

## OJO CON FALSO MAIL DE LOS 33 MINEROS: PUEDEN DESVALIJARLE LA CUENTA



Cuidado con esos **correos electrónicos** que difunden supuestas fotos de **Angelina Jolie desnuda** o el **último chascarro de los 33 mineros** de Atacama. Pueden tener un **troyano** que le vaciará la cuenta corriente.

El troyano es una **aplicación maliciosa** que en vez de llevar al usuario a la página de su banco, lo enviará a una creada por un estafador que replica a la original. **El incauto**

**entregará sus claves y datos y sufrirá el robo de su dinero.**

**Eduardo Albornoz, subcomisario de la Brigada del Cibercrimen** de la Policía de Investigaciones (PDI), explica que este delito se llama **pharming** (del inglés farm, "granja" en castellano, porque es como si un intruso ingresara a una granja y dispusiese de todos sus bienes).

"El pharming **busca obtener dinero de las cuentas corrientes**, cuentas vista, líneas de crédito, tarjetas, todo lo que sea por Internet", explica el subcomisario Albornoz.

"El troyano se instala en el computador y modifica un archivo del sistema operativo para que, cada vez que la víctima entre al navegador, **llegue siempre a la página del delincuente** y nunca a la página legal", añade.

El pharming es un delito parecido al **fishing** (del inglés fish, pescar). Éste consiste en un correo electrónico por el cual los **estafadores se hacen pasar por el banco**, copian la página y solicitan que el cliente actualice sus datos.

"Le comunican que **su cuenta se encuentra bloqueada y que necesitan revalidar los datos**. La gente ingresa nombres, RUT, dirección, teléfonos, claves y también su tarjeta de coordenadas que permite hacer transacciones financieras por Internet", explica Albornoz.

"Ingenuamente, la gente todavía no entiende que **nunca el banco le va a pedir completamente las coordenadas**, sino que sólo los primeros tres dígitos para la transferencia, nada más que eso. Nunca va a pedir actualizar los datos por Internet ni por teléfono, porque también existe el fishing por teléfono", agrega.

**División Seguridad Privada**

“En esta última modalidad, los estafadores meten un cuento del tío por teléfono, por ejemplo, que en tal parte del mundo está un familiar que necesita le envíen plata porque no puede salir del país y la gente cae”, indica.

Además, el subcomisario señala que en esta época del año **aumentan las estafas** con las compras que se hacen por Internet, sobre todo con productos en boga como los computadores y celulares. “Los delincuentes no envían los productos y se quedan con el dinero depositado”, explica.

**RECOMENDACIONES PARA NO CAER**

Para evitar ser víctima de estos delitos subcomisario Albornoz recomienda **no realizar transacciones electrónicas en un cibercafé**, porque pueden tener aplicaciones espías que capturan sus contraseñas. Siempre hacerlo en un lugar seguro y único, su domicilio.

Tampoco en la oficina, porque muchas veces ocupan los computadores varias personas, y **nunca dar las claves por teléfono**, sea cual sea el cuento que inventen.

Asimismo, **tener los antivirus actualizados**, para que detecten la entrada de aplicaciones maliciosas. **También los cortafuegos**.

“La seguridad de las claves siempre es **responsabilidad del cliente, no del banco**, porque todo lo que se hace por Internet es mediante claves y quién cuida las claves, la persona”, recalca el subcomisario.

“La **seguridad en Internet nunca va a ser del 100%**, entonces lo que se busca es disminuir los riesgos, pero siguiendo estas recomendaciones la persona no va a tener problemas”, afirma.

“En cuanto a las estafas, es muy importante **ver la reputación** que tiene el vendedor en la página, si le han comprado antes o no. Confirmar los celulares, sus correos electrónicos, sus nombres y después buscarlos en **Google** y ver qué aparece. A los estafadores los denuncian”, señala.

**“SIEMPRE INVENTAN ALGO”**

En promedio, la Brigada del Cibercrimen recibe **400 órdenes de investigar mensuales**, de las cuales el 80% son por estafas fishing, pharming. El resto es por **pornografía**.

“Estos delitos aumentan año a año, porque los delincuentes siempre inventan algo. Por ejemplo, el troyano puede llegar a través de un supuesto correo de los mineros. “Vea tal cosa de los mineros”, dice el mail, la gente hace click en una **aplicación como un power point** y descarga una aplicación maliciosa, un troyano”, concluye el subcomisario Albornoz.

Fuente. [www.lanacion.cl](http://www.lanacion.cl)