

## COMUNICADO

### ALERTA

#### CIBERCRIMEN – PDI

Santiago, 05 de noviembre de 2015

La **Brigada Investigadora del Ciber Crimen Metropolitana de la PDI** ha recibido en los últimos días, diversos reportes que dan cuenta de la existencia de una página falsa que simula ser del “Banco Santander”, administrada por delincuentes que mediante la técnica del PHISHING, pretenden apoderarse del rut, contraseña de acceso y superclave de transferencia bancaria de los titulares. Estos datos, posteriormente les permiten acceder a los perfiles de sus víctimas, con la posibilidad de sustraer electrónicamente el dinero de la cuenta.

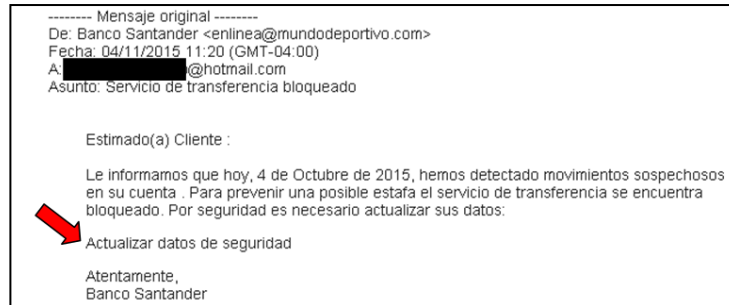
Por lo anterior la **Brigada del Ciber Crimen Metropolitana de la PDI**, junto al “**Banco Santander**”, recuerdan a los usuarios las siguientes medidas de auto cuidado para la utilización de la banca electrónica:

- Mantenga instalados software anti virus actualizados.
- Cree claves seguras y cámbielas periódicamente, sin guardar la contraseña en la opción que ofrece el navegador.
- Digita la dirección del banco ([www.bancosantander.cl](http://www.bancosantander.cl)).
- Consulte periódicamente los movimientos de su cuenta y reporte cualquier transacción sospechosa (enviada o recibida) a la sucursal bancaria más cercana o a los números de call center disponibles.
- El banco NUNCA solicitará sus claves (de acceso o transferencia) vía telefónica en forma verbal. Éstas solo se solicitan cuando se realiza una transacción bancaria y deben ser ingresadas directamente con el teclado del equipo.
- Los e-mails de Banco Santander no contienen link, botones ni enlaces.
- Evite ocupar equipos computacionales desconocidos para realizar operaciones electrónicas bancarias.

## COMUNICADO

A continuación se describe una imagen de referencia del correo electrónico falso que simula ser del Banco Santander y la presentación de la página falsa en el navegador.

### CORREO ELECTRÓNICO FRAUDULENTO



### PAGINA FALSA DEL BANCO SANTANDER

