2020 年 11 月 23 日

お客さま各位

SMBC コンシューマーファイナンス株式会社

当社を装った詐欺サイト（フィッシング詐欺）にご注意ください

いつもプロミスをご利用いただき、ありがとうございます。

今般、プロミスを装って送られてきたＳＭＳのリンク先をクリックすると当社ホームページと酷似したページに誘導され、お客さまのＩＤやパスワード等を入力させ、不正に個人情報を取得しようとする事案が発生しております。
これらの偽装されたページにログインすると、フィッシング詐欺の被害に遭われる可能性が高くなりますので、ログインすること及びログイン後にお客さまの個人情報の入力等は絶対に行わないでください。
万が一被害に遭われた場合は、最寄りの警察署もしくは消費者生活センター等へお問い合わせください。
ご相談・お問い合わせがございましたら、プロミスコール（0120-24-0365）までご連絡いただきますようお願いいたします。

【実例】
以下の文面で、プロミスを装ったＳＭＳが送られます。
「お客様のプロミスに対し、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。」
この文面に「hxxps://is.gd/JBDTY5」というＵＲＬが記載されており、そのＵＲＬをクリックすると「hxxps://my-promise.com/」偽装されたページに誘導され、ＩＤやパスワードを入力する画面が表示されます（ＵＲＬは、アクセスを避けるため一部伏字しております）。
※類似のＳＭＳにもご注意ください。

【プロミスが提供するホームページの確認方法】
プロミスのホームページを閲覧の際は、アドレスバーのURLが「https://cyber.promise.co.jp」から始まっていることを確認してください。

【フィッシング詐欺とは】
フィッシング詐欺とは、金融機関などからのメールや Web サイトを装い、口座番号やカード番号、アカウント情報（ユーザーID、パスワードなど）の重要な個人情報を不正に入手し、その情報をもとに本人になりすまして、買い物をしたり、金銭等を騙し取る手口です。

以上

ご相談・ご質問はプロミスコールへ
0120-24-0365
（受付時間：平日9：00～18：00）