッセージは大丈夫?~



## 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。



クレジットカード 番号

個人情報

## 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)

SMS/MMS 今日19:21

●●銀行を装う偽メールに注意 して、安全のために、設備ロック を行ってください。

http://

.jp/

.asp

SMS/MMS 今日13:35

【●●】お客様の●●銀行口座 に対し、第三者からの不正なア クセスを検知しました。ご確認く ださいhttp://●●ic.com 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

SMS/MMS

お客様宛にお荷物のお届けに 上がりましたが不在の為持ち帰 りました。

配送物は以下よりご確認くだ さい。

http://××/大手宅配業者名

←××運送を装った SMSの画面 (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。

#### ××運送を装った偽サイト画面(イメージ)

LANGUAGE 検索 メニュー		LANGUAGE	検索	メニュー	
× × Ex		× × Ex			
携帯電話の認証					
△△社から送られた製品はセキュリティ 許可の認証が必要となります。		課程コード: 検証コードを入力してください			
携帯番号; 携帯番号を入力してくださ 認証コード送信	<b>\$</b>	確認する			
サイトのご利用について   各種約款・公開情報  個人情報保護方針   ブライバシーボリシー   サイトマップ			引について   各種約却		
©1999-2019 × × Express Cottd. All Rights Reserved.		©1999-2019 × ×	Express CoLtd. All R	ights Reserved.	

# 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。

また偽サイトト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。