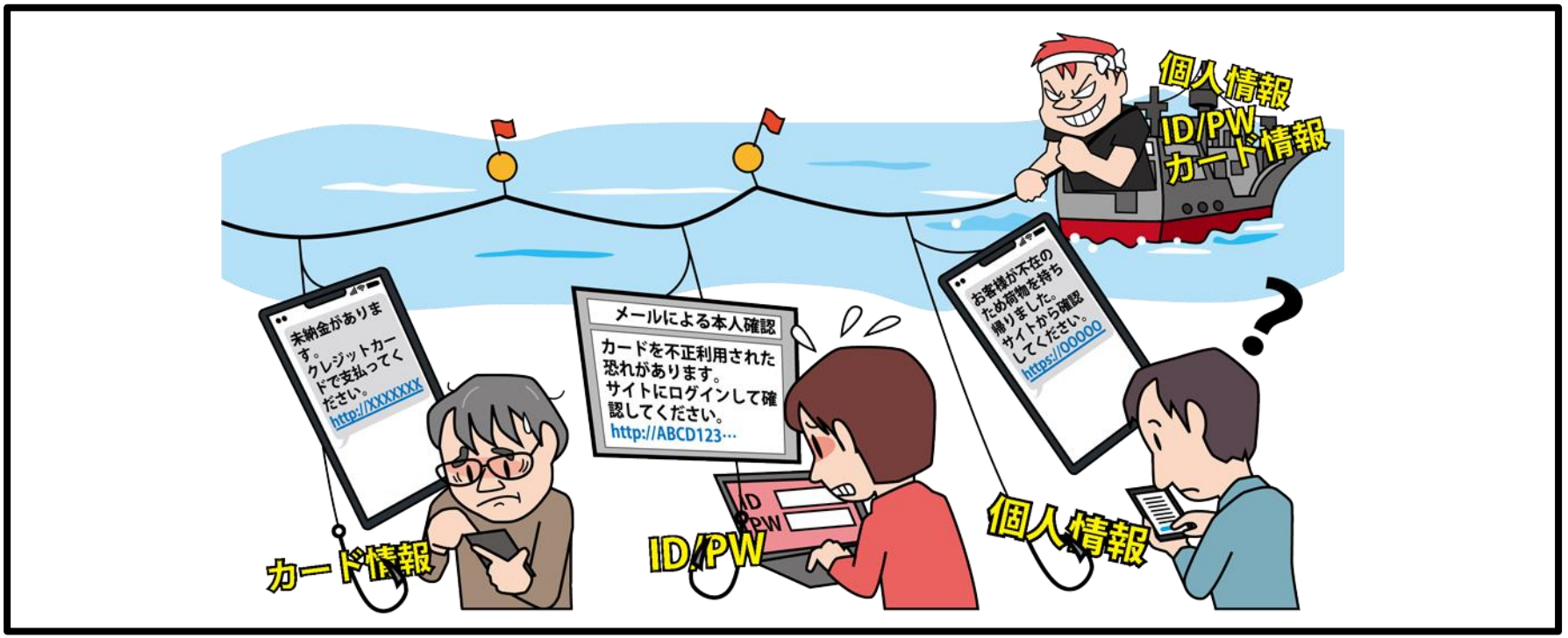
【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～



- 金融機関や有名企業を装った**偽のウェブサイト**（フィッシングサイト）へ利用者を誘導
- 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

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

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ウェブサイトを**模倣**したフィッシングサイトを用意
- 公的機関や有名企業を**装ったメールやSNS、 SMS**（スミッシング）を不特定多数に送信し、フィッシングサイトに誘導
- フィッシングサイトで**利用者が入力した情報を詐取**

■ 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**偽の広告を表示**させ、フィッシングサイトへ誘導

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

IPA

- 2022年の事例/傾向①
  - 過去の本物の内容を模したフィッシング（※1）
    - 2022年3月、JR東日本が同社のチケット予約サービス「えきねっと」を騙った不審メールを確認したとして注意喚起
    - 不審メールは、過去に同サービスが発信していた「【重要】アカウントの自動退会処理について」という**文章を模していた**
    - 「2年以上サービスにログインしていないと自動退会になる」として、**メール内のリンクからログインを促す**内容
    - リンクからアクセスすると、偽のウェブサイトが表示され、個人情報の入力を求められる。**入力するとその情報が盗まれる。**

【出典】

※1 「これ詐欺だったの？」――「えきねっと」をかたるメール、手口の巧妙さが話題に “自動退会処理”に注意（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2203/07/news095.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 2022年の事例/傾向②

■「国税庁」を騙ったフィッシング（※1,2）

- 2022年8月、国税庁が、同庁を騙った不審メールやSMSが確認されているとして**注意喚起**
- 不審メールはe-Tax利用者に**実際に送られたメールに似通っていたり**、税金が未払いであると**不安を煽ったり**する内容
- メールやSMSからアクセスした不審サイトでは、未払い税金の納付のため、個人情報やクレジットカード情報の入力を求められる。**入力してしまうとその情報が盗まれる**。

【出典】

※1　不審なショートメッセージやメールにご注意ください（国税庁）
https://www.e-tax.nta.go.jp/topics/topics_20220815.htm

※2　国税庁をかたるフィッシング（2022/09/20）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/nta_20220920.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 2022年の事例/傾向③

■ 報告件数は依然として増加傾向 (※1,2)

- フィッシング対策協議会の報告書によると、2022年のフィッシング報告件数は97万件(前年は53万件)と**2倍弱に増加**
- フィッシングサイトへの誘導に**QRコードを用いる手口**も確認
- フィッシングメールやSMSの内容はクレジットカードの利用確認や、宅配業者の不在通知、Amazon等のショッピングサイト、通信事業者を**装ったものを引き続き確認**

【出典】
※1 2021/12 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202112.html
※2 2022/12 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202212.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 対策

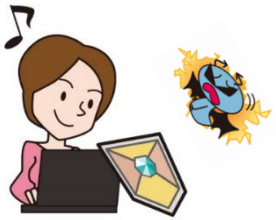
■ インターネット利用者

・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**

－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



・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確認

－利用しているサービスの**ログイン履歴の確認**

－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**

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

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（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）
- サービス運営者（コールセンター等）へ**連絡**する
- 信頼できる機関に**相談**する