青い森のサイバーセキュリティ

令和３年10月
青森県警察本部保安課
サイバー犯罪対策室

各種事業者を装ったフィッシングに注意！

運送事業者・通信事業者を装う偽メール

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、運送事業者や通信事業者など各種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います。

メッセージの送信元も当該企業に偽装されている場合があり、見分けがつきにくくなっていますが、メッセージ中に含まれるリンクをうっかりタップしてしまうと、フィッシングサイトへ誘導され、利用者のID・パスワード等がだまし取られてしまう恐れがあります。

図　運送系企業を装ったSMSの例

「https://」で始まるフィッシングサイトも存在

フィッシングサイトは、巧妙で見た目では本物との判別が難しくなっており、以前はあまり見られなかったＵＲＬが「https://」で始まるサイトも存在しています。

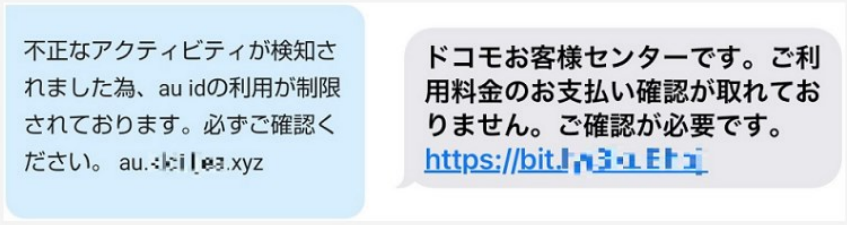

図　通信事業者を装ったSMSの例

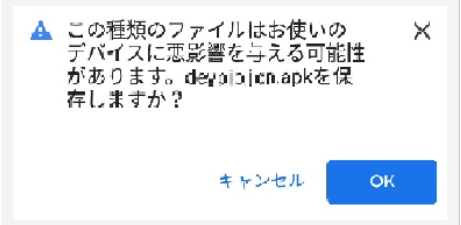

図　不正アプリダウンロードの例

Android端末では、アプリのインストール画面が表示される場合もありますが、ウイルスが仕込まれた不正アプリであることが多く、指示通りにアプリをインストールしてしまうと、自身の端末がフィッシングＳＭＳの送信元として使われてしまう可能性があります。

被害に遭わないために留意するポイント

- メールの中のＵＲＬや画像等をクリックせず、必ず**自分のブックマークや専用アプリからログイン**して確認する。
- アプリのインストールは公式ストア等、信頼できるサイトからのみ行う。
- ＩＤ，パスワードの入力時は必ず信頼できるサイトであることを確認する。
- メールやメッセージの文面は安易に信用しない。特に「**警告**」や「**セキュリティの確認**」などの内容に注意。

出典：一般財団法人日本サイバー犯罪対策センター, “通信事業者を装ったフィッシングの注意喚起“,
https://www.jc3.or.jp/threats/topics/article-382.html