



サイバーセキュリティ情報高島

発行：高島警察署・高島市防犯自治会

QRコードを悪用した詐欺が増加！

QRコードを悪用した詐欺とは？

QRコードを用いて不正なサイトへの誘導や金銭的な取引を行い、個人情報や金銭をだまし取る詐欺で、クイッシングとも呼ばれています。QRコードの送金機能を利用して虚偽の請求を案内する手口やコード決済アプリを利用して返金する旨伝え、実際は利用者が送金するように誘導する手口などがあります。



QRコードを悪用した返金詐欺の手口とは？



利用者

① 偽サイトでショッピング

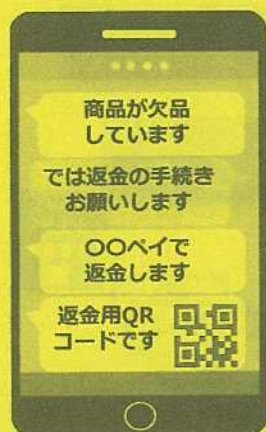
※口座振込や電子マネーで支払い



偽サイト

② サイトから欠品のため返金の連絡

※「商品が欠品しています」、
「返金は〇〇ペイになる」などと言われLINEに誘導される。



③ 偽の返金用QRコードを送信

④ 偽の返金用QRコードを読み込み指示されたとおりに操作・送金

※「返金するためには××××というコードを入力しなければならない」と言われ、指示されたまま入力すると××××円が犯人側のアカウントにチャージされる。



被害防止のポイント!!

商品代金を銀行振込や電子マネーで支払っているにもかかわらず、支払いに用いていないコード決済アプリで返金を行うのは不自然です。
「〇〇ペイで返金します」と言われたら 詐欺 を疑いましょう！



←公式X

「サイバーコネクトSHIG@」定期的にソフトウェアの脆弱性情報をチェックしましょう。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231 (代表)

県警Webページ→



※ QRコードは株式会社デンソーウェーブの登録商標です



サイバーセキュリティ情報高島

発行：高島警察署・高島市防犯自治会

フィッシングによる不正送金被害が多発！

こんなメールやSMSに要注意！

利用停止に関するメール

偽

From: ××組合
件名: 【重要】利用停止のお知らせ

××組合のネットバンクをご利用いただき、ありがとうございます。
お客様のログイン異常により、振込(出金)、ATMのご利用(出金)が一時利用停止されました。

セキュリティを強化するため下記のリンクをクリックして手続きを進めてください。

▼解除手続

本人確認を求めるメール

偽

From: ××バンク
件名: 利用停止のお知らせ

いつも××ネットバンクをご利用いただき、ありがとうございます。
××ネットバンクの利用停止を行いましたので、お知らせします。
下記のリンクにアクセスし、本人確認の手続きをお願いします。

<https://example.co.jp>

クリックすると、フィッシングサイトへ

フィッシングサイトにパスワード等を入力すると？

入力した個人情報や金融情報等が、犯人側に渡ってしまい、ネットバンキングの口座を操作され、犯人側が準備した別の口座に送金されてしまいます。



被害防止のポイント!!

- 利用停止、取引継続のための本人確認など、不安を煽るような件名・内容のメールやSMSは、特に注意！
- メールやSMS中のURL、リンクは、安易にクリックしない！
- 情報の確認は、公式サイトや公式アプリを利用する。
- パスキーや多要素認証を利用する。(パスワードを利用しない。)



←公式X

「サイバーコネクトSHIG@」定期的にソフトウェアの脆弱性情報をチェックしましょう。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231 (代表)

県警Webページ→



<https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html>