スマホを狙う詐欺の話

２０１９・７・４　活き生きクラブ定期講座

スマホの普及とともに、
スマホを狙った詐欺が増えてきています。

どんなケースの詐欺があるのかを知り、
危険を回避する術を身につけましょう。

フィッシング詐欺

クレジットカードの情報
銀行口座の情報
各種アカウント情報（IDとパスワード）

これらの情報を入手して不正利用する詐欺

様々な形で事業者を装い
「獲物を釣り上げる＝フィッシング」

フィッシング詐欺の例（Apple）

「Apple IDがセキュリティ上の理由でロックされました」

→メールで案内が届く
→偽Appleサイトに誘導
→パスワード変更手続きが必要と称して、
　カード情報、ID/PASSを入力させる

フィッシング詐欺の例（ヤマト運輸）

「宅急便の荷物をお届けにあがりましたが
不在のため持ち帰りました」

→メールで案内が届く
→偽クロネコヤマトのサイトに誘導
→荷物の問い合わせと称して詐欺用の不正
アプリをインストールさせる

※日本郵便、佐川急便を装う例もある

フィッシング詐欺の例（アマゾン）

「Amazonに登録しているアカウントの確認です」

→メールで案内が届く
→偽アマゾンサイトに誘導
→アカウントの確認と称して登録しているクレジットカードなどの個人情報を入力させる

フィッシング詐欺の例（銀行/カード）

「あなたの口座/カードがセキュリティ上の理由でロックされました」

→メールで案内が届く
→偽サイトに誘導
→アカウント情報の変更手続きと称して利用中の口座/カード番号、暗証番号などを入力させる

フィッシング詐欺の例（その他）

「○○○に当選しました！と偽サイトに誘導」

→プレゼントのための手続きと称してカード情報や個人情報を盗む
→Webページを見ていると突然案内が現れるケースが多い

「特別セールなどと称した広告から偽の通販サイトに誘導」

→ブランド品、有名な高額商品が70％OFFなど
→本物のブランドや通販サイトに似せた作り
→注文してもお金だけ取られて商品が届かない
　または、ニセモノ商品が届く

フィッシング詐欺の対策

偽サイトを見破るのは難しい

→メールでの案内を信用しない
　特にアカウント情報の変更を求めるもの、日本語表現が
　微妙おかしい場合には注意

→変更手続きの案内があった場合は、その事業者の正規
　窓口から手続きを行う。※メールの案内に従わない

→少しでも怪しいと感じたら事業者に問い合わせる
　または、グーグル検索で調べる

ワンクリック詐欺

URLリンクをクリックすると、何かに
申し込んだ事にされ料金を請求される詐欺

振り込まないと裁判、家族や職場に連絡、
などと脅してくるのが特徴

Webページ上に罠があるケースが大半
メールでURLリンクを送付してくるケースも

ワンクリック詐欺の代表例

成人向け動画サイトの年齢認証ボタンを
クリックしたら有料会員に登録

出会い系サイト、婚活サイトなどでも
ワンクリック詐欺にかかる場合がある

男性の被害者が大半、要注意！

ワンクリック詐欺の対策

いかがわしいサイトに行かない

勇気を持って無視する

→絶対に相手にコンタクト（連絡）しない
　コンタクトすると相手に更に脅される羽目に

→ワンクリックで課金する事は出来ないと知る

→Web上で絶対にカード情報、個人情報を入力しない

偽の警告を使う詐欺

「スマホ画面に突然警告メッセージが表示される」

→ウイルスに感染しました
→システムエラーが発生しました
→クリーンアップが必要です

これは警告に見せかけた広告
→不正アプリのインストールを誘導

その他の詐欺

アンケートを利用した詐欺
→回答者に豪華なプレゼントを用意
→個人情報を盗む

高額アルバイトをうたう詐欺
→広告クリックや口コミ投稿などをさせる
→報酬が全く支払われない

スマホ詐欺の被害に遭わない
ためには、

身に覚えの無い案内は基本的に無視

届いた案内から手続きを開始しない

焦らず、怖がらず人に相談する

次回：7/11 ショート講習

「　リクエスト募集中　　」

私達は川崎市市民活動助成金で活動しています。

NPO団体への寄付のご協力をお願い致します。