

LINEアカウントの乗っ取りが多発！

電話番号やパスワード・認証コードの取扱いは要注意！！

乗っ取りの代表的な手口

- ① SNSのダイレクトメッセージ等で
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から投票お願いします」等
- ② ダイレクトメッセージ等に添付されたリンクにアクセスすると
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、アカウントが乗っ取られる

※他にもLINEをかたり「アカウント停止する」等と不安をあおり、登録情報を盗む手口等もあります

詐欺画面の一例



LINEライセンス投票です

電話番号、パスワード、認証コードを入力して「認証」をクリックすると、LINEの利用規約とプライバシーポリシーに同意したものとみなされます。

電話番号

+81

パスワード

認証コードを入力

認証コードを送信する

認証

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

LINEアカウントが乗っ取られると

- 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金銭を要求される

LINEアカウントが乗っ取られた場合の対応

- LINEヘルプセンターで乗っ取られた場合の対応を確認する
- 乗っ取られたことを電話等で周囲の人に連絡する

被害防止の対応

- 知人からであっても、投票依頼には安易に回答しない
- 登録情報や認証コードを安易に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



設定 ⇒ アカウント ⇒ ログイン許可 ⇒ オフ

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-性1561ろば

北海道警察



YouTube動画
サバ-性1561ろば

