重要なお知らせ

インターネットバンキングを利用した不正出金にご注意ください

インターネットバンキングのＩＤ・パスワード等を盗み取るウイルスを使用する手口等により、インターネットバンキングにアクセスし、不正な送金が行われるという被害が多発しています。

不正送金の被害に遭わない為に、当組合では下記の対策をお願いしています。

不正送金の被害に遭わないためのセキュリティ対策

- インターネットバンキングのログインは当組合のホームページから行い、身に覚えのない不審なメールに添付されたファイル・ＵＲＬは開かないようお願いいたします。

当組合ではＥメールでID・パスワードの入力をお願いすることは絶対にありませんので、入力しないでください。

- パソコンの基本ソフト（ＯＳ）、ウェブブラウザなど、インストールされているソフトウエアを常に最新の状態に更新してください。
- セキュリティ対策ソフトを導入するとともに、常に最新の状態に更新し、定期的にウイルススキャンを実施してください。
- 不審なサイトにアクセスなさらないようご注意ください。
- 信頼のおけないプログラムをダウンロードなさらないようご注意ください。
- インターネットカフェや図書館、ホテルなど、不特定多数の人が利用するパソコンでのご利用はお避け下さい。
- 振込などの限度額を必要な範囲内で出来る限り低く設定して頂きますようお願いいたします。※振込限度額の引き下げはログイン後の操作画面上にて可能です。
- 不審なログイン履歴および取引履歴がないか、お通帳やインターネットバンキングサービスご利用の都度ご確認ください。
- パスワードは毎月ご変更ください。
- パスワードは、名前、自宅の住所・番地、電話番号、勤務先の電話番号、生年月日、自動車ナンバー、同一数字、連続数字等の他人から類推されやすいものはお避けください。

- ID・パスワードは厳重に管理し、パソコン内のファイル書いて保存することはお止めください。
- 取引通知メールの宛先を携帯電話等に設定し、いつでも取引結果を確認できるように設定願います。
- パソコンを利用しない時は電源をオフにして下さい。
- インターネットバンキングにログインした際に不審な入力画面等が表示された場合、ＩＤ・パスワード等の情報を入力せず、当組合事務部（0438-20-1122）にご連絡ください。

特に、法人向けインターネットバンキングのご利用者様におかれましては、次のような対策もご実施ください。

- 取引の申請者と承認者で異なるパソコンを利用する。

セキュリティ対策ソフト「PhishWall（フィッシュウォール）プレミアム」の導入

当組合では、ホームページやインターネットバンキングをより安全にご利用いただくため、フィッシング詐欺や MITB（マン・イン・ザ・ブラウザ）攻撃対策機能を持つセキュリティ対策ソフト「PhishWall（フィッシュウォール）プレミアム」をご提供しています。PhishWall プレミアムは、株式会社セキュアブレインが提供するフィッシング・MITB 攻撃対策ソフトです。

PhishWall プレミアムを導入すると、当組合のインターネットバンキングご利用時に緑のシグナルが表示され、本物の画面であることを簡単に確認できるようになります。
また、インターネットバンキング利用中に不正な偽画面を表示させることによってパスワードなどの認証情報を盗み取る攻撃を検知した際は、警告画面を表示し、お客さまにお知らせします。無料でご利用いただけますので、安全対策として、ぜひ PhishWall プレミアムをご利用ください。

インストールや詳細につきましては下記の URL をご参照ください。
http://kimishin.jp/netbank/phishwall/

その他ご不明点は下記へお問い合わせください。

お問い合わせ先
君津信用組合　事務部
０４３８－２０－１１２２（平日９：００～１７：００）