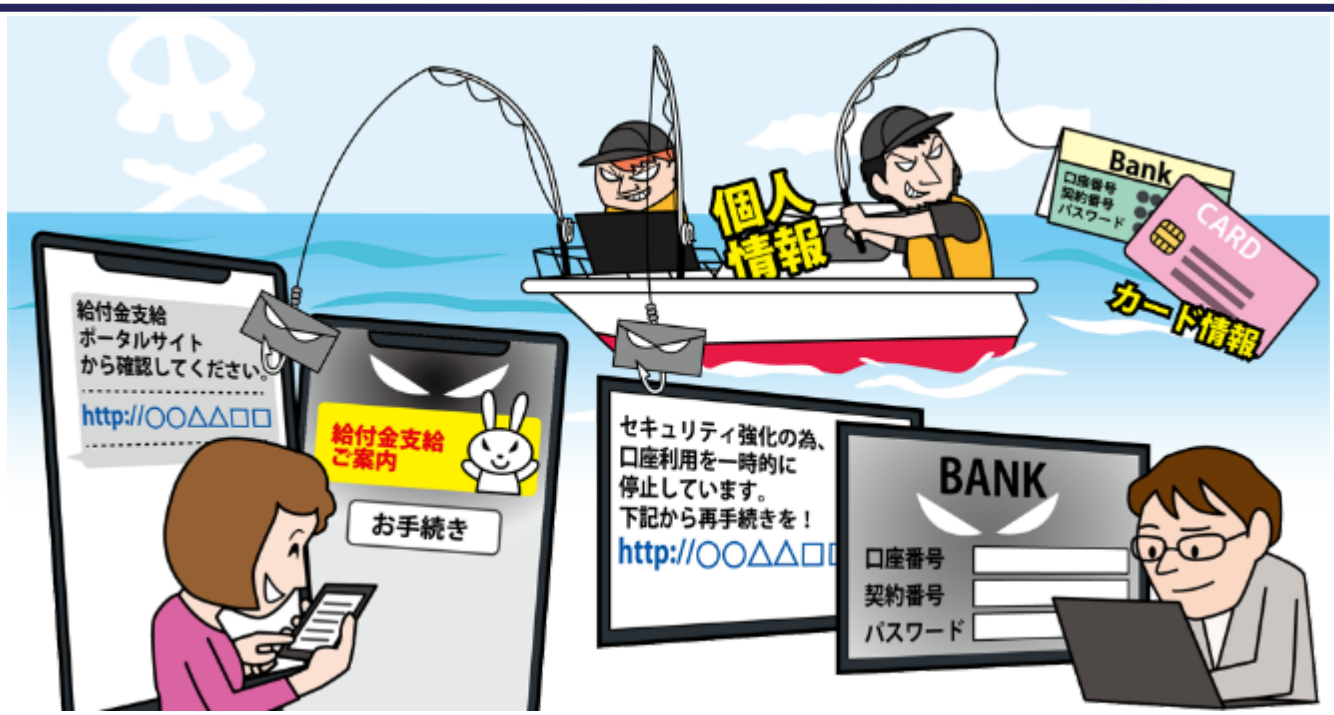
フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～



- 金融機関や有名企業を装ったフィッシングサイト（偽のWebサイト）へ利用者を誘導する
- フィッシングサイト上でIDやパスワード、クレジットカード情報等の個人情報を入力させて窃取する

【参考】 URLリンクへのアクセスに注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

IPA

♦ 攻撃手口

・攻撃者が用意した偽のサイトに情報を入力させて詐取

- **フィッシングサイトへ誘導するメール等を送信**
  - 攻撃者が公的機関や有名企業のWebサイトを模倣したフィッシングサイトを用意する
  - 公的機関や有名企業を装ったメールやSNS、SMSを不特定多数に送信し、フィッシングサイトに誘導する
  - 近年ではSMSによる誘導（スミッシング）が多くみられるが、QRコードによる誘導（クイッシング）も見られている
  - フィッシングサイトで利用者が入力した情報を詐取する
- **検索サイトの検索結果に偽の広告を表示させる**
  - 検索エンジンの検索結果等に表示される広告の仕組みを悪用して虚偽の不正な広告を表示させ、フィッシングサイトへ誘導する

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向①**
  - **給付金の受給申請を装ったフィッシング**
    - 2023年12月、デジタル庁はマイナポータルを騙った詐欺メールおよび偽サイトについて注意喚起を行った
    - 詐欺メールの件名は「電力・ガス・食料品等価格高騰緊急支援給付金（5万円／1世帯）のご案内」等とされており、給付金の受給申請を促して偽のマイナポータルサイトへ誘導する内容であった
    - 誘導先のサイトでは個人情報、クレジットカード情報等の入力が求められ、入力するとその情報が窃取される

【出典】 マイナポータルをかたるフィッシング（2023/12/06）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/mynaportal_20231206.html
マイナポータルを騙った詐欺メール及び偽サイト（フィッシング詐欺）に関する注意喚起（デジタル庁）
https://www.digital.go.jp/news/4750a8f5-1061-4ae6-903b-cfb327a50465

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向②**
  - **フィッシングを発端としたインターネットバンキング不正送金被害急増**
    - 2023年12月、 警察庁と金融庁が連名で、メールやSMSに記載されたリンクからアクセスしたWebサイトにIDやパスワード等を入力しないよう注意喚起を行った
    - 2023年1月から11月末におけるフィッシングによるものとみられるインターネットバンキングの不正送金の被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新している

【出典】 2023年4月24日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230424_press3.pdf
2023年8月8日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf
2023年12月26日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向③**
  - **QRコードを用いたフィッシング攻撃に注意**
    - 2023年12月5日、米連邦取引委員会はQRコードに隠された有害なリンクに注意するよう警告文を公開した
    - 2023年11月、サイバー情報共有イニシアティブ（J-CSIP）においても、マイクロソフトを装った、QRコードを用いたフィッシングメールを確認していることを公開している
    - フィッシングメールではQRコードを読み取ってメールアカウント情報を期限までに更新するように促す内容であり、QR コードを読み取ることでフィッシングサイトが開かれるものであった

【出典】 米FTC、QRコードを用いた「クイッシング」攻撃について注意喚起（CNET Japan）
https://japan.cnet.com/article/35212658/
サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年7月～9月]（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf

♦ 対策

• インターネット利用者

【被害の予防（被害に備えた対策含む）】

- SMSやメールで受信したURLや、SNSの投稿内のURLを安易にクリックしない
  - どうしても内容が気になる場合は、よく使うサービスはあらかじめ公式アプリをインストールしておくことや、Webサイトをブックマーク（お気に入り登録）しておくことで確認時に利用する
- 利用しているサービスの多要素認証の設定を有効にする
- 迷惑メールフィルターを利用する

♦ 対策

• インターネット利用者

【被害の早期検知】

- 利用しているサービスで、いつもと異なるログインがあった場合に通知する設定を有効にする
  - 通知があった際は自身のログインによるものかを確認する
- 利用しているサービスのログイン履歴の確認する
- クレジットカードやインターネットバンキングの利用明細を確認する

♦ 対策

• インターネット利用者

【被害を受けた後の対応】

- 大量のフィッシングメールを受信している場合はメールアドレスの変更を検討する（メールアドレスの漏えいを懸念した対応）
- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
- サービス運営者（コールセンター等）へ相談する
- 信頼できる機関に相談する

【参考】 迷惑メール相談センター（日本データ通信協会）
https://www.dekyo.or.jp/soudan/index.html
フィッシング対策（警察庁）
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
フィッシング対策協議会
https://www.antiphishing.jp/registration.html