インターネットバンキングで不正被害に遭わないために

インターネットの利用に際しては、不正プログラムに感染する危険性が常にあります。
端末が不正プログラムに感染すると、不正送金だけでなく、遠隔操作・情報漏えい等様々な被害に遭うおそれがあります。
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、以下の対策をお願いします。

＜ウイルスがお客様の端末へ侵入することを防ぐための対策＞

	実施する内容	実施することによる効果
1	サポート期限が終了している基本ソフト等((例)WindowsXP)のご利用はお控えください。	サポートが終了した基本ソフト等のご利用を続けると、ウイルスに感染しやすい環境になります。
2	基本ソフトOS((例 Windows)ブラウザ((例)Internet Explorer)等は、常に最新の状態に更新してください。	更新情報にはセキュリティ対策に必要な修正プログラム等が含まれています。
3	ウイルス対策ソフトを導入し、常に最新の状態に更新してください。	最新の状態に更新することで、日々新しく誕生するコンピューターウイルスの検知（駆除）の精度が高まります。
4	当金庫が無料で提供するセキュリティ対策ソフトRapport(ラポート)をインストールしてください。	不正送金用のウイルスの検知、駆除を行うセキュリティソフトです。市販のウイルス対策ソフトと併用することで、不正送金を防止できる可能性が高まります。
5	不審なメールの開封および不審なサイトの閲覧は控えてください。	開封・閲覧するだけで感染するウイルスが存在している可能性があります。

＜インターネットバンキングを安全にご利用いただくための対策＞

	実施する内容	実施することによる効果
1	セコム･プレミアムネットをご利用ください。	ウイルスに感染しない常に安全な環境で、インターネットバンキングが利用できます。
2	電子証明書方式をご利用ください。（法人IB）	電子証明書が未登録のパソコンからは操作できないため、不正ログイン防止につながります。
3	ワンタイムパスワードをご利用ください。	振込等の取引の都度、３０秒毎に変わる使い捨てのワンタイムパスワードを利用することで､セキュリティが高まります。
4	インターネットバンキングをご利用になる際には、ご利用前にセキュリティソフトでウイルスチェックを行い、ウイルス感染がないことをご確認の上でのご利用をお願いします。	ウイルス感染の早期発見に役立ちます。
5	パスワードを定期的に変更してください。（推奨：1ヶ月に一度変更） パスワード入力時は「ソフトウェアキーボード」を推奨します。	定期的に変更することで、万が一パスワードが漏洩した場合でも不正にログインができなくなります。
6	不審な「前回ログイン履歴」がないかログイン時に確認してください。 （画面上に「前回ログイン履歴」を表示しております。）	不正履歴が確認された場合、不正ログインの早期発見につながります。
7	振り込みなどの限度額を必要な範囲で出来る限り低く設定してください。	万が一不正送金された場合、被害を最小限に抑えられます。
8	取引時の通知メールを直ちにご確認いただけるメールアドレスを登録してください。	不正送金被害の早期発見に役立ちます。
9	ID･パスワード等は、利用者以外に教えないでください。	パスワード漏洩リスクを低減できます。
10	通常とは異なる画面が表示された場合、直ちに操作を中止し、当金庫までご連絡ください。	不正送金被害の防止に繋がります。

※上記対策を講じていても完璧なセキュリティ対策が保証されたわけではありませんが安全性は向上します。

万が一被害に遭ってしまったら

身に覚えのない振込メール等が届いたら、すぐにログイン履歴等を確認しましょう！！
被害に遭ってしまったら、まずは三島信用金庫と警察に連絡しましょう！！

※金融犯罪の手口は日々変化しています。ここで紹介している内容や考え方、手順などは一例です。

三　島　信　用　金　庫