サイバーセキュリティ通信【 R7-18】

令 和 7 年 1 1 月 大分県警察本部生活安全部 サイバー犯罪対策課

インスタグラム、フェイスブックなどのSNSアカウントを 乗っ取られる被害が多数発生中!!

投票依頼に関するメッセージに注意!

~手口の紹介~

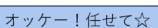
- ① 犯人に乗っ取られた友人等のアカウントから、「アンバサダーに 立候補したので投票して」などと、フェイスブックやインスタグラム でダイレクトメッセージが届きます。
- ② 友人に協力しようとして、投票に了承すると、電話番号を聞かれ、 相手から「SMS(ショートメッセージ)にアカウントの認証番号や リンク先URLをDMに貼って返信して」等と指示されます。
- <u>③ 相手の指示通りにすると、アカウントが乗っ取られます!</u> **。**

友人になりすました犯人

ダイレクトメッセージの例



アンバサダーに立候補したよー! 上位目指してるから、投票に協力 してくれない?「WhatsApp」という アプリをダウンロードして!





被害者



投票のリンクを送るから 電話番号を教えて!

あれ?教えてなかった? 090-**-**だよ!





ショートメッセージが届くよ! メッセージの数字6桁(又はメッ セージのURL)を教えて。

届いたよ! 12345678 (又はhttp:///~)だよ。





アカウントの乗っ取り成功!

※新たに乗っ取ったアカウントの フォロワーへまた被害が拡大していく...

犯人は認証番号やリンク先を入手すれば、フェイスブックやインスタグラムなどのSNSアカウントにIDや パスワードを入力することなく、パスワードを再設定し被害者のアカウントにログインできるのです!

対

- ①SNSで電話番号や認証番号を教えない
- ②アカウントに多要素の認証(生体認証、SMS等)を設定する
- ③SNSのヘルプセンター等に不正アクセス被害を報告する
- ④不正アクセスされたことを自分自身のフォロワーに注意喚起する



