サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和元年
9月11日
Vol.34

宅配業者をかたるスミッシング対策

宅配業者をかたりスマートフォンのＳＭＳを使って偽のメッセージを送信しフィッシングサイトに誘導するスミッシングにより、不正アプリをインストールさせたり個人情報を盗み取られる被害が発生しています。

被害に遭わないためにはどんな対策が必要？

ステップ１

ＳＭＳで偽の不在通知を受信したら・・・

対策

受信したＳＭＳ記載のＵＲＬをタップしない！

ＳＭＳに記載されたＵＲＬにはアクセスせず、業者に電話するか不在票等で事実確認をする。

ステップ２

誤って記載されたＵＲＬをタップしてしまったら・・・

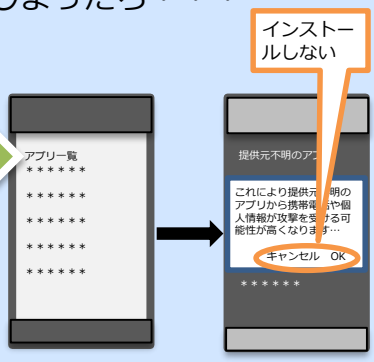
対策

サイトが表示されても画面上をタップしない

もし間違えてリンク先にアクセスしたとしても、不用意に画面上をタップしない。

ステップ３

偽サイトで画面をタップしてしまったら・・・



対策

「提供元不明のアプリ」をインストールしない！

提供元不明のアプリや、警告が表示されるようなアプリはインストールしない。

不正アプリをインストールしてしまった時はどうしたらいい？

・スマートフォンを**機内モード**に設定する。これにより通信を無効化し、不正アプリによる**メッセージ送信を抑止**することが可能です。同時に、スマートフォンから**個人情報等が外部に送信されることも抑止**することができます。
・機内モードの状態でアプリを確認し、悪意のあるアプリと判明すれば**アンインストール**を実施するほか、スマートフォンの**初期化**を検討しましょう。
・アカウントの**パスワードを変更**し、**キャリア決済の履歴確認**をしましょう。
・身に覚えのない決済があれば、連絡窓口や販売店に連絡して**キャリア決済を停止**してもらい、警察に連絡しましょう。

参照元：https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

相談窓口

愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110