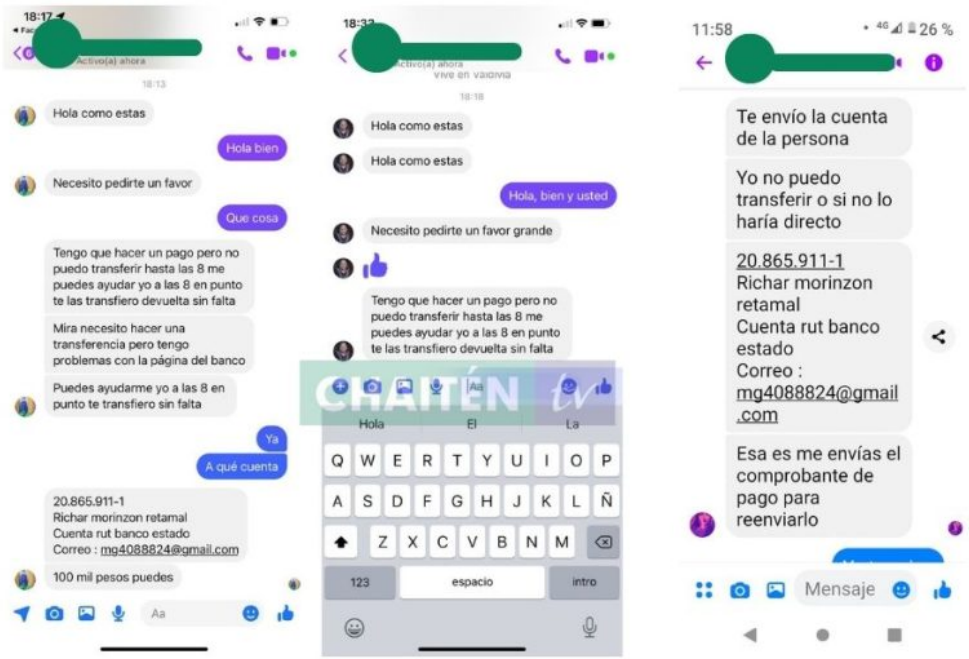
Varias Estafas en estos últimos Días Por Suplantación de identidad en Chaitén

15/11/2022

Varios reportes de personas que han sufrido la suplantación de identidad se han registrados en estos últimos días en nuestra comuna, en redes sociales como Facebook y Grupos de vecinos en WhatsApp han sido el canal de información para alertar de estos casos.

De alguna manera estos antisociales se han apropiado de cuentas de Facebook de vecinos y a través de esta Messenger envían mensajes a los contactos pidiendo dinero, se detecta un modo de operar similar, una vez que se adueñan de la cuenta proceden a contactar y embaucar a los conocidos de la víctima solicitando un favor, poder transferir urgente una cierta cantidad de dinero ($80.000, $100.000 o más), con la promesa que devolverá muy pronto.



Recomendaciones para no caer en estas estafas:

No entregues claves o datos personales a través de un mensaje de texto WhatsApp o llamada telefónica.

No hagas clic en vínculos dentro de mensajes de personas o contactos que no conozcas, que te pidan claves de cuentas bancarias, actualización de datos o contraseñas etc. En el caso de que el enlace venga de un contacto registrado, ve bien el tipo de link y como recomendación no lo abras puede que a tu contacto lo hallan infectado con algún malware.

Corta cualquier llamada sospechosa o poco confiable. No tengas miedo a ser descortés.

No dejes tus perfiles abiertos cuando termines de ocupar algún dispositivo y cambia las claves de forma permanente.

No entregues tus datos personales a través de mensajes públicos, utiliza mensajes privados o DM.

¿Qué es Phishing?

Es una práctica utilizada por cibercriminales para la captación de datos personales a través de internet. De ese

modo, pueden suplantar la identidad de las personas para acceder a sus cuentas bancarias o usar sus identidades para cometer ilícitos.

Consejos de la Brigada Investigadora del Cibercrimen para prevenir ser víctima de este tipo de delitos:

- Tener conciencia que ninguna entidad ni empresa le va a solicitar que ingrese datos personales o el nombre completo, rut, claves, a través de Internet o por medio de llamadas a red fija, celulares o mensajes de textos.
- Nunca debe entregar sus claves de acceso.

- Desconfiar de todo correo electrónico, sobre todo si no proviene de la misma empresa y menos si se le solicita entregar datos personales o alguna clave de acceso.
- A lo que se refiere en particular al phishing, los usuarios de computadoras deben fijarse que cuando reciban un correo electrónico de un entidad o empresa privada que le pida clickear para entregar datos personales, debe tener presente que cuando haga clic, se abrirá una ventana muy parecida a la original, sin embargo, se deben fijar en la dirección http//www pues esta será una página completamente desconocida o, quizás, tenga un nombre parecido para despistar, pero será falsa.

Mas información o denuncias en Policía de Investigaciones de Chile