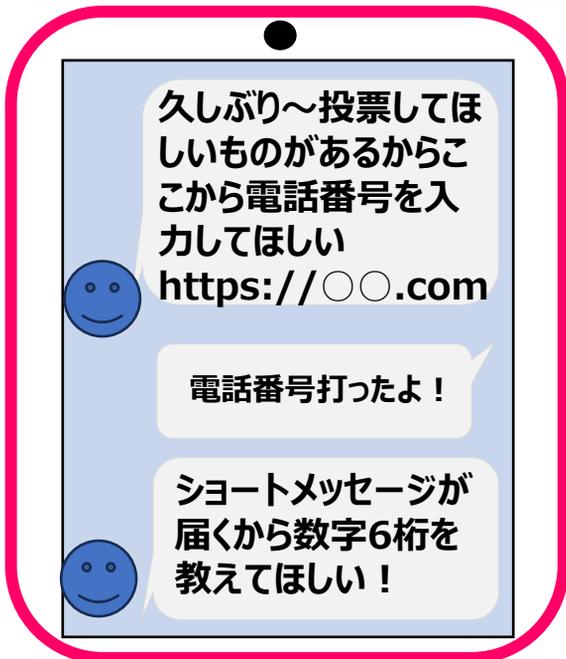


SNSの相手は本人ですか？

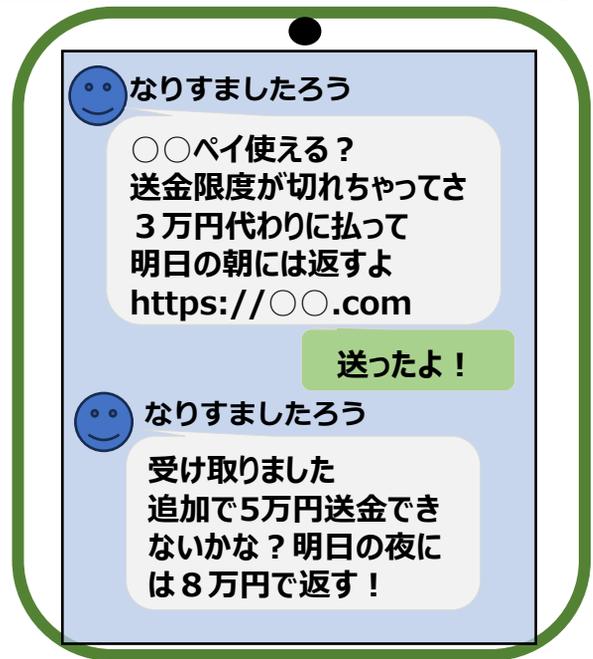
SNSアカウントを乗っ取り、本人になりすまして二次元コード決済で送金を要求するといった相談が急増！だまされると詐欺の被害に！



久しぶり～投票してほしいものがあるからここから電話番号を入力してほしい
<https://〇〇.com>

電話番号打ったよ！

ショートメッセージが届くから数字6桁を教えてください！



なりすましたろう

〇〇ペイ使える？
送金限度が切れちゃってさ3万円代わりに払って明日の朝には返すよ
<https://〇〇.com>

送ったよ！

なりすましたろう

受け取りました追加で5万円送金できないかな？明日の夜には8万円で返す！

～以下の点に注意してSNSを利用しよう～

【送金詐欺被害防止】DMのリンクを開かない

昨日まで、さっきまで連絡をしていた相手が乗っ取り被害に遭っている可能性があります。電話番号の入力や送金を求めるDM、不審なリンクに要注意！

【乗っ取り被害防止】SMS・メールの多要素認証コードを伝えない

SMS認証コードは、自分以外が使用するものではありません。もし、認証コードを聞かれたら**アカウントの乗っ取り**を疑ってください！

【乗っ取り被害防止】安易に個人情報等を教えない・入力しない

偽サイトでアカウント情報を入力させ、アカウントが乗っ取られるという相談を多数確認しています。安易なアカウント情報や個人情報の入力はいらないこと！

