

あなたの口座は大丈夫ですか? インターネットバンキングが 狙われています!

パソコンや携帯電話、スマートフォンから、いつでも利用できるインターネットバンキング。便利である反面、利用者を狙った犯罪も急増しています。被害の実態や犯罪の手口を知って、しっかりと安全対策を行いましょ。



問い合わせ
県警察本部サイバー犯罪対策課
TEL 043(201)0110(代表)
HP <http://www.police.pref.chiba.jp>

インターネットバンキングとは

自分のパソコンや携帯電話、スマートフォンで、銀行の残高照会や振り込みなどのさまざまな銀行取引を利用できるサービス

被害事例



【事例1】

ある日、被害者の携帯電話宛てにショートメッセージサービス(SMS)でメッセージが送られてきた。内容を確認したところ、「インターネットバンキングで利用するパスワードの有効期限が明日まで」というお知らせであった。普段利用している銀行からのお知らせだと思い込んだ被害者は、インターネットを利用してパスワードを変更した。その後、何者かによって、他人の口座に5万4千円振り込まれてしまった。

フィッシングメール(イメージ)

差出人：○×△銀行(○○○@●●●.△)
件名：【○×△銀行】メールアドレスの確認

利用者の個人情報漏えい事件が occurred。お客様のアカウントの安全性を保つため、「○×△銀行システム」がアップグレードされましたが、お客様のアカウントが凍結されないように直ちにご登録の上、ご確認ください。

以下のページより登録を続けてください。

<http://○×△.jp/login>

表記上は正規サイトのURLですが、クリックするとフィッシングサイトが表示されます。

※フィッシングメールの本文内容は、いろいろなパターンがあります。



銀行が、電子メールやショートメッセージサービスなどで、パスワードなどの入力を求めることはありません。フィッシングメールといって、メッセージなどに記載されているリンクを開くと偽画面が表示されるので、絶対に開かないでください。



【事例2】

ある日、被害者は自宅のパソコンでインターネットバンキングの預金残高を確認するため、いつも使っているサイトからIDとパスワードを入力してログインした。しかし、ログイン後、第2パスワード、第3パスワードを入力する画面が表示され、被害者は画面の指示どおり、パスワードを入力した。その後、何者かによって他人の口座に約300万円振り込まれてしまった。



いつもと違う画面表示、暗証番号の入力を要求された場合は、パソコンがウイルスに感染し、偽画面が表示された可能性があるので安易に入力をしないでください。



インタビュー



千葉県警察本部サイバー犯罪対策課の冢入興樹課長に、ニュースなどで耳にするインターネットバンキングの被害についてお聞きしました。

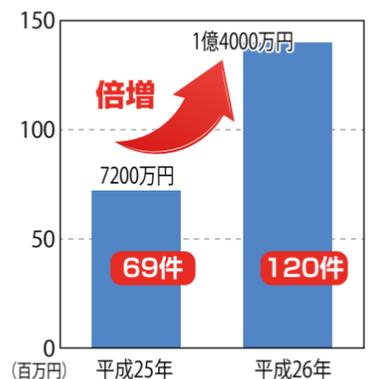
Q最近、インターネットバンキングの不正送金が急増していると感じましたが、どのような犯罪ですか。

Aインターネットバンキングで利用するID・パスワードなどを盗み出して、利用者が気付かないうちに口座からお金を引き出してしまうものです。

Q被害はどのくらい増えているのですか。

A全国の被害については、平成25年は1,315件、約14億600万円だったのが、平成26年は1,876件、約29億1千万円と拡大し、過去最悪の被害となっています。

千葉県の被害状況



過去最悪!

県内の被害についても、平成25年は69件、約7,200万円に対し、平成26年は120件、約1億4千万円に増えています。

Q被害の特徴や犯罪の手口を教えてください。

A不正送金事犯は、都市銀行や地方銀行だけでなく信用金庫・信用組合にも及んでおり、個人口座に対する被害に加え、昨年末あたりから、法人口座の被害も急増しています。

手口は、金融機関などを装って利用者にメールを送り、偽のサイトへ誘導してID・パスワードなどを盗み出したり、インターネットバンキングへログインすると同時に、コンピューター・ウイルスによって、本人が気付かないうちに口座からお金を引き出されてしまったりする被害が確認されています。

悪質・巧妙化!

Q口座を守るための対策を教えてください。

Aインターネットバンキング利用者にとっていただきたい対策は、次の4つです。

- ①ウイルス対策ソフトの導入
- ②パソコンのOSや各ソフトウェアを常に更新
- ③ワンタイムパスワードといって、ログインごとに変わる、一度使い切りのパスワードを利用
- ④不審に感じたり、見慣れない入力画面などを発見した場合は、金融機関などに通報



サイバー犯罪対策課の冢入課長

しっかり対策を!

警察では、都道府県警察間で被害情報を共有し、合同捜査を進めています。また、金融機関や通信事業者などと連携して被害の状況や対策などを情報共有するとともに、利用者に対する知識の啓発にも努めています。