コラム

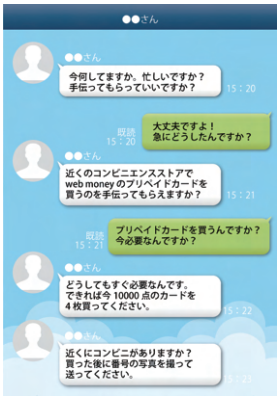
SNSアカウントが乗っ取られる被害が増えています！

スマートフォンの普及でSNSの利用者が増えてくると、SNSでも悪質サイトへ誘導する迷惑メッセージや詐欺被害なども発生するようになりました。知らないうちにアカウント（ID・パスワード）を乗っ取られて不正利用されるという被害もあとを絶ちません。

●アカウント管理がとても重要です

アカウントを乗っ取られるとクラウド上に保存してあるプライベートな情報が盗まれたり、詐欺サイトへ誘導しようと、つながっている友人知人にあなたのアカウントで不正なメッセージが送信されたりします。

特に、SNSアカウントとアプリの連携には注意が必要です。アプリ側がこの機能を利用できるようになると本来アカウント利用者しか行えない操作をアプリ側が外部から行えるようになってしまいます。不正なアプリだった場合、不正ログインされてアカウント情報を盗みとられてしまうわけです。



●アカウント乗っ取りでこんな被害も

IDとパスワードを不正な手段で入手した乗っ取り犯が、勝手にログインしたうえで、そのアカウントの友人・知人へ「緊急で必要だからプリペイドカードを購入して番号を知らせて」とメッセージを送り、金券番号をだましとるという事件もありました。

全く知らない他人なら、怪しんだり警戒したりしますが、友人・知人の名前で送られてきたメッセージだったために疑うことはなく協力してしまい、多数の被害が発生してしまいました。少し不審な内容でも信じて協力してしまったようです。

●パソコンなどからはログインできないようにもできます

LINEはパソコンやタブレットからも利用することが可能です。もし、乗っ取り犯がパソコンやタブレットから不正にログインしたとしても、スマートフォンでは、いつもどおりLINEアプリが利用できるため、通知が届いても乗っ取られたことに気づかない可能性があります。

スマートフォンでの利用しかしない場合は、パソコンなどからログインできないよう設定しておくと安全です。

「設定」→「アカウント」→「ログイン許可」をタップし、チェックを外す

乗っ取られないための対策

アカウントを乗っ取られないために、以下の点に注意し、対策をしておきましょう。

1．複数サービスでIDやパスワードの使い回しをしない
乗っ取り犯は、入手したIDやパスワードで他のサービスにも不正ログインを試みます。同じID・パスワードにしておくと複数のSNSが乗っ取られる可能性があり危険です。

2．SNSサービス間のアカウント連携を避ける
最近のSNSの多くは連携機能を利用して同時投稿などができますが、上記と同じように、１つのアカウントが乗っ取られた場合、連携機能を利用して他サービスにもアクセスされることになってしまいます。

3．２段階認証を利用する
２段階認証は、ログイン時にSMSで届く認証コードの入力を必要とする機能です。多くのSNSサービスでは、アカウント乗っ取り対策として、いつもと異なるスマートフォンやパソコンなどの環境からログインした場合、登録しておいた携帯番号へSMSで認証コードが送られ、そのコードを入力しないとログインできない設定とすることができます。もし、IDやパスワードが流出してしまっても、これにより不正ログインを防ぐことができます。

乗っ取られてしまったときは

乗っ取り犯により不正ログインされたことに気づいたときは、すぐにパスワードを変更しましょう。もし、既にパスワードが変更されてログインできないときは、運営会社に連絡して対処してください。

参考Webサイト

LINE
ヘルプセンター

Facebook
ヘルプセンター

X(旧Twitter)
ヘルプセンター

Apple
サポート