スマホ決済の不正利用に御用心

スマートフォンの普及に伴い、キャッシュレス決済の1つであるスマートフォンを利用した決済（スマホ決済）が登場しました。政府の推進したキャッシュレス・ポイント還元事業などを機に利用を始めた方も多いのではないでしょうか。

スマホ決済は、財布いらずでスピーディーに支払いをすることができ、コロナ禍の中では現金に直接触れる必要がないということから注目されていますが、利便性の反面、第三者のなりすましによるサービスの不正利用や連携口座からの不正な引き出し等が問題になっています。

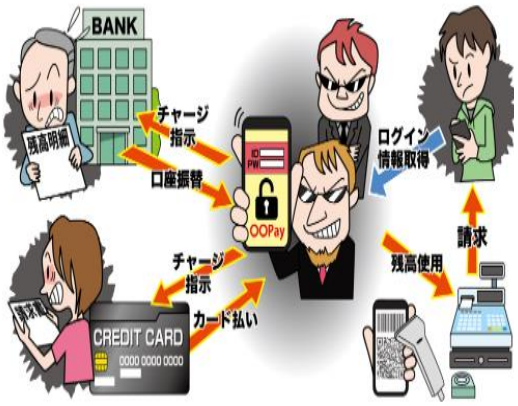
○ 攻撃手口

● パスワードリスト攻撃

- 何らかの方法で入手した認証情報（アカウント）をリスト化し、それを利用して複数のサービスへのログインを試みる攻撃で、複数のサービスでパスワードを使いまわしている場合、1つの認証情報（ID とパスワード）が漏えいすると他のサービスに不正ログインされるおそれがある。
- 二要素認証等のセキュリティ機能を利用している場合、不正ログインされる危険性は減少する。

● セキュリティ上の不備を悪用

- 決済用システムやアプリの脆弱性を悪用し、利用権者が意図しない不正な決済がされるほか、連携している他のサービスも狙われる場合がある。
- 二要素認証等のセキュリティがより強固な認証方式を利用していない場合、攻撃が成功しやすい。



（出典　IPA 独立行政法人情報処理推進機構）

対策

● 多要素認証の活用

ワンタイムパスワードや指紋認証など、複数の認証方式を組み合わせ、セキュリティを向上させる。

● アカウントの適切な管理

パスワードリスト攻撃への対策として、パスワードの使い回しはせず、利用する各サービスのアカウントごとに、長く複雑なパスワードを設定する。

また、利用頻度が低いサービスや不要なサービスのアカウントは削除する。

● パスワード管理ソフトの利用

利用するサービスの増加に伴い、各サービスごとのアカウントの管理が煩雑だと感じる場合は、パスワード管理ソフトの利用も検討する。

● 添付ファイルやリンク先を不用意に開かない

犯罪者は、フィッシングサイトに誘導して、認証情報などを収集しようとするので、添付ファイルやリンク先を不用意に開かない。

● 過剰なチャージはしない

被害額を抑えるために、過剰なチャージはしない。

【参考】　IPA 独立行政法人情報処理推進機構

情報セキュリティ 10 大脅威 2021 ［個人編］ https://www.ipa.go.jp/files/000089480.pdf

岩手県警察本部サイバー犯罪対策課の公式ツイッターはQRコードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

@Iwate_cyber

岩手県警察本部生活安全部サイバー犯罪対策課

令和3年 10 月1日発行