

LINEアカウントの乗っ取りが相次いでいます！

引継ぎ以外で電話番号やパスワード・認証コードは入力しないで！

乗っ取りの手口について

1 SNSのダイレクトメッセージなどで**投票依頼**が送られてくる

例) 「子供が絵画コンクールに応募したので投票してください」など

2 ダイレクトメッセージに添付されたリンクを開くと**電話番号**や**パスワード**、**認証コード**の入力画面(**フィッシングサイト**)に誘導される

3 誘導されたフィッシングサイトに自身の電話番号やパスワード、認証コードを入力すると、アカウントが乗取られる

詐欺画面の一例

jp.voteg5z1.pics

LINEとうひょう

LINE

LINE認証投票へようこそ

電話番号、パスワード、認証コードを入力し、「次へ」(→)をクリックすると、LINE利用規約およびプライバシーポリシー。

*でんわばんごう
入力してください

*パスワード
入力してください

*LINE認証コード
入力してください

LINEのトークルームを開いてご確認ください。

*SMS認証コード
入力してください

参照:LINEヘルプセンター (<https://help.line.me>)

LINEアカウントが乗取られると

- 他のアカウントの乗っ取りに利用される！
- LINEでつながっている知人に対して金銭を要求される！



LINEアカウントが乗取られた場合の対応

- LINEヘルプセンターで乗取られた場合の対応を確認する！
- 乗取られたことを、電話などで周囲の人に連絡する！



被害を防ぐためにできること

- 知人からのメッセージであっても、投票依頼には安易に回答しない！
- 自分で引き継ぎを行う場合以外に、電話番号やパスワード、認証コードを入力したり送ったりしない！
- LINEの設定を確認して「ログイン許可」を「オフ」にしておく！



さらに詳しく知りたい方はLINE公式ページを確認！
(<https://guide.line.me/ja/cyber-bousai/>)



北海道警察公式HP
サバセキリイひろば

北海道警察



YouTube動画
サバセキリイひろば

