２０２５年 ３月

お客様各位

金融機関等を騙る不審電話（ボイスフィッシング）や詐欺メールについて

現在、金融機関や関係機関等を装い、インターネットバンキングの利用停止や契約情報の更新、不正アクセスの通知などと不安を煽り、言葉巧みにお客様のメールアドレスやインターネットバンキングの契約者情報、ワンタイムパスワードを聞き出す不審な電話（自動音声含む）や詐欺メールが確認されています。

金融機関や関係機関からお客様に対し、①お客様情報の確認や個人情報等の提供を依頼すること②キャッシュカードの暗証番号、インターネットバンキングの ID・パスワード等の確認や入力をお願いすること③現金等の支払いを要求することは、いずれも一切ありません。

このような電話があった場合は、速やかに電話を切り、誘導された操作は絶対に行わず、メールや SMS についても絶対にリンク先 URL のクリックや添付ファイルの開封等せず、当該電子メールを削除する（下記参照）など、ご注意いただきますようお願い申し上げます。

万が一、アクセスされた場合には、速やかにインターネットバンキングのパスワード変更を実施ください。

また、少しでも不審に感じられましたら、すぐに当金庫へお問い合わせください。

以　上

まっすぐ未来
滋賀中央信用金庫

【ボイスフィッシングの概要】

・悪意のある第三者が金融機関担当者を騙り、電話をかけ（自動音声の場合あり）、メールアドレスを聞き出す。

・聞き出したメールアドレスへ詐欺メールを送信し、電話で指示をしながら、フィッシングサイトへ誘導、インターネットバンキングの契約者情報やワンタイムパスワード情報等を入力させ、盗み取る。

・フィッシングサイトに入力された情報を使い、第三者がインターネットバンキングへログインし、口座から資金を不正に送金する。

【不審メールの概要】

・不審メールのリンク先 URL を開くと、信用金庫業界等のポータルを騙ったフィッシングサイトへ誘導され、ID やパスワードが盗まれたりウィルスに感染したりする可能性がある。

≪被害防止に向けて≫

・金融機関の担当者を騙る者から連絡があった場合には、取引店窓口へ連絡し確認するなど慎重にご対応ください。

・電話やメール、SMS 等で契約者情報やパスワード等の入力を求められても、回答や入力は絶対に行わないでください。

・メールや SMS に記載されているリンク先の URL はクリックせず、添付ファイルも開封しないでください。

・万が一、アクセスされた場合には、速やかにインターネットバンキングのパスワード変更を実施ください。

・インターネットバンキングのログイン時は、当金庫ホームページからアクセスください。

・振込限度額が普段の取引金額と比べ過大になっていないか、再度ご確認ください。

・各パスワードやトークンの管理を徹底ください。

・パソコンからご利用の場合は、ご利用のパソコンに Rapport をインストールください。（アクセスしているウェブサイトが本物であることをご確認いただけます。）

・ログインパスワードを定期的にご変更ください。

（インターネットバンキングにログイン後のサービスメニューよりご変更いただけます。）