

## Seguridad en Internet

### Robo de identidad y secuestro de correos electrónicos

Todos tenemos una identidad en Internet, esta la creamos al obtener una cuenta de correo, al acceder a redes sociales como el Facebook o Hi5, mediante el establecimiento de un usuario y *password* en cualquier sitio que sea de nuestro interés.

Esta es nuestra “tarjeta de presentación” cuando navegamos y es tan importante como en cualquier otra actividad que realizamos día a día. Por lo mismo, no estamos exentos de ser suplantados malintencionadamente con diversos fines.

El darle poca importancia a la información que registramos en cualquier sitio de Internet, es tan delicado como el proporcionar información no necesaria por teléfono a un extraño.

En la actualidad tenemos la opción de obtener muchos servicios mediante la red, pagos bancarios, contrataciones, etc; y en la mayoría de los casos establecemos las mismas contraseñas para todos nuestros usuarios en los diversos servicios que obtenemos de Internet, esto es una acción común y lo hacemos más por comodidad y facilidad de no olvidarlos. Por esta misma razón es que debemos extremar precauciones ya que en dado caso de que un “hacker” tenga acceso a la administración de alguna de nuestras cuentas, tendrá acceso al resto de nuestros servicios.

¿Te imaginas a un hacker enviando mensajes de difamación, robando las cuentas de tus amigos y contactos o peor aún extorsionando gente en tu nombre?

Ten cuidado estas cosas están pasando. Microsoft propone cuatro consejos clave que permiten mantener tus credenciales libres:

1. No aceptes contactos desconocidos en tus páginas, cuando alguien que no conozcas te solicite acceso NIEGALO con esto evitarás que personas ajenas a tu círculo de amistades tengan acceso a tus galerías fotográficas, comentarios de tus amistades o datos personales que puedas tener publicados.
2. No abras videos o aplicaciones que no has solicitado o que compartan tus contactos contigo a menos que confíes totalmente en la información que estas recibiendo.
3. El amigo de un amigo que nunca has visto es en realidad un desconocido para ti, por lo que es mejor no correr riesgos, puede no ser quien dice ser.
4. En la medida de lo posible utiliza contraseñas diferentes en cada servicio que tengas en Internet, eso ayuda a reducir riesgos.

Hablando en términos tecnológicos la forma más común en la que se pueden apropiarse de la administración de nuestras cuentas es a través del “phishing” que es una forma de estafa principalmente usada para fraudes bancarios vía Internet.

Phishing es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

De forma más general, el nombre phishing también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un e-mail parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de la ingeniería social.

### ***Una historia real...***

“Acepté un contacto que no conocía y me extorsionó y asustó por teléfono”

Suena lejos de la realidad pero sucedió así: una chica aceptó a un chico que no conocía dentro de sus contactos de Facebook. Él colocó un comentario público al resto de los contactos de ella pidiendo su teléfono pues era “una vieja amiga” con la que no tenía contacto desde hace tiempo y quería sorprenderla, de buena fe varios de los amigos respondieron proporcionando los datos de la chica.

Al cabo de unos días comenzaron las llamadas amenazadoras. No se explicaba como un total desconocido podía tener tanta información sobre ella, las llamadas no pararon hasta que se vio en la necesidad de cambiar su número telefónico, al analizar su situación y comentarla con los amigos salió a relucir el comentario público que había aparecido tiempo atrás de una persona que ella no conocía.

Esta es, hasta cierto punto, una historia afortunada que no pasó a mayores, pero no podemos sustraernos de la realidad en que estas actividades pueden desencadenar delitos graves que dañen la integridad física de una persona.

\*\*\*

Es importante alertarnos y mantenernos actualizados de las políticas de seguridad de nuestra información que todos los sitios de Internet ofrecen, todos los sitios serios y bien intencionados te piden que tu solicites desde que información deseas recibir en tu correo electrónico como la que quieres hacer pública para tus amistades.

Podemos cerrar filas a los navegantes malintencionados de la red todo es cuestión de poner atención y darle “click” a todas las medidas de seguridad que están a nuestro alcance.

Fuentes:

<http://blogs.technet.com/seguridaddigitalmexico/>

[http://www.sitiosargentina.com.ar/notas/Febrero\\_2004/101.htm](http://www.sitiosargentina.com.ar/notas/Febrero_2004/101.htm)

Si has sido víctima de la delincuencia:  
¡NoTeCalles. No + inseguridad!!!

[www.notecalles.org.mx](http://www.notecalles.org.mx) )))

Con el apoyo de

**Microsoft®**

¡lo que no se conoce, no se puede resolver...!

Si te callas te puede pasar a ti  
**ayudanos**  
a prevenir la delincuencia  
la barrera de la inseguridad

entra a  
[www.notecalles.org.mx](http://www.notecalles.org.mx)

no **Te** CALLES