

－自分のFacebookアカウントが乗っ取られてしまう被害に注意！－

フェイスブックのメッセージで友達から送られてくる動画ファイルをタップしてしまい、アカウントが乗っ取られてしまう！

ソーシャルネットワーキングサービスの一つに「Facebook（フェイスブック）」があります。

このソーシャルネットワーキングサービスで、友達から送られてきた動画ファイルを再生しようとして、自分のアカウントが乗っ取られてしまう被害が全国的に発生しており、新潟県内でも相談が複数寄せられています。

Facebook（フェイスブック）の友達から動画メッセージを受信しても安易に動画ファイルをタップしたり、誘導されたサイト内で個人情報等を入力したりしないように注意しましょう。



1. 手口

この手口は、動画を再生しようとしてメッセージをタップすると、Facebook（フェイスブック）の偽サイトに誘導されます。

誘導された偽サイト内で自分のFacebook（フェイスブック）のID・パスワードを入力すると、ID・パスワードが騙し取られます。（フィッシング）また、そこから更に誘導されるアンケートサイト等で、自分の個人情報やクレジットカード情報等を騙し取られてしまうケースも確認されています。



図1 【Facebook（フェイスブック）アカウント乗っ取り手口の流れ】

2. 対処方法

動画を装った不審なメッセージが送られてきた場合、不審なメッセージをタップしないことが一番の対策ですが、万が一メッセージをタップしてしまい、アカウント情報などの入力をしてしまった際は以下の対処をしましょう。

■偽サイトにFacebookアカウントのID・パスワードを入力・送信してしまった場合

- ➔ 至急、Facebookアカウントのパスワードを変更してください。
パスワードの変更後に二段階認証設定を行ってください。
- ➔ Facebookアカウントにログインが出来なくなっている場合はFacebookヘルプページから不正使用されたアカウントの報告を行い、アカウント削除等の対応を取ってもらってください。

【参考】：Facebook：ヘルプページ

- ◆【Facebookにログインできない場合】
<https://www.facebook.com/help/105487009541643>
- ◆【不正使用されたアカウントの報告】
<https://www.facebook.com/hacked>

■偽のセキュリティ警告画面から誘導され、アプリをインストールしてしまった場合

- ➔ アプリが必要でない場合は、アプリのアンインストールをしてください。
自動継続課金を知らないうちに登録している場合があるので、解約手続きを行なって下さい。

■不審なアンケートサイト等へ情報を入力してしまった場合

- ➔ アンケートサイトへの誘導を受けて、当該サイトでクレジットカード情報等を入力してしまった際には、速やかにクレジットカード会社へ連絡を行い、クレジットカードの停止措置等を依頼してください。
- ➔ 何らかの契約や申し込み等を行った場合、解約等には、事業者への申し出が必要となります。
事業者のウェブサイト上の【問い合わせフォーム】・【メール】で直接退会の申し出を行なってください。
自分で対処が難しい場合は、最寄りの消費生活センターへ相談し、アドバイスを受けるようにしましょう。
(消費生活センターへの相談は、原則、事前の電話予約が必要です。)

3. 自分のFacebookの友達へのメッセージ送信確認・注意喚起も重要！！

この手口に引っかかってしまい、Facebookアカウントを乗っ取られた場合、事後に自分のFacebookアカウントから友達に対して、同様に動画メッセージが送信され、更に友達がFacebookアカウントを乗っ取られてしまうといった二次的被害も発生しています。

自分のアカウントから友達に不審なメッセージが送信されていないか確認すると共に、不審なメッセージが送信されていた場合には、友達に対して受信した動画ファイルをタップしないように注意を促すことが被害拡大を防止する対策の一つです。