REPÚBLICA DEL PERÚ

CONSULADO GENERAL
LONDRES

- Se comunica a la comunidad peruana en general que se tiene conocimiento de diversas redes criminales que vienen llevando a cabo estafas a personas de diversas nacionalidaddes que desean residir en el Reino Unido.

- La modalidad de engaño se inicia cuando una supuesta compañía briánica contacta al ciudadano ofreciéndole un puesto de trabajo altamente remunerado en el Reino Unido.

- Una vez hecho el contacto con la potencial víctima, se le hace un requerimiento de desembolso dinerario a través de transferencias de persona a persona mediante servicios como MoneyGram o Western Union, con el presunto objetivo de realizar el procedimiento de obtención de visas británicas de trabajo. Luego de recibido el dinero, las enitdades criminales no vuelven a contactarse con las víctimas.

- Debido a ello, resulta importante que esta información sea transmitida no solamente a la comunidad peruana en el Reino Unido, sino también a los connacionales que pudieran residir en otras áreas y que puedan ser víctimas de este delito.

MODALIDADES CONOCIDAS

El contacto:

- Se ofrecen beneficios muy altos (visas rápidas, mucho dinero)
- Se utiliza lenguaje que parece oficial para aparentar veracidad.
- Parece que conocen información real sobre usted (nombre o dirección, o que ha aplicado por una visa)
- Le piden dinero o información personal para solicitar una visa.
- Hay un incremento de esta modalidad utilizando el nombre de la empresa Cairn Energy, que ha emitido un anuncio avisando de estas potenciales estafas (https://www.cairnenergy.com/careers/hoax-offers-of-employment/)

Una empresa formal nunca solicitará información ni dinero, ya que el procedimiento regular de visado es personal y solamente el interesado puede realizarlo. Una empresa real y formal dirigirá al aplicante al enlace web real del gobierno británico (que siempre terminará en gov.uk)

La visita del Home Office

- Una persona se presenta en su domicilio e indica que pertenece al Home Office y ofrece tramitar la visa que necesita (suya o la de un familiar). También pueden ofrecerle tramitar una visa utilizando documentos de sustento falsificados; o
- Una persona llama por teléfono e indica que pertenece al Home Office, y señala que hay un serio problema con su visa. Esta modalidad es más utlizada en contra de estudiantes.
- En ambos casos requieren el envío de dinero a la brevedad (usualmente mediante MoneyGram) para evitar una deportación o cancelación de una visa. En el caso de la oferta de visas con documentos falsos, se solicita a la víctima el apgo mediante vouchers de iTunes

Un oficial del Home Office nunca irá a su domicilio, sino que le atenderá en sus oficinas. Tampoco le llamarán, menos aun si nunca se ha establecido un contacto personal y directo con anterioridad.

La prueba de fondos

El falso empleador o la supuesta tramitadora de visas pedira hacer un depósito como prueba de contar con suficientes fondos para vivir en el Reino Unido hasta recibir su primer salario.

El gobierno británico nunca le pedirá realizar un depósito como prueba. Bastará con evidencias documentales (de estados bancarios, propiedades o garantías)

Páginas web e emails falsos

- Se han registrados página que aducen pertenecer al gobierno británico pero que son falsas.
- Todas las cuentas oficiales del Reino Unido terminan en gov.uk
- Todos los emails tienen los siguientes formatos:
  - Home Office: nombre.apellido@homeoffice.gov.uk
  - Foreign and Commonwealth Office: nombre.apellido@fco.gov.uk xxxxxxxxx@fco.gov.uk
- A veces los emails falsos se ven en la pantalla iguales a los originales, pero al hacerles click generan otros emails con formatos diferentes. Revise siempre el email al que le esta enviando un mensaje.

COMO PROTEGERSE

Sospeche…

- De ofertas demasiado buenas, fáciles o no solicitadas
- Si se le solicita dinero, especialmente en efectivo o a través de medios inseguros o de fácil falsificación (transferencia de persona a persona como MoneyGram) Ukash vouchers, o Paysafecard. Estos métodos de pago no permiten identificar al beneficiario.
- Si le preguntan por los detalles de su cuenta bancaria, tarjetas de crédito o débito, o información confidencial.
- Si se le exige confidencialidad o le presionan para actuar de manera inmediata.
- De una página web que no se vea profesional (con errores de redacción o diseños incorrectos) o si no cuenta con información sobre la organización.
- De emails provenientes de servidores gratuitos, como Hotmail, Yahoo Mail, o Gmail, o aquellos que no terminan en gov.uk.
- De emails que tengan errores de redacción
- NUNCA ENVÍE DINERO SI SIENTE SOSPECHAS, SI LO PRESIONAN O SI SE LA FORMA DE ENVÍO LE PARECE INSEGURA

REPORTELO

- En el Reino Unido:

  Action Fraud al teléfono 0300 123 2040 (https://www.actionfraud.police.uk/)
- En el Perú:

  Policía Nacional del Perú, División de Investigación de Delitos de Alta Tecnología (DIVINDAT) al teléfono 431-8898
- En otros países: Ante la oficina especializada en delitos informáticos de la policía local