ぐんま版消費者教育教材

１６　相談事例　⑦フィッシング詐欺

群馬県　生活こども部　消費生活課

令和５年２月作成

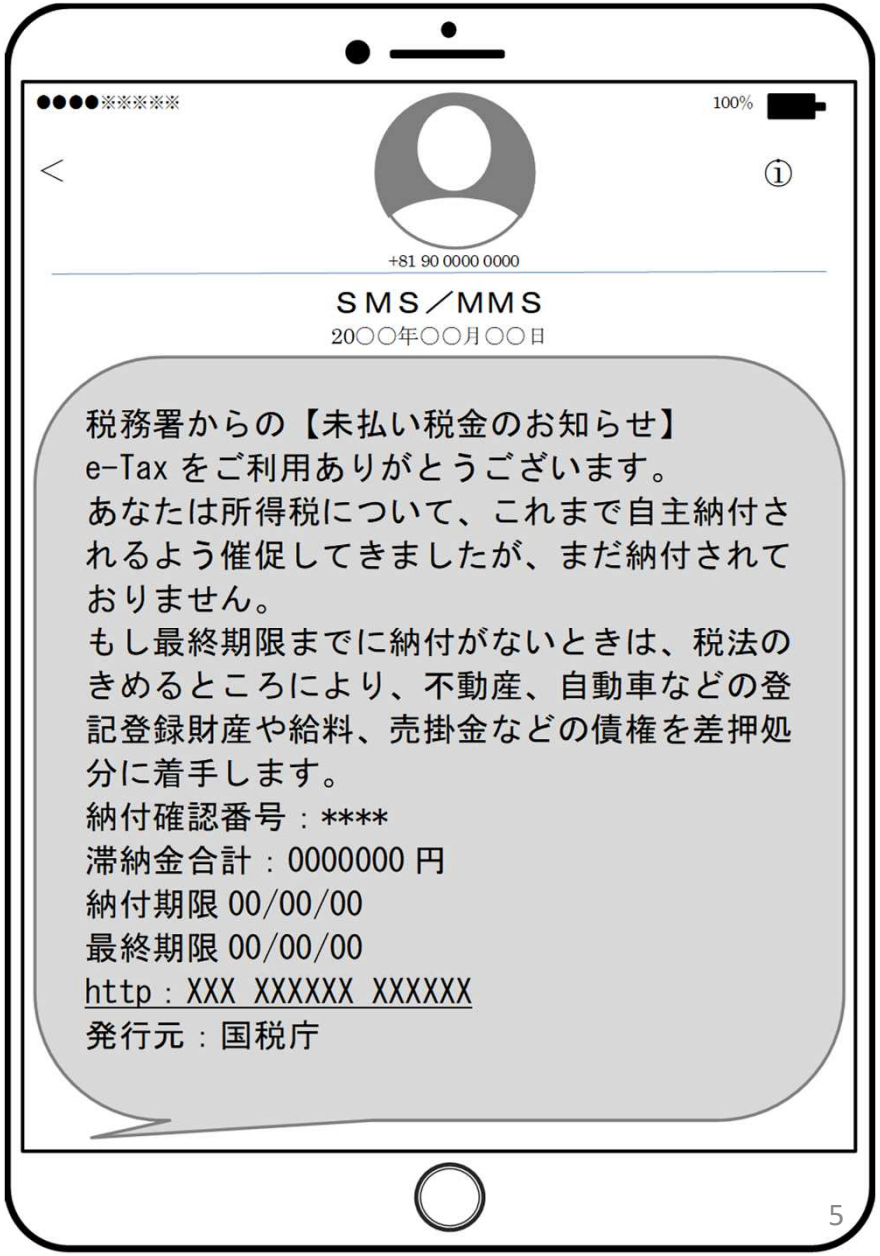
フィッシング詐欺

SMSやメールに、宅配会社、クレジット会社、銀行、ネット通販会社、フリマアプリ、携帯会社、国税庁などになりすまし、「荷物を届けたが不在だった」、「未払いがあり、要連絡」との嘘の通知が届くことがあります。
なりすましメールのURLを押して、指示に従って操作すると、個人情報を盗まれたり、スマートフォンが乗っ取られて勝手にメールを送られたり、盗まれたアカウントで勝手に通販で買い物されるなどの被害に遭います。これをフィッシング詐欺といいます。

