サイバーセキュリティパートナーシップだより

R8-5

注意！ LINE アカウント乗っ取り 事案が多発！！金銭的被害も確認

県内でもLINEアカウントの乗っ取り事案や乗っ取りに起因するPayPay詐欺事案を複数認知しています。

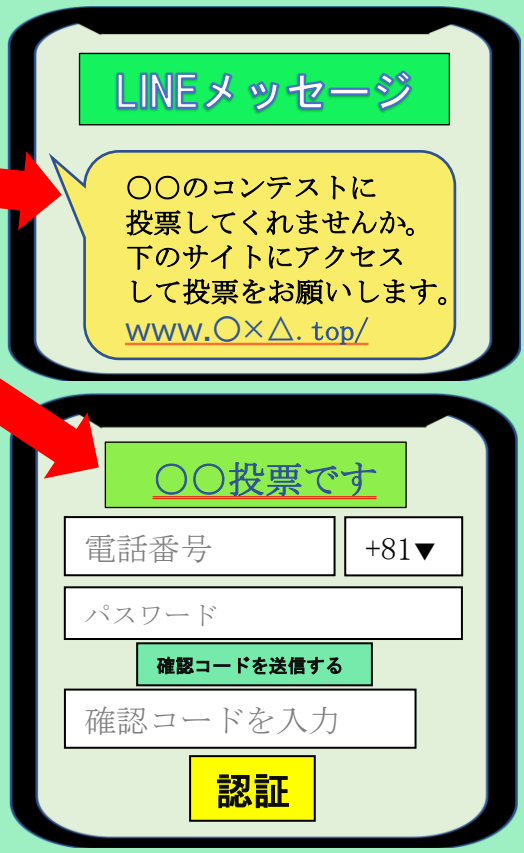
被害の流れ

①既に乗っ取り被害に遭っている、LINEでつながっている友だちから、右のようなメッセージが来ます。

②投票ページに繋がるリンクが送られて来て、ページにアクセスすると、偽の認証ページに移動します。

③「認証」ボタンを押してしまうと、LINEアカウントが乗っ取られ、
「アカウントからログアウトされました。」
という画面が表示されることもあるようです。

④さらに、あなたをログアウトさせるために、相手からLINEアプリを一旦削除するかアンインストールしてから、再インストールするように指示を受ける場合もあるようです。



乗っ取り(フィッシング)手口には、この他にも、**宅配業者を装い**「再配達」「宛先不明」や、**LINEからの公式の案内を騙り**「再認証が必要」「安全確認」などといった文言で、リンクにアクセスさせようとするものがあります。

アカウントが乗っ取られると

あなたの友だちに対して、さらに乗っ取りの拡大を試みるだけでなく、中にはこんな金銭的被害も・・

いま、ひまー？ PayPayやってるー？

PayPayの送金限度額が切れちゃって、
３万円、代わりに払ってもらえない？
明日、朝には返すよー。

これまでやりとりのある
LINEの友だちだと勘違いし
PayPayを送金してしまう

【対策は次のページで】

乗っ取られないために

① 知人からであっても、投票依頼には安易に回答しない
② 登録情報（電話番号やパスワード、メールアドレス）を入力したり送ったりしない
③ LINEの「ログイン許可」設定をOFFにしておく
（他の端末でLINEにログインすることを拒否する設定です）
④ **「認証番号」は、絶対に誰にも教えない！！**

偽SMS/偽メールの見分け方

１つでも当てはまると危険!!

☑ URLに不自然な点がある
・ LINEの公式サイトのURLは
https://www.line.me/ja/
です。
・ 届いたメールやメッセージに記載のURLからアクセスせずに、必ずLINE公式サイトから公式情報を確認してください。

☑ LINEアカウントの登録情報（電話番号やパスワード、メールアドレス）や認証番号の入力を求められる
・ LINEから送信された認証番号は、決して他人には伝えないでください。
☑ 過度に緊急性を強調している
・ 「今すぐ」「至急」「48時間以内」「LINEアカウント停止」「利用制限」など、強い言葉で不安をあおる場合は注意しましょう。

乗っ取られた（かもしれない）時は

LINEアカウントを利用できている場合

① パスワードを変更する
② 「ログイン許可」を「オフ」に変更する
⚙設定→アカウント→ログイン許可
③ ログイン中の端末を確認して、身に覚えのない端末をログアウトさせる
「ログイン許可」がオンの状態で、「ログイン中の端末」を確認する

利用できなくなった場合

① 「アカウントからログアウトされました」という画面が突然表示された場合は「再ログイン」を選択することで、取り戻せる場合があります。
② LINEのヘルプセンターにある注意事項を確認し、「お問い合わせフォーム」から、アカウントを乗っ取られた状況を報告してください。
③ 状況を正確に報告するためスクリーンショットを準備しておきましょう。

※ LINE HP(ヘルプセンター)URL　https://help.line.me/line/smartphone?lang=ja

サイバー犯罪相談事例
対処法と対策・相談窓口

山口県警サイバー課LINE友だち募集中！
サイバー犯罪に関する防犯情報を配信中です

山口県警察本部 サイバー犯罪対策課