

事例

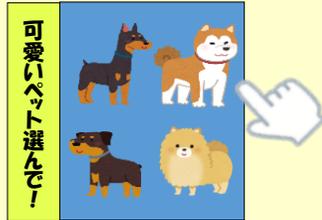
SNSで「可愛いと思うペットに投票してください。」というダイレクトメッセージが届いたので、投票したらLINEアカウントを乗っ取られてしまった。

LINEやInstagramなどのSNSで、友達登録しているアカウントから「可愛いと思うペットに投票してほしい。」「料理コンテストの投票に協力してほしい。」等の内容のダイレクトメッセージを受信し、投票の手続きを進めていくと最終的にSNSのアカウントが乗っ取られ、登録している友達にメッセージを送信されるという相談が増加しています。

- ① LINEやInstagramなどのSNSで、友達登録しているアカウントからURL入り(リンク)のダイレクトメッセージが届く



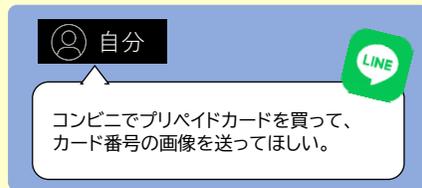
- ② リンクをクリックすると投票画面に移動



- ③ 「投票のために必要」と偽り、偽のログイン画面に切り替わり、ログイン情報を入力することでアカウントを乗っ取られる



- ④ 登録している友達に『電子マネーを購入してほしい』などとメッセージを送信



被害に遭わないために

- ◆ 知人から届いたダイレクトメッセージであっても、すでにその知人のアカウントが乗っ取られている可能性もあるので、メッセージに添付されたリンクは安易にクリックしないようにしましょう
- ◆ 複数端末で利用しない場合は、他端末の「ログイン許可」をオフにしましょう

SNSでサイバー犯罪の最新手口を随時投稿中です。ぜひフォローしてチェックしましょう！

詳しくはこちら



公式 (LINE) 公式 (Instagram)

知る！学ぶ！防ぐ！サイバー犯罪

福岡県田川警察署

相談事例から「知る！学ぶ！防ぐ！」

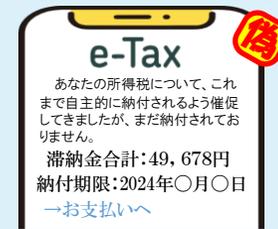
事例

国税庁から「未納の国税を納付しなければ財産の差押えを行う」という内容のメールが届いた。納付方法はキャッシュレス決済になっているが、そのまま支払っても大丈夫？

「クイッシング」という言葉を聞いたことがありますか？これは二次元コードのQR（クイックレスポンス）コードとフィッシング詐欺を掛け合わせた造語です。クイッシングは、利用者をだまして二次元コードをスキャンさせることで偽のサイトに誘導し、ログイン情報やクレジットカード情報などの個人情報を盗み出す手口です。最近では、二次元コードを悪用した犯罪が増加傾向にありますので、特に注意が必要です。

【ケース1】

○国税庁を装った偽のメールを受信



○滞納金の支払いをキャッシュレス決済で要求される



【ケース2】

海外では、店舗に貼られた二次元コードからアンケートに答えたところ、**銀行口座からお金を盗み取られるケースも報告されています。**



【ケース3】

偽のサイトに誘導する二次元コード付きの広告がポストに投函されるケースも...



被害に遭わないために

- ◆ 二次元コードのサイトアドレスを確認し、安全か矛盾点がないか確認しましょう
二次元コードをスキャンすると、二次元コードのウェブサイトのアドレスが表示されるので、クリックする前に、必ず矛盾点がないか確認しましょう
- ◆ 二次元コードを送付してきた企業の公式サイトなどを確認しましょう