サイバー防犯通信

№62

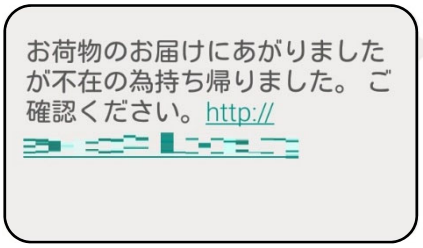
令和３年２月５日

兵庫県警察本部
サイバー犯罪対策課

～　本当に多発しています！　～

SMSからのフィッシングサイト誘導にご注意を！

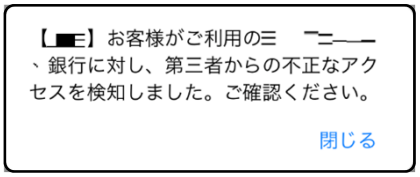
（SMSからフィッシングサイトに誘導する手口は「スミッシング」と呼ばれています）



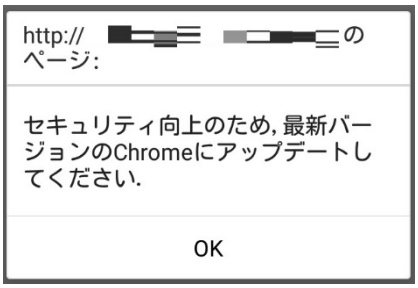
フィッシングメールの一例

【ある日、自分の端末にこんなSMSが…】
大手宅配業者（ヤマト運輸・佐川急便・日本郵便）はSMSでの不在通知は行っていません
宅配業者から来たSMSに記載されたリンク先URLはフィッシングサイトの可能性が極めて高いです

【宅配業者からなのに…銀行から不正アクセス？？】
宅配業者の不在メールなのに銀行のサイトへアクセスするのはフィッシングサイトへの誘導の可能性が高いです



リンク先表示の一例　①



リンク先表示の一例　②

【あれ？なぜかセキュリティ更新を求められた…】
宅配業者の不在メールなのにセキュリティ強化を求めてくるのはフィッシングサイトへの誘導の可能性が高いです

誘導されたフィッシングサイトの一例

【あれあれ？最終的に銀行のサイトに誘導された…】
口座番号、アクセス用パスワードを入力したら、次にワンタイムパスワードの入力を求められた！
ワンタイムパスワードの入力を求めるのはフィッシングサイトの可能性が高いです！！

Check!

～～防犯ポイント～～

被害に遭わないために、SMSに記載されたリンク先に容易にアクセスしないようにしてください。
以下の点に留意することも重要です。
- **事前に正しいウェブサイトのURLをブックマーク登録し、ブックマークからアクセスする**
- **表示されたウェブサイトのURLを確認する**
- **インターネットバンキングの口座情報やワンタイムパスワードの入力を求められた場合は、直ちに入力を中止し、金融機関の正規サイトを確認する、又は問合せ先に連絡する**

注意喚起動画URL　：　公益財団法人警察協会ホームページ　（　サイバー犯罪、鷹の爪団のサイバー犯罪撲滅大作戦【フィッシング編】　）
https://api01-platform.stream.co.jp/apiservice/plt3/NDI4Nw%3d%3d%23MjM4%23280%23168%230%2333E6A0586400%23MDoyOjc6YTpmOzEw%23

記事引用元　：　一般財団法人日本サイバー対策センター（JC3）　～フィッシングによる不正送金の被害に注意～
独立行政法人情報処理推進機構（IPA）安心相談だより　～宅配便業者をかたる偽ショートメッセージに引き続き注意！～