

当金庫を装った不審な電子メールにご注意ください

現在、インターネットバンキングのパスワードなどお客様の情報を盗み取ろうとする不審な電子メールが、各金融機関とのお取引の有無に関わらず不特定多数のお客様に発信されています。

1. 不審な電子メールとは

電子メールで「セキュリティ強化のためご契約カードを再発行することになった。」などのもっともらしい名目で、お客様を偽装サイトに誘導し、暗証番号を盗み取る手口で、以下の様な電子メールが送られてくる場合があります。

<p>(偽メール例)</p> <p style="text-align: center;">信用金庫より重要なお知らせです</p> <p>信用金庫をご利用のお客様へ</p> <p>平素は 信用金庫をご利用いただきありがとうございます。</p> <p>このお知らせは、 信用金庫のDirectwebをご利用のお客様に送信しております。</p> <p>この度、 信用金庫Directwebのセキュリティ向上に伴いまして、「お客様カード」を再発行することになりました。</p> <p>再発行の手続きはこのメールと一緒に添付されている申し込みソフトに必要事項を記入し、送信していただければ手続き完了となりますので、添付ソフトを右クリックし対象をファイルに保存を選択後、必要事項を記入し送信をお願いします。</p> <p>再発行のカードは、後日郵送で届きますので到着まで現在の「お客様カード」をお使いください。</p> <p>この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします。</p> <p style="text-align: right;">信用金庫 部</p>
--

(注)実際には実在の金融機関名であるほか、一部表現が異なる場合もあります。



指示に従い添付ファイルを右クリックして開くと、次のような画面が表示されます。

お客様カードの(1)(2)・・・(8)に対応した数字を半角でそれぞれ入力してください。							
ア	イ	ウ	エ	オ	カ	キ	ク
(1)	(5)	(2)	(6)	(3)	(7)	(4)	(8)
(1)(ア)	<input type="text"/>	(2)(ウ)	<input type="text"/>	(3)(オ)	<input type="text"/>	(4)(キ)	<input type="text"/>
(5)(イ)	<input type="text"/>	(6)(エ)	<input type="text"/>	(7)(カ)	<input type="text"/>	(8)(ク)	<input type="text"/>
<input type="button" value="送信"/>							

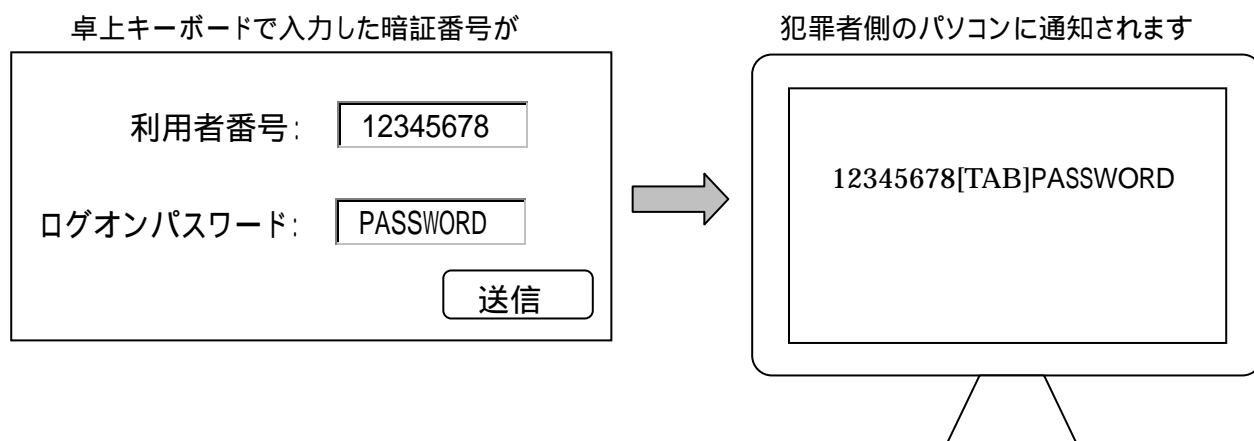
ここで利用者番号、確認用パスワードを入力して送信ボタンを押すと、入力内容が犯罪者側に通知されて「お客様カード」の情報が盗み取られてしまいます。

