教職員向け指導資料（8月）

≪LINEの乗っ取り詐欺≫

北海道教育委員会
ネットトラブル未然防止のための総合ヘルプサイト

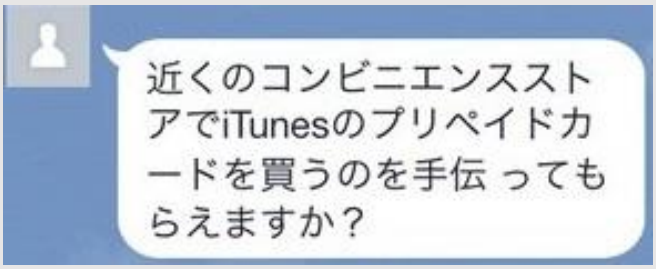
LINE乗っ取り詐欺

6月頃からLINEのアカウントを不正に乗っ取り、本人になりすましてプリペイドカードを騙し取ろうとする「LINE乗っ取り詐欺」が起こっています。手口は不正に知り得たメールアドレスとパスワードを使ってLINEにログインし、乗っ取ったアカウントを使い、その友だちにプリペイドカードを買うのを手伝ってほしいと持ちかけ、プリペイド番号を聞き出そうとするものです。

※プリペイドカードとは、あらかじめ前払いで支払った金額分の商品を購入できるカードで、発行された番号を入力することで、インターネット上でも利用することができます。

≪乗っ取り詐欺の流れ≫

乗っ取られたアカウントからは右のようなトークが送られてきます。さらに返信を行うと具体的な指示が送られてきます。例は「iTunes」のプリペイドカードを要求していますが、「web money」などコンビニエンスストアで買えるその他のプリペイドカードの場合もあります。



対策と注意すべき点

これまでLINEにログインする際には、メールアドレスとパスワードのみで本人認証を行っていましたが、7月17日から新たに「PINコード」という4桁の暗証番号を設定し、ログインの際にはメールアドレス、パスワード、PINコードの3つで本人認証を行うようセキュリティの強化が行われました。

≪設定時の注意点≫

PINコードは自分で設定しておかなければいけません。LINEの「設定」から「アカウント」→「PINコード」を選択し、任意の4桁の数字を設定することになります

LINEに限らず、パスワードを設定するときには、他のサービスですでに設定しているパスワードや、「1111」「1234」といった推測されやすい文字列を避けることがセキュリティ上、安全です。

乗っ取り詐欺を防ぐためには、まずこのような詐欺があることを児童生徒へ広めましょう。そして、LINEはその他の無料通話アプリと同様にフィルタリングの対象となりますので、トラブルを未然に防ぐために、利用している児童生徒の年齢、インターネットへの理解度に合わせてフィルタリングの設定を行うよう、保護者への啓発を行いましょう。

ピットクルー株式会社