銀行の不正利用のお知らせになりすましたSMS

携帯会社になりすましたSMS

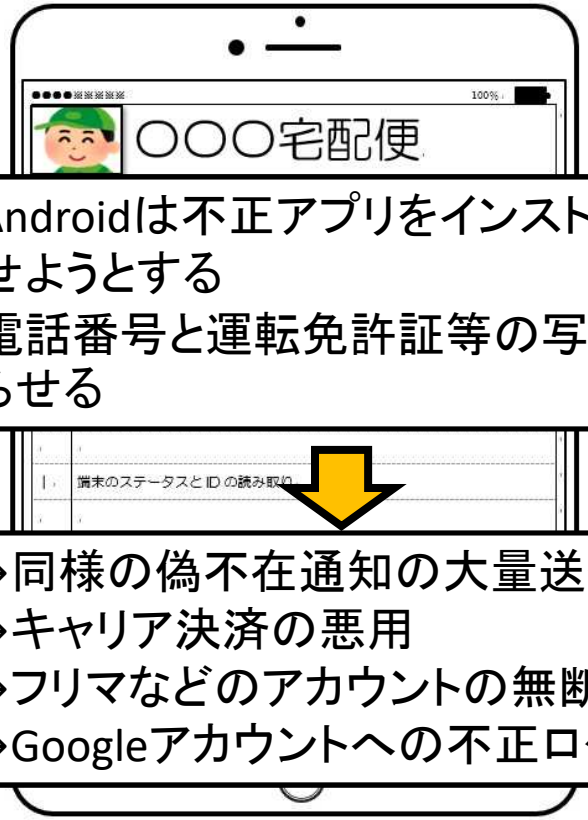
国税庁になりすましたSMS



宅配便の不在通知になりすましたSMS

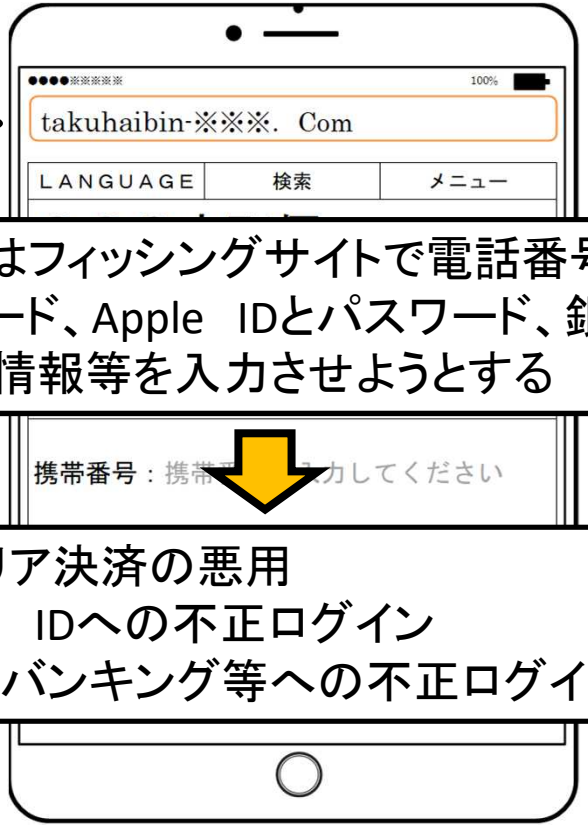
宅配の不在配達通知を装った SMSのトラブル事例のイメージ

画面上でどこをタップしても
次の画面に進む。



Androidは不正アプリをインストールさせようとする
電話番号と運転免許証等の写真を送らせる

→同様の偽不在通知の大量送信
→キャリア決済の悪用
→フリマなどのアカウントの無断作成
→Googleアカウントへの不正ログイン



iPhoneはフィッシングサイトで電話番号と認証コード、Apple IDとパスワード、銀行の認証情報等を入力させようとする

→キャリア決済の悪用
→Apple IDへの不正ログイン
→ネットバンキング等への不正ログイン

不審なSMSやメールが届いても

①心当たりのない相手からのSMSやメールは開かずに削除する。

・件名に「緊急」「重要」「セキュリティ」とある場合でも無視。

②メール内のURL・リンクは絶対にクリックしない。

・本物の業者からのメールだと思っても、公式アプリや
公式ホームページから業者のサイトにアクセスする。

③住所、氏名などの個人情報やアカウント、パスワード、クレジット番号などの入力は絶対にしない。

・個人情報を入力する必要がある場合は、改めて公式サイトに
接続してから入力する。

被害に遭ってしまったら

①不審なアプリをインストールした場合は、すぐに機内モードに切り替える。

②不審なアプリをアンインストール。

③スマホに紐付いたアカウントのパスワードを変更する。

④クレジットカードやキャリア決済の支払い情報を確認し、身に覚えのない支払いがあれば、すぐにカード会社、携帯会社、警察などに通報する。

⑤ IPA（情報処理推進機構）にも相談。

【解説】
16　相談事例⑦　フィッシング詐欺

③2～7頁　「なりすまし偽SMS」

有名企業、銀行、クレジットカード会社、ネットモール、宅配業者、デパートや友達を騙ってメールが届き、メール内のURLやリンクをクリックすると、個人情報が盗まれ、アカウントが乗っ取られることがあります。勝手に買い物される。銀行口座からお金が引き落とされるなど、経済的な被害に遭う相談が急増しています。普段から迷惑メール対策をしたり、個人情報の入力を求められたら警戒しましょう。

