

お客様 各位

釧路信用組合

インターネットバンキングの不正送金被害にご注意ください

本年9月頃から、メールやショートメッセージ、SMS等を用いたフィッシングや、スパイウェア等の不正プログラムを用いた手口により、インターネットバンキングのID・パスワード等を搾取し、預金を不正に送金する事案が急増しております。

【主な手口】

① SMS等を用いたフィッシング手口

- ・金融機関を騙ったSMS等のフィッシングメールを通じて、インターネットバンキング利用者を金融機関のフィッシングサイト（偽のログインサイト）へ誘導し、インターネットバンキングのIDやパスワード、ワンタイムパスワード等の情報を搾取して預金の不正送金を行うもの。

② スパイウェア等を用いた手口

- ・何らかの方法でインターネットバンキング利用者のパソコンにスパイウェアを感染させ、利用者の知らない間にID・パスワード等を搾取し、当該ID等を利用して預金の不正送金を行うもの。

こうした被害に遭わないために、

- ・心当たりのないSMS等は開かない。
- ・金融機関のウェブサイトアクセスする場合、事前に正しいURLをブックマーク（お気に入り）登録しておき、ブックマークからアクセスする。
- ・表示されたウェブサイトのURLを確認する。
- ・パソコンのOSやセキュリティ対策ソフトを最新版にする。

など、十分ご注意くださいようお願い申し上げます。

また、当組合からインターネットバンキングのパスワード等を求める事はございませんので、このような状況に遭遇した場合は、下記のヘルプデスクまでご連絡願います。

なお、当組合のインターネットバンキングサービスをご利用のお客様からの被害報告等はございませんが、引き続き情報収集に努めて参ります。

以 上

【本件に係る問い合わせ先】

釧路信用組合
インターネットバンキングヘルプデスク
釧路市北大通9-2
TEL 0120-037-493