

サイバー犯罪対策通信 第1号

令和2年1月31日

愛知県警察本部
サイバー犯罪対策課

インターネットバンキングを利用していなくても不正送金被害!

1

ピローン♪

SMS/MMS
今日 10:05

お客様の【〇〇銀行口座】
セキュリティ強化、カード・
通帳一時利用停止、再開
のお手続きの設定
<https://〇〇〇〇.jp/>

あれ?
〇〇銀行からだ。
最近、家賃の引き落とし
を〇〇銀行に変えたから
不備かな?

早く手続き
しないと…
URLをタップ♪

マホ巡査

2

\〇〇銀行のサイトだ /

えっと
最後の手続きは…

あとは、
〇〇銀行から電話
がかかってくる
のを待つよね!

ブルブル♪

私の口座の店番と、
口座番号を入力して
ログイン

次は、私の名前・
電話番号・暗証番号
など入力して実行

3

こちらは、〇〇銀行です。
お客様の番号は
123456 です。

この番号を入力
すればいいのね!
これで手続き完了!

4

えっ!? ない!!
私のお金がなくな
ってる----!!!

残高 0円

問題

マホ巡査はインターネットバンキングの利用はしていませんでした。
しかし、マホ巡査は不正送金の被害に遭ってしまったのです。
なぜでしょうか??

解説

- 1 マホ巡査が最初に受け取ったメールは、〇〇銀行を騙ったフィッシングメール(偽メール)です。URLをタップすると、フィッシングサイト(偽サイト)に誘導されます。
- 2 このフィッシングサイトに口座情報や暗証番号などを入力してしまうと、リアルタイムでその情報が犯人に盗まれてしまいます。
- 3 本物の〇〇銀行からマホ巡査の電話番号に音声案内で番号が通知されます。
- 4 犯人は、盗んだ情報を使ってマホ巡査の口座のインターネットバンキングを開通して、預金を他人の口座に送金して盗み出したのです。

※ 送金の際には、銀行から口座開設時の電話番号に本人確認の電話がかかることがあります。マホ巡査が電話で通知された番号をフィッシングサイトに入力してしまうと、これも犯人に盗まれてしまいます。結果、犯人が送金できるようになってしまい、被害に遭ってしまうのです。

この事例はあくまでも一例で、銀行を騙る偽メールがたくさん出回っているのでご注意ください。

皆様の大切な財産を守るために、
この情報を家族や友人など一人でも多くの人に伝えましょう!!

