2023 年 2 月 6 日

総務課　楢崎

スマートフォンの情報セキュリティ対策について

お疲れ様です。総務課の楢崎です。

今日は皆さんが使われているスマートフォンの情報セキュリティについてお話したいと思います。

皆さんがお持ちのスマートフォンを利用することで様々なサービスが利用できますが、

その際右図のように様々な利用者情報が蓄積されます。これらの情報は、アプリケーションを通じて広告配信事業者などへ提供され、利用者の趣味・趣向に応じた広告の表示などに利用される場合もあります。

（提供：総務省）

その情報が悪用されると様々な影響が出てしまうので注意が必要です。

次に、「情報セキュリティ 10 大脅威　2022」を紹介したいと思います。

これは 2021 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、情報セキュリティ分野の研究者、企業の実務担当者約 150 名の審議・投票で決定したものです。

なお、ランキングは個人、組織で別々に発表されるのですが、今回は個人についてを紹介します。（もちろん、個人と言っていますが、組織にも当てはまります）

（出典：IPA 情報セキュリティ 10 大脅威2022）

1. **フィッシングによる個人情報等の詐取**
2. **ネット上の誹謗・中傷・デマ**
3. **メールや SMS 等を使った脅迫・詐欺の手口による金銭要求**
4. **クレジットカード情報の不正利用**
5. **スマホ決済の不正利用**
6. **偽警告によるインターネット詐欺**
7. **不正アプリによるスマートフォン利用者への被害**
8. **インターネット上のサービスからの個人情報の窃取**

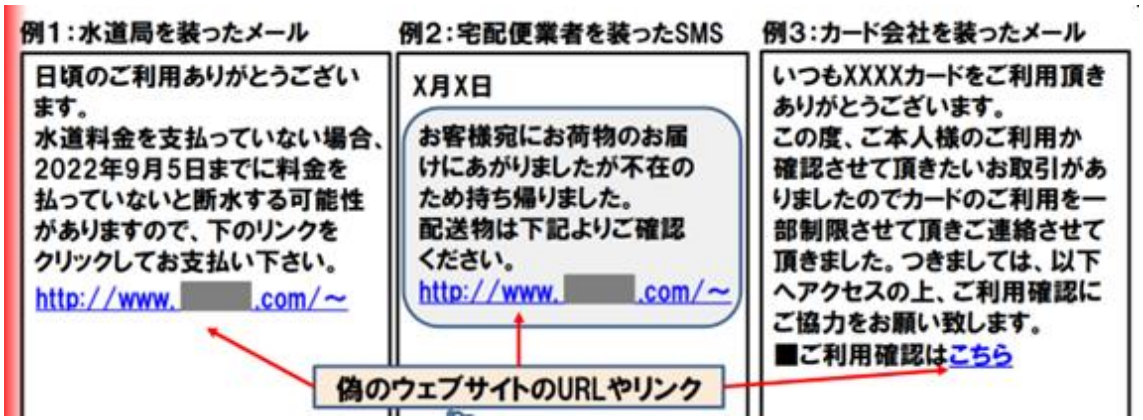
9.　インターネットバンキングの不正利用
10.　インターネット上のサービスへの不正ログイン

多くの方が所持されているスマートフォンは、手軽に使用できることからどうしても気が緩んでしまうことから、これまで以上に上記の脅威に注意を向け、安全に使用する必要があります。

上記の「情報セキュリティ 10 大脅威 2022」のうち、「1. フィッシングによる個人情報等の詐取」「5. スマホ決済の不正利用」「6. 偽警告によるインターネット詐欺」について紹介したいと思います。

1.　フィッシングによる個人情報等の詐取

フィッシングは実在する様々な公共機関や企業を装い、以下のように様々な内容のメールや SMS を送り付けて利用者を騙そうとしてきます



（出典：IPA 情報セキュリティ 10 大脅威2022）

⇒メールや SMS は偽物ではないかと疑うという心構えが大事です
そのためには、メールや SMS には慌てさせたり、心配させられるような記載があっても
まずは一呼吸おくことが大切です。

5. スマホ決済の不正利用

スマホ決済サービス(PayPay とか)のアカウントが乗っ取られると、チャージ済みの残高を利用して決済されたり、また登録口座から勝手に残高をチャージされて使われたりする恐れがあります。

・盗んだ ID やパスワードを使ってサービスに不正ログイン

⇒対策は上のフィッシング対策を参照

・”パスワードの使いまわし”をしている人を狙って不正ログイン
⇒・パスワードの使いまわしをしないようにしましょう
・パスワードは長く、複雑なものにしましょう

6. 偽警告によるインターネット詐欺

インターネットを閲覧中に「あなたのパソコンがウイルスに感染している」など
の警告（偽警告）が表示され、電話のサポート窓口へ誘導されます。その窓口に
電話すると、不要なサポート契約やソフトウェアの購入を勧められ金銭被害に
つながります

（出典：IPA 情報セキュリティ 10 大脅威2022）

⇒不安に感じる警告が表示されても、慌てて言われるがままに対応しない。
警告の内容は様々ですが、偽物なのか本物なのか判断ができない場合は警告の指示に
安易に従わず、まずは信頼できる人に相談しましょう。

冒頭でも述べましたが、スマートフォンを利用すると様々な有益なサービスを利用することができます。
当社内でも、勤怠管理（VG クラウド）、年末調整に加え、給与明細の電子化が始まります。
また、今後は elgana というビジネスチャットも導入する予定です。
（※elgana とは、NTT グループ公式のビジネスチャットで、LINE と違いビジネスに特化した作りになっています。詳細は後日紹介します）

そんなスマートフォンを安全に使用するため、以下に示した情報セキュリティ対策の基本を押さえ、有益に活用してみてください。

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

（出典：IPA 情報セキュリティ 10 大脅威2022）

最後にクイズです。
以下の１～４の中でもっとも安全なパスワードはどれでしょうか。

1. 92674538
2. nR9Wj8vZ
3. m9Wu1f
4. w5ux8psf

⇒答え　2
大文字の英字が入っており、3 よりも桁数が長いので、この中ではこれが一番安全。（記号や桁数が長くなればさらによい）
これでも最新のコンピュータを使えば解析可能ですので、単純な 12345678 や abcdefgh などは論外です。