2020 年 11 月吉日

浜松いわた信用金庫

お客さま各位

ビジネス WEB－FB の偽画面表示によるパスワード搾取について

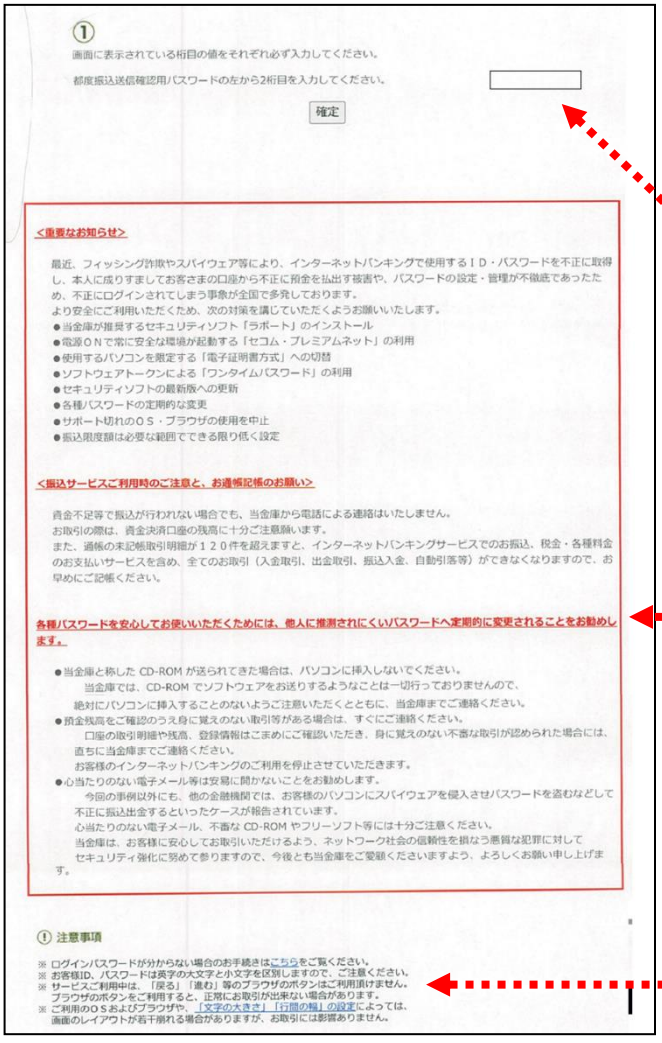
一部の信用金庫におきまして、ビジネス WEB－FB の偽画面を表示させ、お取引に必要な ID・パスワードを盗み取る事例が確認されております。（※11 月現在、当金庫において同様の事案は発生しておりません。）

ビジネス WEB－FB では、ログイン直後に、振込用のパスワードを入力していただくことはありません。

（※初回開通操作、パスワード再設定操作を行う場合のみ、ログイン直後にパスワード変更画面が表示されます。）

普段とは異なる、見慣れない画面でパスワード入力を求められた場合は、絶対にパスワードの入力は行わず、当金庫までご連絡ください。

実際に確認された偽画面のイメージ画像



① ログイン画面で ID とパスワードを入力すると、左図のような偽画面が表示されます。
偽画面の URL は本物と同じ URL が表示されています。

② 左図では、都度振込送信確認用パスワードの2桁目の入力を要求しています。
入力を行うと、次は別の桁数の入力を要求してきます。
この繰り返しにより、犯人はパスワード情報を不正に入手します。

③ 画面中央の＜重要なお知らせ＞以下は、犯人側が作成した文章です。
表示されているリンク先へは絶対にアクセスしないでください。

被害を防ぐために

偽画面の表示は、お客様のパソコンがウィルスに感染したことが原因である可能性があります。
インターネットバンキングをご利用のお客様は、ウィルス感染からの情報流出を防ぐために、以下の点にご注意をお願いします。

・ウィ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、定期的にウィ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ィルスの検知・駆除には、セキュリティソフト「Rapport」が効果的です。「Rapport」は無料でご利用いただけます。詳細は下記 URL よりご確認ください。

Rapport のご案内：http://www.shinkin.co.jp/info/kyotsu/oshirase/20141010/

・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利用者は、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。詳細は下記 URL よりご確認ください。

ワンタイムパスワードのご案内：https://hamamatsu-iwata.jp/netbank/business/post_5.html

・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。

・ウィ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。

・パスワードの管理方法を見直す

パソコンやスマートフォン、クラウドサービスへのパスワード保存はお控えください。ウィルス感染時に情報流出のリスクが高まります。

以　上

【本件に関するお問い合わせ】

浜松いわた信用金庫ＩＴサポートセンター
０１２０－１８６－１３１
音声ガイダンス【２】をプッシュしてください
受付時間　平日９：００～１７：００