HSBC グループの名を騙った投資勧誘や詐欺行為等について

HSBC グループとは無関係の第三者による、HSBC と誤認される名称を使用した違法な投資勧誘やその他詐欺的な行為が発生しております。昨今においては電話だけでなく、ソーシャルメディア（SNS）やメール、携帯アプリを使った詐欺的な行為が発生しており、投資した資金が戻ってこないという問い合わせを多く受けております。このような投資勧誘等により、被害または迷惑に遭われた場合は、最寄りの警察署等に対応をご相談いただき、HSBC との関係についてご不明な点がある場合は、こちらまでご連絡ください。
下記は一例となっております。

- SNS を通して、HSBC の抽選に当選したので、賞金の振り込みに送金手数料をプリペイドカードの番号を送信させる
- SNS を通して HSBC の名を騙った行員がシリア震災復興の為の寄付を募ったり、遠い親戚の遺産が相続できるなど呼び掛け、送金手数料を振り込ませる
- HSBC の名を騙った FX アプリを提供し、少額の投資で儲けさせ、徐々に金額を上げて返金しない

フィッシング詐欺 / スパムメール
フィッシング詐欺とは、金融機関等を装い、偽のウェブサイトで ID やパスワード等を入力させ、それら個人情報を利用して預金を不正に引き出したり、なりすまし口座を開設する等の犯罪を言います。
フィッシング詐欺を働く者は、あたかも実在の金融機関等から皆様にメールが送られているかのように装います。そのようなメール（スパムメール）を受信された場合は、添付ファイルを開けることなく、直ちに削除していただきますようお願いいたします。こういったメールを見破るのは容易ではなく、また詐欺の手口自体も常に変化していますが、一般的には以下のような特徴があります。

- 送信者の E メールアドレスが信頼できる金融機関等のウェブサイト上のアドレスと一致しない。
- 金融機関等の名を騙っているが、送信元がその金融機関等と全く違う E メールアドレスや、無料の E メールアドレスである。
- E メールの宛名がお客様の名前ではなく、「お客様各位」など不特定多数向けのものになっている。
- 目立つようにウェブサイトがリンクされている。このような偽造ウェブサイトは正規のものと酷似していますが、ほんの一文字の違いでも、それは別のウェブサイトになることにご留意下さい。
- ユーザーネーム、パスワード、取引の詳細などの個人情報を入力するよう要求される。

- 心当たりのない送信元からのＥメールである。

偽装ウェブサイト

偽装ウェブサイト詐欺を働く者は、容易にウェブサイトを偽造することが出来ます。そのようなウェブサイトを見破るためには、以下のような点に留意して頂く必要があります。

- 会社の実体を示すもの、例えば、住所や電話番号などの記載があるか。疑いがある場合、電話を掛けたり、文書を郵送するなどして、実際に存在している場所の特定に努めて下さい。
- ウェブサイトのアドレスが見慣れたものと異なっているか(新たな文字や文言が足されていたり、全く違う名称を使用したり、数字のみで名称を全く使用していない例があります)。
- ハイパーリンクを右クリックし、プロパティを選択すると、リンク先がわかります。Ｅメールに書かれているリンク先と違う場合には、注意が必要です。
- 通常はユーザーネームのみ確認されるのに、突然ユーザーネーム、パスワード、及びその他の詳細などの全ての個人情報の照会があった場合。