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2年
7月8日
Vol.47

宅配業者の「不在通知」をかたるフィッシングに注意

宅配業者を装った偽のＳＭＳやメールにより偽サイトへ誘導され、不正アプリをインストールさせられたり、個人情報を窃取されたりする被害が発生しています。

【宅配業者を装った偽の不在通知メッセージ例】

※ 大手ショッピングサイト、携帯電話事業者、金融機関を装っている場合もあります!!

記載されたＵＲＬにはアクセスしない。
→ 偽サイトにアクセスしてしまいます!!
（正規の連絡先に電話するか不在票等で事実確認をする。）

URLをタップしてしまったら・・・

Androidの場合

提供元不明の不正なアプリをインストールさせられる

不正アプリのインストール後、偽の警告メッセージによりフィッシングサイトに誘導され、IDやパスワード等の個人情報を窃取される手口もある。

＜影響＞
- 自身の端末から大量のSMSが勝手に送信される。
- 端末内のデータを不正に使用され、キャリア決済サービスを利用されたり、アカウントを勝手に作成されたりして、不正使用される可能性がある。

不正アプリをインストールしてしまったら・・・

iPhoneの場合

Apple IDやパスワード、認証コードを入力させられる

最近ではApple ID等の入力のほか、「不正ログインが発生した」という偽のメッセージを表示して、実在する銀行のインターネットバンキングのアカウント情報を入力させられる手口もある。

Apple IDやパスワード、認証コード等を入力しない。

＜影響＞
- アカウントの不正ログインや不正使用

- ○ スマートフォンを**機内モード**に設定し、通信の無効化を図る。
- ○ 不正アプリを**アンインストール（削除）**するとともに、ダウンロードフォルダからも削除を行う。（不正アプリがホーム画面に表示されていない場合、設定のアプリ一覧を確認する。）
- ○ スマートフォンの**初期化**を検討する。
- ○ アカウントの**パスワード**を変更し、**キャリア決済の請求**や**利用履歴**を確認する。身に覚えのない決済があれば、**連絡窓口や販売店に連絡**した上で**警察にも相談**する。

対　策

- ○ **フィッシングの手口を知る。**
- ○ **SMSやメールに記載されたURLを安易にタップしない。**
- ○ **パスワードや認証コード等を安易に入力しない。**

参照元：IPA(https://www.ipa.go.jp/security/anshin/mgdayori20200220.html)

相談窓口

愛媛県警察本部サイバー犯罪対策課 TEL089-934-0110(代)