

あさまセキュリティニュースレター



スマートフォンのSMSを利用した運送系企業のフィッシング急増中！(2019年5月17日)

↑携帯番号で送れるショートメッセージサービス

攻撃パターン



URL からアクセス
してしまおう...

Android端末
不審アプリを
インストールさせる手口

iPhone
フィッシングサイトで
「Apple IDとパスワード」や
「電話番号と認証コード」を
入力させる手口

iPhone **追加**
不審な構成プロファイル
をインストールさせたあと、
フィッシングサイトに誘導
する手口

偽のログイン画面



フィッシング対策協議会

HP抜粋

JC3 HP抜粋

今回のSMSを利用してフィッシングサイトに誘導する手口（スミッシング）が、今後も増えそうです。AppleIDの詐取され、身に覚えのないAppleコンテンツ等の請求が発生といった被害が！SMSからの攻撃があることを知りご注意ください！！



攻撃のパターン

- SMSを利用し、偽サイトに誘導、偽のアプリをインストール、AppleID等の入力をさせる
- 不正に入手した情報で決済サービス等を利用、その他サービスへの不正アクセスも
- 不正アプリインストールさせることにより、スマホ内の情報搾取、スマホ画面をロックし金銭要求、他のSMS宛に勝手に配信等、様々な攻撃

被害

サービスの不正利用

情報搾取

身に覚えのない請求

不正アプリインストールによる様々な被害

対策

- SMSを利用した攻撃の手口を知る、SMSのフィルタリング設定を見直す
- 手口、本文の内容等、巧妙化しているため、少しでもおかしいと思ったら、サービス提供元に確認する
- 最新の情報を得る、最新の脅威を知る、手口を知る、セキュリティに対し常に意識をもつ

情報源

フィッシング対策協議会 <https://www.antiphishing.jp/>

日本サイバー犯罪対策センター <https://www.jc3.or.jp/> JC3で検索！（Amazon、Line、Apple等、偽メールの最新情報掲載）