④9頁　「IPA」

IPAとは「独立行政法人情報処理推進機構」のことです。

IPAのホームページではワンクリック請求の対策や請求画面の削除方法が紹介されています。

IPAでは「情報セキュリティ安心相談窓口」を開設しており、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対し、電話やメール、FAXや郵送で相談を受け付けし、アドバイスを行っています。

●URL　　http://www.ipa.go.jp/security/

●電話：03－5978－7509　　受付時間10:00～12:00／13:30～17:00

土日祝日・年末年始は除く

（※新型コロナウィルスの感染拡大に伴う緊急事態宣言等によって、電話相談窓口が停止している場合があります。）

④9頁 **「IPA」の続き**

●メール：anshin@ipa.go.jp
●FAX：03－5978－7518
●郵送：〒113-6591　東京都文京区本駒込2-28-8
　　文京グリーンコート　センターオフィス16階
　　IPAセキュリティセンター　安心相談窓口

④12～13頁 **「普段からの注意点」「個人情報等を入力してしまったら」**
参考資料としてご活用ください。

フィッシング詐欺への普段からの注意点

①迷惑メールフィルターを設定する

・各携帯電話会社やプロバイダの多くは無料でフィルタリングを提供しています。自分の環境にあった設定をしましょう。

②セキュリティソフトを利用する。

・各携帯電話会社が提供するセキュリティーサービスやセキュリティ対策ソフト提供会社のセキュリティソフトを利用しましょう。

③スマホのOSは常に最新に。

・古いOSを使っていると、ウイルス感染の危険性が高くなるので、更新の通知が来たら、速やかにインストールしましょう。

④利用するサービス毎に異なるパスワードを登録。

・複数のサービスで同じパスワードを使用すると、情報漏洩したときに、別のサービスでも不正利用される可能性があります。

もし個人情報等を入力してしまったら

①当該サイトのパスワードを変更する。

・同じID・パスワードの組み合わせで登録しているサイトのID・パスワードも変更する。

②漏洩したパスワードを使っているサイトへの連絡

・通販サイトのサポート窓口に連絡する。

・携帯電話会社に不正なキャリア決済の有無を確認。

・金融機関で口座凍結の手続きをする。

・クレジットカード会社へカードの利用停止やカード番号の変更など不正利用防止の手続きをする。