サイバーセキュリティだより

発行 ： 愛媛県警察本部生活安全部生活環境課サイバー犯罪対策室

平成29年
8月18日
Vol.11

ＳＮＳやクラウドサービスの乗っ取りに注意！！

○　現在、LINE・Twitter・FacebookなどのＳＮＳサービスやiCloudなどのクラウドサービスのアカウント乗っ取り被害が増加しています。
○　乗っ取り犯人は、様々な手法を用いてアカウント情報やパスワードを引き出し、アカウントを乗っ取ります。
○　アカウントが乗っ取られると、サービスにログインできなくなり、
・利用者になりすましての電子マネー詐取やクレジットカード不正利用。
・保存していた情報（写真・連絡先・重要情報）の流出。
など、様々な被害の二次発生が予想されます。

代表的な乗っ取りの手口

○　**フィッシング**
ＳＮＳやクラウドサービスの運営を騙り、公式サイトに似せたフィッシングサイトに誘導して、アカウント情報等を入力させて乗っ取る。

○　**知人のなりすまし**
ＳＮＳのメッセージ機能を利用し、家族や友人になりすまし、「電話番号と認証番号を教えてほしい。」などとメッセージを送信して必要な情報を送信させて乗っ取る。

○　**不正プログラム（コンピュータウイルス等）**
「宝くじに当選しました」、「お得な情報のお知らせ」など興味を引く内容の偽メールや取引先を装ったメールなどを送信し、添付している不正プログラム（コンピュータウイルス等）をインストールさせ、情報を盗む。

○　**パスワードを予測される**
公開している情報等から容易に予測できるパスワードを設定している場合、犯人にパスワードを予測され、乗っ取られる。

【対策】

○　セキュリティ対策ソフトを導入し、常に最新の状態にするとともに、ＯＳを常に最新の状態にしておく。
○　推測されにくいパスワードを使用し、パスワードの使い回しをしない。
○　身に覚えのない不審なメールは開かず、ファイルが添付されている場合は、安易に展開しない。
○　リンク先にアクセスを促している場合は、アドレスをよく確認する。
○　二段階認証機能のあるサービスについては、必ず導入する。
○　電話番号や認証番号は絶対に教えない。
○　機密情報をクラウドサービスに保管したままにしない。

愛媛県警のホームページとTwitter・facebookの愛媛県警公式アカウントにLINE乗っ取りの手口について動画で紹介していますので、参考にして下さい。

相談窓口　愛媛県警察本部生活安全部生活環境課
サイバー犯罪対策室　TEL　089-934-0110