偽ショートメッセージによる被害にご注意！

宅配便の不在通知やAmazon等の通信販売事業者を装うSMS（ショートメッセージサービス）を使い、金融機関等をかたるフィッシングサイトへ誘導してID、パスワード、クレジットカード情報等を入力させる通称スミッシング詐欺や偽サイトに誘導してコンピュータウイルスに感染させ、大量のSMS送信や不正購入による代金等を請求される被害が発生しています。

偽ショートメッセージによる犯行手口

犯　人

（偽SMSの例）　SMS/MMS　9月30日(水) 3:01

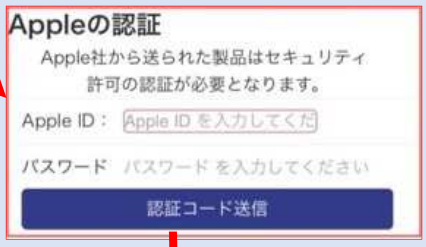
Amazon アカウントの情報を更新する必要があります。https://account.amazon[redacted].com/

お荷物のお届けにあがりましたが不在の為持ち帰りました。 ご確認ください。http://[redacted].duckdns.org

URLをクリックしてしまうと…

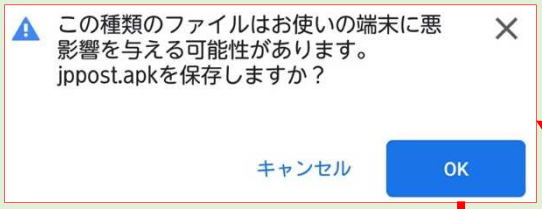
iPhoneの場合

ID、パスワード等を入力させるフィッシングサイトへ誘導



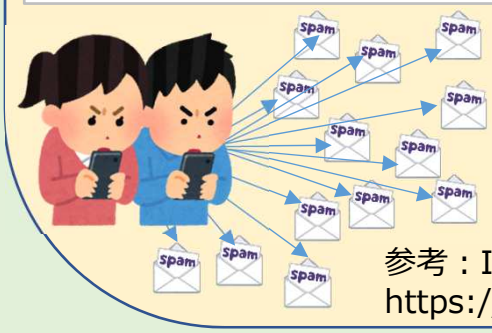
Androidの場合

不正なプログラム（コンピュータウイルス）をダウンロードさせる偽サイトへ誘導



表示されたボタンをクリックしてしまうと…

- 身に覚えのない高額な請求がくる
- 苦情電話が掛かってくる
- 大量のSMSが送信される
- ログインできなくなる
- アカウントが乗っ取られる
- 個人情報がネット上に流出してしまう
- フリマサイト等になりすまし登録される　等



偽SMSに記載されたリンク先（https://●●●●●.org等）は、
絶対にクリックしないで下さい！！

偽SMSの送信元（携帯電話番号等）には、
電話をかけたり、メッセージを返信しないで下さい！！

参考：IPA 安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayori20200220.html

最新セキュリティ情報はこちらから

2020年12月1日 発行

鳥取県警察本部
総合相談電話　☎　＃9110
サイバー犯罪対策課　警部補　福井 貴
☎　0857-23-0110　（内線　3424）
URL　https://www.pref.tottori.lg.jp/police/