

サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和3年
6月30日
Vol.62

県内で多発しているサイバー犯罪に要注意！

スミッシング、偽サイト・詐欺サイト、セクストーションの手口や被害にあわないための対策方法について紹介していますので、是非参考にしてください。また、少しでも不安に感じた際は警察に相談してください。

スミッシング

偽のSMSを不特定多数に送信し、URLをタップさせて個人情報を盗む。運転免許証やマイナンバーカード等の身分証の写真を詐取る新たな手口も発生。

【SMSの例 送信元が知らない電話番号】

11:30 [知らない電話番号] SMS/MMS 昨日 18:34
ご本人様不在の為お荷物を持ち帰りました。ご確認ください。
<http://...duckdns.org>

【SMSの例 送信元が知人の電話番号】

17:45 [知人の電話番号] SMS/MMS 今日 9:15
気を付けてよ、写真がネットに載っているじゃん、気まずいな
<http://...duckdns.org>

宅業者をかたる
duckdns.org ドメイン
フィッシングサイト
個人情報盗まれる
さらには...
身分証等の流出
ウイルスに感染

対策

- SMSのURLをタップしない。
URLをタップする前に公式サイトなどで真偽を確認しましょう。
- 身分証の画像を送らない。
運転免許証、マイナンバーカードなどを安易に撮影、送信しないでください。
- 重要な情報は簡単に入力しない。
パスワード、認証コードなど、重要な情報は安易に入力しないでください。
- 手口を知る。
インターネット詐欺など、犯罪の手口の基本を知ることが被害防止につながります。

参考元：IPA安心相談窓口(<https://www.ipa.go.jp/security/anshin/mgdayori20210623.html>)

偽サイト・詐欺サイト

代金を支払っても商品を送せず、個人情報や決済時のクレジットカード情報等を盗み取る悪質なショッピングサイトが乱立。

【悪質なショッピングサイトの例】

売切れて手に入らないものが「在庫あり」。
一般価格よりも大幅に安い。
会社概要に、架空の情報を記載。実在する会社の情報を勝手に記載していることもある。
不自然な日本語表現

超レア 激安Sale!!
【在庫あり】
Bag 販売価格 50,000円 → 9,000円
注文
【会社概要】
会社名：愛媛商店
住所：愛媛県松山市●●町△△
TEL：089-xxx-xxxx
【配送】
休日が悪い天気会った時、届けた日より2,3日遅れるの可能性になっています。
【支払い方法について】
銀行振込、クレジットカード決済

ログイン
ID
パスワード
新規会員登録
氏名
住所
電話番号
メール
配送先
名前
住所
電話番号
支払い方法
銀行振込

個人情報盗まれる。
支払い方法の説明と実際の決済画面とで対応している支払い方法が異なる。

対策

- インターネット上で検索
会員登録や商品注文する前に、サイト名やURL、サイトを運営する会社の名称、住所、電話番号などをインターネット上で検索すると、住所の番地や、電話番号が実在しないものであったり、実在する会社の住所や電話番号などが勝手に使われていることに気付くことができ、同様の被害にあった事例などの記事を見つけることもできます。
- ブックマーク、公式アプリを利用
お金の支払いや、IDやパスワードなど大切な情報を扱うウェブサイトを利用するときは、ブックマークや、ウェブサイトの運営会社が配布している公式アプリを利用してアクセスしましょう。

参考元：JC3日本サイバー犯罪対策センター(https://www.jc3.or.jp/topics/malicious_site.html)

セクストーション

性的脅迫メール。録画した動画と引き換えにビットコインを要求してくる。英語や不自然な日本語で書かれていたが、最近は自然な日本語で書かれている。

送信元アドレスを偽装

【メールの例 ※一部抜粋】

「アダルトサイトを見ているあなたの恥ずかしい姿を撮影し、あなたの連絡先の情報も入手しました。この映像を家族や同僚にばらまかれたいくなくれば、20万円分のビットコインを僕に送金してください。」

性的な映像を撮ったと主張
ビットコインを要求

対策

- 無視する。
このような脅迫メールは不特定多数に送信されている架空請求メールなので慌てず無視しましょう。
- ウィルス対策ソフト等を導入する。
市販のウィルス対策ソフトや、メールのフィルタリング機能の導入により被害の未然防止対策になります。

※ メール本文に現在自分が利用しているパスワードが記載されていた場合は、なんらかの原因でパスワードが漏洩している可能性があるため、**すぐにパスワードの変更を実施**しましょう。パスワードを変更する時は、メールのリンクを開くのではなく、ブックマークやアプリなど、いつもそのサービスを利用している環境から変更しましょう。

参考元：JC3日本サイバー犯罪対策センター(<https://www.jc3.or.jp/topics/sextortion.html>)