あなたのLINEが狙われています！

事　例

知人のSNSのアカウント(すでに乗っ取られているもの)から、絵画コンテストなどの投票を依頼するメッセージとURLが届き、URLにアクセスして、LINEアプリのパスワードなどを入力したところ、アカウントが乗っ取られた。

代表的な手口

①SNSでコンテスト等への投票を依頼するメッセージが送られてくる。

URLに企業と関係のない不自然な文字列が含まれている

②メッセージに添付されたリンクにアクセスし投票しようとするとLINEの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情報を入力すると、アカウントが乗っ取られてしまう。

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

アカウントが乗っ取られると…

私に3万円を●ペイを使って送金して！

LINEで繋がっている知人に金銭を要求するメッセージを送信される。

被害に遭わないために

- **知人のアカウントからであっても、安易に信じ込んで投票しないようにしましょう。**
  ※すでに乗っ取られたアカウントを犯人に使われているおそれがあります。
- **登録情報や認証番号を安易に入力したり、送信したりしないようにしましょう。**
- **LINEの「ログイン許可」設定を活用しましょう。**
  （他の端末でLINEにログインすることを拒否する設定です）