

インターネットバンキング・法人WEB-FBにおける ウイルスメールについて

昨今、信用金庫の名をかたった件名のウイルスメール(ウイルスと判定されたファイルが添付されたメール)が多く確認されております。

ウイルスメールは、巧妙かつバリエーションが豊富であり、添付されているファイルを誤って開いてしまうと、ウイルスに感染し情報を抜き取られる恐れがあります。

ついては、インターネットバンキング・法人WEB-FBを安全にご利用いただくため、以下をご参照のうえ、ウイルスメールにご注意いただきますようお願いいたします。

電子メールを開く際の注意点

1. 送信元や件名を確認して、不審なメールと判断したら開封せず削除してください。
2. 開封しても、本文中に不審な点がないか確認してください。
3. 本文中のURLをクリックしないでください。
4. 添付ファイルを開かないでください。開いてしまった場合、マクロの有効化を求められても応じないでください。

ウイルスメールの特徴

1. 送信元

送信元は詐称されている場合があります。

- ・英単語を組み合わせたメールアドレス
- ・ランダム of 英数字を組み合わせたメールアドレス
- ・adminやinfoなどの代表アドレスを連想させるメールアドレス
- ・名前を連想させるメールアドレス

2. 件名、本文

以下のような件名があります。

- ・信用金庫からのお知らせを装った件名
- ・ワンタイムパスワードの利用開始やトークンの交換を装った件名
- ・事故登録解除完了のお知らせを装った件名
- ・資金移動操作完了を装った件名
- ・インターネットバンキングからのお知らせを装った件名
- ・振込受付完了を装った件名
- ・振込に関するお知らせを装った件名
- ・電子証明書の更新完了、更新、再発行のお知らせを装った件名
- ・合併に伴う振込先変更のお知らせを装った件名
- ・ホームページのリニューアルを装った件名

なお、本文には、添付されているパスワード付zipファイルを解凍するためのパスワードが記載されています。

3. 添付ファイル名

(1) ファイル名

- ・ランダム英数字と受信年月日を組み合わせたファイル名
- ・作業計画を連想させるファイル名

(2) 形式

- ・パスワード付きzipファイル(解凍後はdocファイル)

以 上



ふれあい地元とともに

知多信用金庫