現在、法人のお客さまを狙った「ボイスフィッシング」と呼ばれる巧妙な詐欺電話が増えております。

悪意のある第三者が「インターネットバンキングの利用を停止する」「インターネットバンキングの契約情報を更新する」「不正なアクセスがあった」など不安を煽り、言葉巧みに、お客さま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等を聞き出そうとする不審な電話が確認されております。

当行では、当行発信での自動音声の電話案内を一切行っておらず、自動音声や電話、E-mail 等でお客さまの契約者情報やパスワード等をお伺いすることは一切ございません。

このような電話があった場合は、すぐに電話を切り、誘導された操作については絶対に行わないようにしてください。

ー　手口のポイント　ー

- 銀行を装う偽のショートメッセージ（SMS）やメールを送りつけ、偽のホームページ（インターネットバンキングの模倣画面）へと誘導する
- ID やパスワードなどの情報を入力させて盗み取り、口座から預金を不正に引き出す

ー　対策のポイント　ー

- 不審な SMS やメールは開封しない
- SMS やメールに記載された URL に安易にアクセスしない
- URL へアクセスする前に、正しいホームページの URL であるかを確認する

ー　手口の例　ー

- 銀行を装った偽の SMS やメールを送るなどして、インターネットバンキングのログイン画面を精巧に
- 模倣した偽のホームページに誘導し、インターネットバンキングにおける ID やパスワード、乱数表、合言葉などの認証情報を入力させて盗み取り、口座から預金が不正に送金されるものです。

＜銀行を装った偽の SMS 例＞

- また、携帯電話会社などの他社を装い、偽のホームページにアクセスさせ、入力を進めていくと、銀行の偽のホームページにリンクし、インターネットバンキングにおける ID やパスワードなどの情報の入力を求められる場合もあります。
- 金融機関を装い、マネー・ローンダリング・テロ資金供与・拡散金融対策（マネロン等対策）の名目で、お客さまの口座暗証番号・インターネットバンキングのログイン ID・パスワード等を不正に入手しようとするフィッシングメールも確認されています。

ー　犯罪の防止策　ー

不審な SMS やメールは開封しない

- 予め銀行からの注意喚起内容を確認し、ID やパスワードの入力は慎重に行う。

SMS やメールに記載 URL に安易にアクセスしない

<銀行を装った偽の SMS のメッセージ例>

- お客様の○○銀行口座がセキュリティ強化のため、一時利用停止しております。再開手続きをお願いします。http://marumarubank.○○○○
- お客様の【○○銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定 http://marumarubank.○○○○
- ○○銀行を装う偽メールに注意して、安全のために、設備ロックを行ってください。 http://marumarubank.○○○○
- お客様の○○銀行口座に対し、第三者からの不正なアクセスを検知しました。ご確認ください。 http://marumarubank.○○○○
- 弊社では金融庁によるマネー・ローンダリング及びテロ資金供与対策に関するガイドライン等を踏まえ、お客さまが弊社にご登録されている各種情報等について、メール、DM などの方法で、現在の情報に更新されているかどうかのご確認をさせていただいております。
  ご利用確認はこちら。http://marumarubank.○○○○

URL へアクセスする前に、正しいホームページの URL であるかを確認する

- 表示されたホームページの URL を必ず確認して、不審な URL にはアクセスしない。

※SMS やメールに書かれた URL が正しく見えても、実際にリンクをクリックしてアクセスする URL が違う場合もあります。ご注意ください。

- 正しいホームページの URL を予めブックマークに登録しておき、ブックマークからアクセスする。

本件に関するお問い合わせ先
福邦銀行お客さま相談室
0120-298-294
（平日 9：00～17：00）