金融機関のマネロン等対策を騙ったフィッシングメールにご注意ください

最近、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（以下、マネロン等対策）の名目で、利用者の口座の暗証番号・インターネットバンキングのログインID・パスワードや、クレジットカード/キャッシングカード番号等を不正に入手しようとするフィッシングメールが確認されています。

現在、金融機関等は「マネロン等対策」の一環として、お取引の内容や状況等に応じて、過去に確認した氏名・住所・生年月日・ご職業・取引の目的等につきまして窓口や郵送書類等により再度確認をさせていただく場合がございます。

しかしながら、利用者の暗証番号やインターネットバンキングのログインIDおよびパスワード等について、お客様に対してメールやSMSで直接お問い合わせたりすることも、メールやSMSを利用してウェブサイトに誘導したうえでこれらの入力を求めるようなこともございません。

こうしたフィッシングの被害に遭わないために、

- 心当たりのないメールやSMSに掲載されたリンク等は開かない。
- 不審なメールやSMS等を受信した場合には、直接金融機関に問い合わせる。
- 金融機関のウェブサイトへのアクセスに際しては、事前に正しいウェブサイトのURLをブックマーク登録しておき、ブックマークからアクセスする。
- 各金融機関のウェブサイトにおいて、インターネットバンキングのパスワード等をメールやSMS等で求めないといった情報を確認する。
- パソコンのセキュリティ対策ソフトを最新版にする。

といった対策を実施するなど、十分にご注意をお願いいたします。

《主な手口としては…》

① 金融庁が公表している『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』への対応のためであるとして、金融機関の名前で暗証番号・インターネットバンキングのログインID・パスワード等を確認する必要があるといった説明と一緒に、金融機関の偽サイトのURLが記載されたメールやSMSが送信されます。

② 偽サイトのURLをクリックすると自動的に入力フォームが表示され、そこに

暗証番号やパスワード等を入力・送信することで第三者に個人情報が詐取されてしまいます。

あかぎ信用組合

This page designed by ALON corporation