

特殊詐欺事件（政府関係者なりすまし詐欺）に関する注意喚起

最近、ICA（入国管理庁）やMOM（人材開発省）、SPF（警察庁）の職員になりすまし、ビデオ電話やSMS等で銀行口座番号や暗証番号、ワンタイムパスワードを聞き出す、またはPAYNOWなどによりその場で送金させる手口の詐欺が増加しており、日本人の方も被害に遭われています。政府関係者が個人のビザやパスポート等に関する事項で、電話やSMS等で、IDや口座番号、暗証番号やワンタイムパスワードなどを尋ねること及び指定口座にお金を振り込ませたり、送金させたりすることは決してありません。詐欺の被害に遭わないよう、細心の注意をお願いします。

1 典型手口

ICAなどの政府関係者を名乗る人物からビデオ電話（ビデオ電話の場合は相手が制服を着ている若しくは警察手帳などを提示してくる）やWhatsApp若しくはSMSで、ビザが無効になった、パスポートや銀行口座が他国で悪用されたなどといったメッセージが届きます。まずは本人確認のためとパスポート番号やID番号、さらには銀行口座番号などの個人情報を聞き出し、そして、「ビザを更新する必要がある」「被害を回復するためあなたの協力が必要である」などの口実で、PAYNOWなどにより、その場で指定の電話番号等に送金させるよう指示してきます。言葉が通じないなどの場合でもアプリを使用し、日本語に翻訳したメッセージを通話中でも送ってくるなど、手の込んだことをしてくる傾向も見受けられます。

また、最近はマルウェアと呼ばれるリンクをSMSなどでいきなり送りつけ、開いた瞬間にスマートフォンを乗っ取られ、電話内のアプリから個人情報や銀行口座情報を抜かれるという事例も増加しています。

2 対応策

- (1) 少し前までは、+65 から始まる電話番号をシンガポール国内で受けた場合、ほぼ詐欺師からの電話だと言えましたが、最近は、+65 以外から始まる国際電話や国番号を表示しない電話番号も詐欺に使用されています。また、電話に出て、音声アナウンス案内が流れるものは全て詐欺です。さらにいきなりWhatsAppなどのビデオ電話をかけてくる場合がありますが、これらについても無視するか、出てしまったとしてもすぐ電話を切るようにして下さい。SMSも無視し、WhatsAppメッセージであれば、ブロックして、アプリ管理者に報告して下さい。
- (2) 警察、公共機関などが個人情報や銀行口座番号、ワンタイムパスワードを電話やメールなどで尋ねることはありません。他人からの要求により、電話やメール、チャットアプリなどでIDや銀行口座番号、ワンタイムパスワードを決して教えないようにして下さい。
- (3) もし、何度も電話やSMSなどで連絡がある場合は、その場で対応せず、一旦電話を切って、自ら警察などの政府機関などに電話やメールをし、相談して下さい。大使館に相談してもらっても結構です。

3 もし被害に遭ってしまったら…

- (1) 口座をお持ちの銀行の緊急対応電話へ速やかに連絡してください。(キャッシュカードの裏側等に緊急電話番号が記載してあります)。
- (2) また、最寄りの警察へ被害届 (POLICE REPORT) を提出してください。これは警察に足を運ばなくても SPF のウェブページの「I Witness」というサイトからも提出可能です。

<https://www.bing.com/ck/a?!&&p=49f00639c742247fJmltdHM9MTY5Nzc2MDAwMCZpZ3VpZD0zNWQyMmQ2OS0wZjU2LTY0Y2UtMGQ1My0zZWNiMGU5NzY1YWImaW5zaWQ9NTE5MA&ptn=3&hsh=3&fclid=35d22d69-0f56-64ce-0d53-3ecb0e9765ab&psq=iwitness&u=alaHR0cHM6Ly93d3cucG9saWNlLmdvdi5zZy9pd210bmVzcw&ntb=1>

- (3) 不審な電話に対応している途中で気づいた場合は、電話等を切って、すぐに銀行に連絡し、速やかに口座の凍結を依頼したうえ、警察に報告してください。