2. キーロガーを組み込んだウイルスへの感染

キーロガーとはキーボードの入力信号を記録するソフトウェアです。キーロガーを組み込んだウイルスに感染すると、そのパソコンの利用者がキーボードから入力した暗証番号等を記録して、犯罪者側に通知されてしまいます。

キーロガーは、電子メールに添付されたファイルやインターネット上からのダウンロード、他の媒体等(USBメモリなど)により感染することが多くあります。キーロガーによる詐欺を防止する方法として、卓上のキーボードでなく、パソコンの画面上に表示されるキーボード(「ソフトウェアキーボード」といいます)で入力する方法があります。

【ウイルスに感染すると】



ウイルスに感染すると、キーボード入力した暗証番号がいつも簡単に犯罪者側のパソコンで盗みとられてしまいますので、安全管理のためソフトウェアキーボードをご利用ください。

3. お客さまへのお願い

- (1) 当金庫が電子メール等でお客さまに暗証番号をお問い合わせすることはありません。
当金庫が電子メールで暗証番号の入力をご依頼することは絶対にありませんので、決して入力することのないようにご注意ください。また、当金庫職員や警察等が店舗外や電話等で暗証番号の数字をお問い合わせすることもあります。
- (2) 不審なメールが届いたら
不審なメールが届いた場合は、安易にリンク先にアクセスしたり、添付されたファイルを開いたりせず、削除してください。万が一、リンク先の不正サイト等に暗証番号等を入力した場合は、速やかに末尾記載の問い合わせ先(ヘルプデスク)までご連絡くださいますようお願い申し上げます。

4. 今後の安全管理のために

- (1) インターネットサイト(ホームページ等)のご利用時
知らないサイトには訪問しない。
安全なサイトでも、そこで紹介されているリンク先は危険なことがあります。意図しないサイトに移動した場合は画面を閉じてください。また、暗証番号を入力する場合は、正規のサイトであることを必ず確認してください。

不要なファイルはダウンロードしない。

画像ファイルを開くだけでウイルス感染することがあります。ダウンロードしたファイルは、開く前にウイルスチェックを行ってください。

不要な入力をしない。特に個人情報を書き込まない。

入力した情報は不特定多数の人に見られます。また、SSLと呼ばれる暗号化を利用していないサイトでは、入力した内容が第三者に読まれることがあります。入力者の特定による攻撃や情報漏えいにつながります。

(2) 電子メールのご利用時

心当たりのない電子メールは開かない。

ご案内した事例以外に、公的機関やその職員を装って送られることもあります。

メールや添付ファイルに記載されたリンクをむやみにクリックしない。

クリックすることでウイルスなどの不正ソフトがインストールされる場合や、フィッシングサイトに誘導されることがあります。暗証番号を入力するように依頼しているメールに書かれたリンク先は開かなでください。「緊急のお知らせ」等であれば、企業のトップページ等も確認してください。

(3) その他の安全管理

ウイルス対策ソフトを導入し、常時ウイルスパターンの更新を行うことで新しいウイルスに備えることができます。

サポート期限の切れたソフトウェアは、脆弱性の対応がされていないので、極力使用しないことをお奨めします。

新たな脆弱性に対応するため、ソフトウェアは常に更新することをお奨めします。

ファイル交換ソフトは、交換ファイル内に違法ソフトやウイルスが非常に多く危険なため、極力使用しないことをお奨めします。

お子様をご利用するパソコンも、家族や自分自身に被害が及ばないように管理しておくことをお奨めします。

【お問い合わせ先】

不審なメール、サイト等を発見した場合や、心当たりのないお取引があった場合は速やかにヘルプデスクまでご連絡ください。

受付時間 / 12月31日～1月3日を除く平日の9:00～17:00
かわしんヘルプデスク フリーダイヤル：0120-047-581

受付時間 / 12月31日～1月3日を除く平日の17:00～22:00
及び土・日・祝日の9:00～17:00
しんきんIBヘルプデスク：0120-933-810

(※050からはじまるIP電話の方はご利用できません。

以上