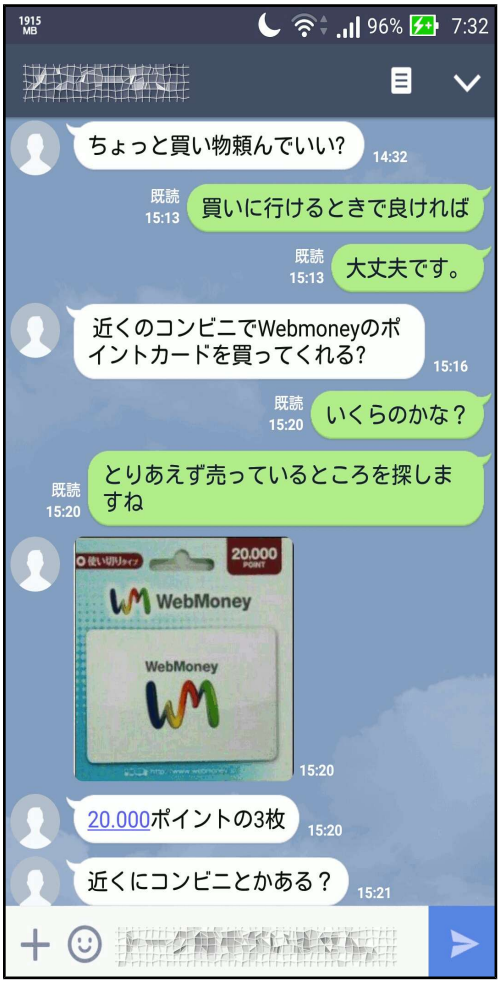
LINE 乗っ取り（＝不正ログイン）に気を付けよう！

皆さん、こんにちは。今回はセキュリティについてお話しします。テーマは、"LINE（ライン）乗っ取り"です。LINE とは、スマートフォン（iPhone、Android）で使うアプリで、楽しくチャットによるコミュニケーションができます。

去年 2014 年の夏頃に、「LINE 乗っ取り詐欺」が流行ったことは、新聞やテレビなどで報道されたので知っている方も多いと思います。最近、私たちの周りで、この LINE 乗っ取り詐欺が発生したため、被害が増えないようにするためにも注意喚起をさせていただきます。



LINE 乗っ取り詐欺とは、大体次のような流れです。
(1)知らない人に自分の LINE が勝手に使われる状態に
なってしまう（＝乗っ取られる）
(2)乗っ取った人（＝犯人）は、元の持ち主に成り
すまして、LINE に登録されている「友達」に、
コンビニで売っている電子マネー（Webmoney
など）を購入するように依頼してくる
(3)騙された「友達」が電子マネーを購入した後、
スマートフォンのカメラで撮影して
乗っ取った人の LINE に送るよう依頼してくる。
送った後は、乗っ取った人は逃げる（＝詐欺成立）
（参考：右写真）

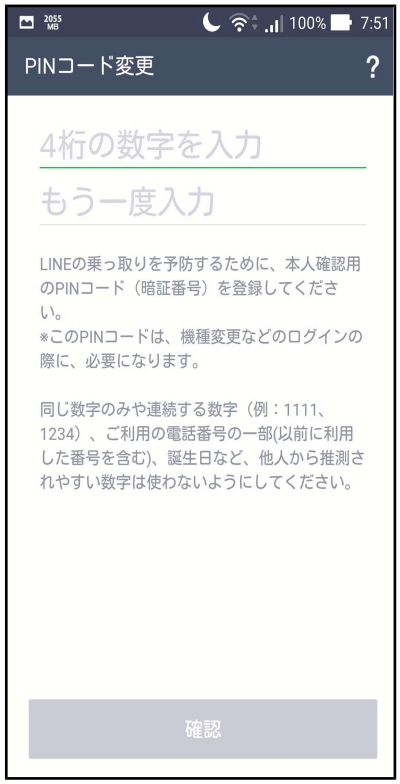
この LINE 乗っ取り詐欺の怖いところは、LINE でのやりとりで相手の顔が見えないために、相手が本当に本人かどうかわからない点です。

なので、いつもと違う話し方になっていないか、いきなりお金を要求することはありえないのではないか、という風に普段から気を付けることが大切です。

もし、LINE 乗っ取り詐欺かもしれないと思われることが起きたら、LINE 以外の方法で本人に必ず確認するようにしてください。たとえば、パソコンメールやファックス、あるいは直接本人の家に行って状況説明するのも有効です。

次に、乗っ取り詐欺に遭わないように対策する方法をご紹介します。

① PIN コードを登録する



PIN コードとは、パスワードの一種で、４桁の数字で作ります。
このPIN コードを入れておけば、万が一自分の LINE が乗っ取られそうになったときに、PIN コードを知らないと LINE に入られないため、乗っ取りを防ぐことができます。

（1）LINE アプリの[その他]→[設定]→[アカウント]
→[PIN コード]をタップする
（2）４桁の数字を２回入力し、「OK」をタップする

※なお、「3333」や「1234」などの簡単な数字や自分の誕生日、銀行の口座番号で使っている数字などは、危険なのでやめましょう。

②パスワードの変更方法

LINE でメールアドレスを登録している場合は、パスワードを設定していると思います。このパスワードを簡単な文字にしていたり、facebook やメールアドレスのパスワードと同じにしていると、乗っ取られる可能性が高くなってしまいます。
LINE しか使わないパスワードにし、パスワードの内容も他の人が簡単に予想できないように、文字や数字の組み合わせで８文字以上の長さにしておきましょう！

(1) LINE アプリの[その他]→[設定]→[アカウント]
→[メールアドレス登録]をタップする
(2) [パスワードの変更]をタップする
(3)「現在のパスワード」を入力し、「新しいパスワード」に新しく変更したいパスワードを２回入力し「確認」をタップする

以上の①と②の対策をしっかりすることで、乗っ取りを未然に防ぐことができます。ぜひ実施しておきましょう！