偽画面を表示させてしんきん個人・法人インターネットバンキングサービスのID・パスワードを盗み取ろうとする事例について

東京信用金庫

一部の信用金庫におきまして、しんきん個人・法人インターネットバンキングサービスの偽画面を表示させて、お取引に必要なＩＤ・パスワードを盗み取る事例が確認されております。

当金庫のしんきん個人・法人インターネットバンキングサービスでは、ログイン直後にパスワードを入力していただくことはありません。

このような、不正アクセスを未然に防ぎ、サービスをより安全にご利用いただくため、以下の点にご注意いただきますようお願いいたします。

・ウイルス対策ソフトを導入する。

常に最新版にアップデートして利用し、定期的にウイルスチェックを行ってください。

インターネットバンキングを狙ったウイルスの検知・駆除には、セキュリティソフト「Rapport」が効果的です。

・OS やブラウザ、ソフトウェア（アプリケーション）は常に最新の状態に更新する。

これらの脆弱性情報は日々更新されていますので、最新の状態を保つことが脆弱性対策になります。

・ウイルス感染の原因となる行動をしない。

不審なウェブサイトや、送信元が不明な E メールは開かないでください。また、インターネットカフェなど不特定多数が利用するパソコンでは、USB メモリ等の使用を避けてください。

・各種暗証番号等の管理方法を見直す。

スマートフォンやパソコン、クラウドサービスへの保存はお控えください。ウイルス感染時の情報流出リスクが高まります。

・ワンタイムパスワードを利用する。

ワンタイムパスワードは一定時間で自動的に変更されることから、第三者に搾取されたとしても、不正送金のリスクを低減させることができます。実際に不正送金被害にあったお客様は、ワンタイムパスワードを利用していないケースが多く見受けられます。

以　上