2020年1月9日

お客様各位

株式会社　佐賀共栄銀行

【重要】　フィッシング詐欺にご注意ください。

警察庁の発表によりますと、フィッシング詐欺【※】によるインターネット バンキングの不正送金被害が全国的に増加しており、2019年11月の被害件数（573件）と被害総額（7億7,600万円）は、いずれも統計を開始した2012年以降で月間最高を記録しています。

つきましては、お客さまの被害防止を図るため、不正送金の手口や対策のポイントをとりまとめてお知らせしますので、内容をご確認のうえ十分にご注意いただくようお願いいたします。

なお、当行からお送りするショートメッセージ（以下、「SMS」といいます。）や電子メールで、インターネットバンキングのID・パスワードや暗証番号等のお客様情報をお尋ねしたり、入力をお願いすることは絶対にございません。万一、疑わしいウェブサイト等にインターネット バンキングのID・パスワードや暗証番号等のお客様情報を誤って入力された場合には、末尾記載の問い合わせ先へ速やかにご連絡くださるようお願いいたします。

【※】　フィッシング詐欺とは、銀行やショッピングサイトなどを装ったSMSや電子メールを送りつけ、正規ホームページとそっくりの偽サイトに誘導し、パスワード等の重要情報を入力させて盗み取る手口をいいます。

記

フィッシング詐欺の手口

［1］　以下の例のような銀行を装った偽のSMSや電子メールを送りつけ、偽のホームページ（もしくは、インターネットバンキングの模倣画面）へ誘導する。

＜例1 ＞　お客さまの口座セキュリティ強化手続きが未完成のため、再開手続きをもう一度お申し込みください。⇒https://●●●●●.com

＜例2＞　お客さまの銀行口座はセキュリティ強化手続きが未完成のため、再開手続きをもう一度お申し込みください。 ⇒https://●●●●●.com

＜例3＞　お客さまがご利用の口座が不正利用されている可能性があります。
口座一時利用停止、再開手続きはこちらへ⇒https://●●●●●.com

＜例4＞　セキュリティ強化の為、本人認証する前に口座は一時利用停止となります。
本人認証の設定はこちらへ⇒https://●●●●●.com

＜例5＞　お客さまの銀行口座に対し、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。⇒https://●●●●●.com

［2］　IDやパスワードなどの情報を入力させて盗み取り、預金を不正に別の口座に送金する。

フィッシング詐欺対策のポイント

➢ 心当たりのない不審なSMSや電子メールは開封しない。

当行がお送りするSMSの正規発信元電話番号は次のとおりです。

① docomo、auユーザーさま向け ⇒ 0952-26-2161（営業統括部リテール営業グループ）
0952-37-0379（営業統括部ローン管理グループ）

② ソフトバンクユーザーさま向け ⇒ 0032069000

➢ SMSや電子メールに記載されたURLに安易にアクセスしない。

➢ 当行からお送りするSMSや電子メールで、インターネットバンキングのID・パスワードや暗証番号等のお客様情報をお尋ねしたり、入力をお願いすることは絶対にありません。

＜ 本件に関するお問い合わせ先 ＞

佐賀共栄銀行 事務統括部 システムグループ
0952-22-2244 （受付時間は、銀行営業日の9:00～17:00です。）

以 上