サイバーセキュリティパートナーシップだより

No.5

令和4年3月4日　山口県警察本部生活環境課

ＬＩＮＥアカウントの乗っ取り被害に注意！

Facebook やＬＩＮＥ上で知人になりすまして嘘のメッセージを送り付け、要求に応じた者のＬＩＮＥアカウントを乗っ取る手口を県内で認知しています。乗っ取りの手口と対策を紹介しますので、被害に遭わないよう十分注意してください。

【メッセージの例①】

私の line アカウントはロックされました、解除するには、何人かの友人の確認が必要となりますので、下の line のサイトにログインして解除していただけますか　www.line●●●.xyz

知人のアカウントからのメッセージだが、送信元のアカウントも乗っ取られている

【アクセス先の表示画面】

ＬＩＮＥ

友達にアカウントロックを解除するのを協力したら、下の（はじめる）をクリックしてください。

はじめる

ＬＩＮＥ

携帯電話番号【　　】

パスワード　【　　】

確認

※ＬＩＮＥ公式を装ったフィッシングサイト

入力してしまうと乗っ取られる!!

【メッセージの例②】

携帯電話番号教えて。そして、ラインの確認メッセージを認証してもらえる？

四桁の認証番号が届いたら、教えてね。

※相手に携帯電話番号を教えると、自分の携帯電話にＳＭＳ（ショートメッセージ）で４桁の認証番号（ＰＩＮコード）が届く。

認証番号を教えてしまうと乗っ取られる!!

アカウントが乗っ取られると、登録している友だち宛に「近くのコンビニでプリペイドカードを買ってきて。買ったら裏面のＩＤを教えて。」といった金銭を要求するメッセージ等を送信されてしまいます。

【乗っ取り被害に遭わないための対策】

- **他人に「電話番号」や「パスワード」、「ＳＭＳ認証番号」を教えない！**
- **複数端末で利用しない場合は、他端末の「ログイン許可」の設定をオフ！**
- **パスワード設定は、推測されにくい複雑なものにし、使い回しは避ける！**

不自然な日本語で認証番号を聞かれたり、金銭を要求された場合は、相手のアカウントが乗っ取り被害に遭っている可能性がありますので、相手の要求には応じないようにしましょう。

山口県警察本部サイバー犯罪相談窓口
TEL　０８３－９２２－８９８３
mail cyber.soudan@police.pref.yamaguchi.lg.jp

詳しい設定方法等は、LINE の使い方ガイド「乗っ取り被害に遭わないために～アカウント泥棒から身を守る方法～」を参照
https://guide.line.me/ja/cyber-bousai2020/