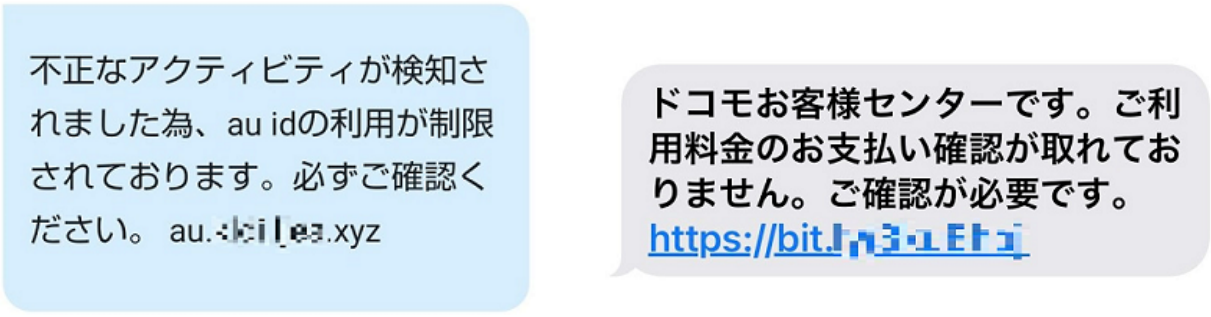
サイバー防犯通信

令和3年6号
兵庫県警察本部
サイバー犯罪対策課

SMSからのフィッシングサイト誘導にご注意！
～通信事業者を装ったフィッシングが増加傾向！～

（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。）

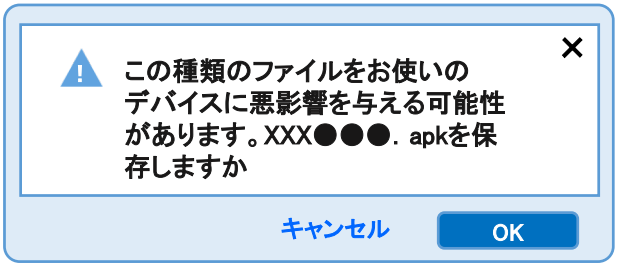
電子メールやSMS（ショートメッセージサービス）を利用して、通信事業者を装ったフィッシングサイトに誘導する手口が増加しており注意が必要です。



通信事業者を装うSMSの一例

フィッシングメール/SMSの送信元は偽装されている場合があります。また、利用者の不安をあおり、早急に確認を促す内容も見られます。
メッセージに含まれるリンク先をクリックしてしまうと、当該通信事業者を装ったフィッシングサイトへ誘導され、利用者のID・パスワード等が詐取されてしまうおそれがあります。
フィッシングサイトは見た目では本物との判別が難しく、「https://」で始まるフィッシングサイトも存在するので注意が必要です。

Android端末では、不正アプリのインストール画面が表示される場合があります。
指示通りに不正アプリをインストールしてしまうと、ウイルスに感染し、自身の端末がこの種のSMSの送信元となってしまう場合もあります。



不正アプリダウンロードの例

Check!

～～防犯ポイント～～

SMSに記載されたリンク先に安易にアクセスしないようにしてください。
- 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
- アプリのインストールは、正規のアプリ配信サイト等信用できるサイトから行う
- ID、パスワードを入力する際は、公式サイトであることを確認したうえで入力する

JC3記事リンク先
二次元コード

記事引用元：一般財団法人日本サイバー対策センター（JC3）「通信事業者を装ったフィッシングの注意喚起」