「UAE PASS」を悪用した詐欺への警戒

令和５年 10 月 24 日
在ドバイ日本国総領事館

【ポイント】
●当地の行政手続等で利用されている「UAE PASS」を悪用した詐欺が横行しています。
●「UAE PASS」の仕組み上、携帯電話番号を入力すれば、誰でも他人の「UAE PASS」の認証要求画面を遠隔で起動させることができます。
●自身で操作していないにも関わらず、「UAE PASS」の認証要求画面が突然表示され、その直後に電話が架かってきた場合には、焦ることなく冷静に対応してください。
●当地では様々な手口の詐欺が横行していることを理解の上、引き続き詐欺に対する高い警戒を維持してください。

【本文】
当地の行政手続等で利用されている「UAE PASS」を悪用した詐欺が横行しています。その手口や対策を以下のとおり御案内します。当館のこれまでの注意喚起等も改めて御覧いただき（以下４参照）、当地では様々な手口の詐欺が横行していることを認識の上、詐欺の被害に遭わないよう、引き続き詐欺に対する高い警戒を維持してください。

１　「UAE PASS」について
(1)　概要
「UAE PASS」はアラブ首長国連邦（UAE）政府が承認したデジタル ID であり、政府機関のほか一部の民間企業においても利用されています。「UAE PASS」のアプリケーションをダウンロードし、登録することで利用可能となります。登録時にエミレーツ ID 番号、携帯電話番号、メールアドレスの入力が求められます。最後に顔認証や指紋登録を行うと登録完了となります。
登録後は、「UAE PASS」によるサービスを提供している機関や企業のウェブサイトやアプリケーションに、ユーザーID やパスワードを入力することなく、顔認証や指紋照合のみでログインすることが可能となるほか、「UAE PASS」のアプリケーションを通じて公的書類の取り寄せをはじめ各種申請手続が電子上で行えるようになります。
(2)　「UAE PASS」を利用したログイン方法の一例
①政府機関のウェブサイトにて、個人のアカウントにログインする際、「UAE PASS」によるログインを選択
②ウェブサイト上で対象となる個人のエミレーツ ID 番号、メールアドレス又は携帯電

話番号の入力が求められる

③「UAE PASS」の登録時に登録したエミレーツ ID 番号、メールアドレス又は携帯電話番号のいずれかの情報を入力する

④「UAE PASS」のアプリケーションをダウンロードした携帯電話等で「UAE PASS」のアプリケーションが自動的に起動し、認証が求められる

⑤「UAE PASS」のアプリケーション上で、事前に登録した認証方法（顔認証／指紋認証）で承認を行う

⑥ウェブサイト上でログインが完了する

２　「UAE PASS」を悪用した詐欺の手口の一例

突然、「UAE PASS」のアプリケーションが起動し、ログイン認証画面が表示されるとともに犯人から電話が架かってきます。犯人は電話口で「政府機関の職員である。現在、ドバイで不正な取引が多発しているので、居住者一人一人に確認の作業を行っている。」などと騙った上で、起動している「UAE PASS」の認証要求を承認するよう求めてきます。

これに応じて「UAE PASS」の認証要求を承認してしまうと、犯人に個人情報を詐取されてしまいます。また、犯人は、入手した個人情報（エミレーツ ID 番号や携帯電話番号等の個人情報）をあたかも元から知っていたかのように装って、自分が政府機関の職員であると信じ込ませ、その上で銀行口座情報を聞き出そうとしたり、「送金手続のテストを行う」などと言って現金を犯人の銀行口座に送金させようとします。

また、犯人が銀行のウェブサイトから「UAE PASS」の認証画面を起動させた場合には、犯人からの要求に応じて「UAE PASS」の認証要求を承認した時点で、犯人が銀行口座の操作（送金や PIN コードの変更）を行えるようになってしまうケースもあり得ます。

３　対策

犯人からの電話は「05XXXXXXXX」の携帯電話番号から架かってきますが、政府機関の職員等が携帯電話で個人に直接連絡することは通常はあり得ません。身に覚えのない携帯電話番号の相手方が、政府機関の職員、警察官、銀行員等を名乗る場合、詐欺である可能性を疑ってください。

「UAE PASS」のログイン時、上記１⑵③で携帯電話番号を入力すれば、誰でも他人の「UAE PASS」の認証要求画面を遠隔で起動させることができます。犯人はこの点を利用して、無作為に携帯電話番号を入力して他人の「UAE PASS」の認証要求画面を遠隔で起動させ、その直後に入力した電話番号に電話を架けることで、あたかも「UAE PASS」を操作する権限のある政府関係者であるかのように装いますが、電話の相手が政府機関の職員であるとは限りません。「UAE PASS」の機能を十分に理解の上、「UAE PASS」の認証要求画面が突然表示された場合でも、焦ることなく冷静に対応してください。

また、普段は詐欺と見破れるような内容の連絡であっても、偶然にも、エミレーツ ID

等の身分証を更新した直後や銀行口座の登録情報の更新を行った直後に、犯人から電話が架かってくると、「あの時の更新作業でトラブルがあったのか」などと、詐欺に対する警戒心が緩んでしまい、犯人の要求に従いやすくなってしまうこともあり得ます。身分証の更新や銀行口座の登録情報の更新を行った後でも、普段と同じく詐欺に対する高い警戒心を維持するよう心がけください。

犯人からの連絡を受け、どうしても不安が解消されない場合には、そのまま相手の指示に従って行動することなく、すぐに電話を切り、一人で悩まず、周囲の信頼できる人や当館に相談してください。犯人との電話を切り、犯人が名乗った機関（警察、銀行等）に直接連絡し、手続の必要性について確認することも不安を解消する方法の一つです。特に電話による詐欺の場合、被害者に冷静に判断させないようにするため、「この電話で手続を終えないと大変なことになる。」などと強く不安を煽って来ることもありますが、電話を切られて困るのは犯人だけですので、冷静になって、相手との接触を断つようにしてください。

４　当館ＨＰ

詐欺被害の防止に関する情報

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

※上記ウェブサイトの「詐欺被害の防止に関する情報」をご参照ください。