最近の詐欺被害等に関する注意喚起

令和５年３月２０日
在ドバイ日本国総領事館

【ポイント】
●新たな手法の詐欺として、配送サービスを装ったケースが確認されています。
●政府機関関係者を名乗る者による詐欺、起業家や投資家を狙った詐欺も引き続き確認されています。
●当館ＨＰに掲載している注意喚起も改めて御覧いただき、詐欺の被害に遭わないよう注意してください。
●不動産や仮想通貨等の投資案件に起因する日本人同士のトラブルも散見されていますのでご注意ください。

【本文】
本年に入り、報道ベースでのみ明らかになっているものも含めて、以下のような手口の詐欺が横行しています。それらの中には、配送サービスを装った新たな手口の詐欺も確認されています。これまでの当館からの詐欺被害防止に関する注意喚起も改めて御覧いただき（以下４参照）、同類の詐欺被害に遭わないよう注意してください。
また、当館には、不動産や仮想通貨等の投資案件に起因する日本人同士の金銭トラブルに関する相談も多く寄せられています。こうしたトラブルにも巻き込まれることがないよう、事前の調査、情報収集に努めてください。

１　配送サービスを装った詐欺（所謂、フィッシング詐欺）
（１）手口
ア　詐欺の新たな手口として、大手配送業者からのメッセージを装って「配送料支払い」のためのリンクとして偽造した不正なウェブサイトに誘導させ、個人情報をだまし取り、銀行口座からお金を詐取する手口が確認されています。
イ　また、当館が把握している情報によれば、いわゆるフリマサイトの買い手を装って、「出品されている商品を購入したいが引き取りに行けない。こちらで配送業者を手配する。」などと述べて出品者にアプローチし、その後の配送手続のためのリンクとして不正なウェブサイトに誘導するケースもあるとのことです。
（２）対策
ア　身に覚えのないメッセージに添付されているリンクには絶対にアクセスしない。
イ　フリマサイトの相手から指定されたリンクであっても安易にアクセスしない（相手が指定したリンクからではなく正規のウェブサイトからアクセスする、相手が指

定したリンクの URL と正規のウェブサイトの URL を比較するなどして、不正なウェブサイトにアクセスしてしまわないよう注意してください。)。

２　政府関係者を名乗る者による詐欺

（１）手口

ア　連邦内務省等の政府機関関係者を名乗る者が SMS や電話でアプローチし、登録情報の更新のためなどと述べて、個人情報をだまし取るケースが引き続き確認されています。

イ　相手は、メッセージのやり取りや通話の中で聞き出した被害者の個人情報を使って政府機関のサイトに不正にログインし、被害者から聞き出した以上の個人情報を詐取した上でその情報を被害者に送りつけ、自身が当局関係者であることを主張して被害者を誤信させ、要求をエスカレートさせることもあるようです。

（２）対策

ア　SMS や電話でむやみに個人情報を開示しない（政府機関や銀行が SMS や電話で個人情報の更新を行うことはあり得ません。)。

イ　チャットを中断する、電話を切るなどして相手との接触を一旦中断する。

ウ　真正な連絡かどうか迷う場合には、相手からの指示に従うのではなく、代表電話にかけ直して手続の必要性について確認する。

３　銀行融資のサポートを装った詐欺

（１）手口

ア　起業家や投資家に対し、銀行からの融資をサポートするなどと述べてアプローチし、被害者の代わりに銀行からの融資を受けるための手数料と称してお金をだまし取るケースが確認されています。

イ　これまでにも、いくつかの起業家や投資家のドバイでの起業や事業拡大を支援し、成功しているとした実績をアピールするほか、銀行に知り合いや友人がいるなどと述べて、銀行からの融資が容易に得られると誤信させてくるようです。

（２）対策

ア　「おいしい話」を安易に信用しない。

イ　相手の説明だけに頼ることなく、「信頼できる業者であるか」、「提案されている手続は適正か」について、自身で情報収集する。

４　当館ＨＰ「詐欺被害に関する注意喚起」

https://www.dubai.uae.emb-japan.go.jp/itpr_ja/visa_top.html

※上記ＨＰの「5. 詐欺被害に関する注意喚起」をご参照ください。