

お客さま各位

【重要】信用金庫名をかたった件名のウイルスメールについて

2020年9月以降、信用金庫名をかたった件名のウイルスメール(ウイルスと判断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、巧妙かつ数多くの種類があり、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IDやパスワード等を抜き取られる恐れがあります。

ついては、しんきんインターネットバンキングを安全にご利用いただくため、以下を参照のうえ、ウイルスメールにご注意いただく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.本文中のURLをクリックしないでください。
- 3.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(メールアドレス)

送信元は詐称されている場合があります。

- ・英単語の組み合わせ
- ・ランダムな英数字の組み合わせ
- ・adminやinfoなどの代表アドレスを連想させるもの
- ・名前を連想させるもの

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もの
- ・インターネットバンキングに関するお知らせ
(電子証明書、ワンタイムパスワード、資金移動、振込先等に関すること)
- ・ホームページのリニューアルのお知らせ

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

【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】を押ししてください
受付時間平日9:00~17:00