にししんインターネットバンキングの

不正送金対策全体図

不正送金対策は、１種類の対策だけでなく複数行う必要があります!!

【フィッシング詐欺】

偽装ホームページにアクセスさせる内容のＥメールを不特定多数に送付し、ＩＤ・パスワードを入力させ詐取する。詐取したＩＤ・パスワードを利用し、なりすましてＩＢを利用する。

対策!!

・EV SSL 証明書
・Phish Wall プレミアム
➡ ｾｷｭﾘﾃｨ対策 ③
右図のように表示されていることを確認する。

【ウイルスの侵入】

対策!!

・ウィルス対策ソフト（ウィルスバスター、ノートン等）を更新し、常に最新の状態に保つ。
➡ ｾｷｭﾘﾃｨ対策 ④

・心当たりのない送信元からのメール（添付ファイル）は開かない。

・ＯＳのアップデートを必ず行う。

・インターネット対戦ゲームやアダルトサイトは利用しない。

ＩＤ・ﾊﾟｽﾜｰﾄﾞ取得!!

偽装ﾎｰﾑﾍﾟｰｼﾞ
ＩＤ・ﾊﾟｽﾜｰﾄﾞ入力

ｱｸｾｽ

《お客さま》

正常な振込データ➡

第三者が遠隔で振込操作

ウイルスが振込ﾃﾞｰﾀ改ざん

第三者が不正に詐取したＩＤ・ﾊﾟｽﾜｰﾄﾞを利用して振込操作

西尾信用金庫
ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ

不正送金!!

【不正口座】

ｳｲﾙｽ侵入!!

ｳｲﾙｽ侵入!!

【ＩＤ・パスワード詐取による不正送金】

対策!!

・電子証明書方式（法人ＩＢのみ）
➡ ｾｷｭﾘﾃｨ対策 ②
・ワンタイムパスワードサービス
➡ ｾｷｭﾘﾃｨ対策 ①

【遠隔操作】

ウイルスをお客さまのパソコンに侵入させ、遠隔で操作し不正送金を行う。

対策!!

・ワンタイムパスワードサービス（法人ＩＢ、個人ＩＢﾊｰﾄﾞｳｪｱﾄｰｸﾝ）
➡ ｾｷｭﾘﾃｨ対策 ①

【ＭＩＴＢ攻撃】

振込データを改ざんするウイルスをお客さまのパソコンに侵入させ、お客さまが振込操作を行うと不正口座へ自動的に送金される。

対策!!

・Phish Wall プレミアム
➡ ｾｷｭﾘﾃｨ対策 ③

セキュリティ対策

セキュリティ対策	特　徴	メリット	デメリット
① ワンタイムパスワードサービス	３０秒毎に作成（生成）される使い捨てのパスワード（ワンタイムパスワード）を入力して振込等の取引を行う。	・ワンタイムパスワードが詐取されても、不正に利用することができない。 ・法人ＩＢと個人ＩＢにおけるハードウェアトークンは、遠隔操作をするウイルス対策に効果がある。	・トークン（パスワード生成機）を準備しないと振込等の取引ができない。 ・トークン変更時に変更前のトークンがない場合は、金庫に届出・登録が必要になる。
② 電子証明書（法人ＩＢのみ）	利用するパソコンを限定する。	・ＩＤ・パスワードを詐取されても、詐取した第三者のパソコンで利用することができない。	・パソコン買替時には金庫への届出・再取得が必要になる。

セキュリティ対策	特　徴	メリット	デメリット
③ Phish Wall ﾌﾟﾚﾐｱﾑ（パソコンのみ）	ウイルスの行い（振る舞い）を検知する。不正送金に特化した対策ソフト。	・発見しにくいデータ改ざんによる不正送金も、改ざんする振る舞いを検知して防止する。 ・ウイルス対策ソフトをすり抜けた最新のウイルスでも防止できる。 ・正しい金庫ホームページでは緑の信号を表示する。	・パソコン毎にソフトをインストールする必要があり、パソコン買替時も再インストールが必要。 ・スピードが多少遅くなる。
④ 市販のウイルス対策ソフト（ウイルスバスター、ノートン等）	ウイルスの侵入を防止する。	・ソフトを発売しているメーカーが確認したウイルスの侵入を防止する。 ・不正送金用のウイルスだけでなく、ウイルス全般の浸入を防止する。	・最新のウイルスを検知する為には、常に更新する必要がある。 ・ソフトを発売しているメーカーが確認していないウイルスの侵入は防止できない。 ・パソコン毎にソフトをインストールする必要があり、パソコン買替時も再インストールが必要。

西尾信用金庫