Ajustadores Ltda.

NOTI-AJUSTES

NUMERO 191 AGOSTO DE 2011

LA SEGURIDAD INFORMÁTICA: ¿QUÉ TAN SEGURA ES? (1)

Siempre se ha sostenido que la seguridad de los sistemas de información de los gobiernos, de las empresas –y de las personas- depende en gran medida de la forma como se maneja la seguridad de los denominados Passwords o claves de acceso.

Todos tenemos que lidiar diariamente con un número creciente de claves para acceder a los sistemas de la empresa en la cual trabajamos, de nuestro banco en línea, de las redes sociales o de los sitios de correos por Internet, para solo mencionar algunos de ellos. Cada acceso implica crear y mantener confidencial una o dos claves para ingresar, las cuales se nos recomienda cambiar con regularidad para evitar ser víctimas de alguna persona que pueda conocerla y disponer de nuestra información o de nuestros fondos.

Para muchos de los usuarios de los modernos sistemas de manejo de información, esta circunstancia del manejo de claves se ha convertido en un verdadero dolor de cabeza. No es inusual escuchar que determinadas personas manejan un pequeño cuaderno en el que deben anotar sus numerosas claves, lo que no hace sino añadir mayor carga de angustia a las agendas personales.

También resulta frecuente conocer de casos en los cuales las personas y las empresas pierden altas sumas de dinero, a veces más de las que pueden darse el lujo de perder sin sufrir perjuicios a veces irreparables, debido a la intrusión en sus cuentas de individuos que de alguna manera, sofisticada o no, acceden al secreto de sus claves y proceden a apropiarse de los dineros depositados en cuentas, o a utilizar el buen nombre comercial de su víctima para realizar compras, contratos o algún otro tipo de suplantación.

En algunos casos, los bancos o las entidades que manejan los sistemas de tarjetas de crédito son las víctimas de dichas maniobras y en consecuencia proceden a reembolsar los dineros perdidos o a revertir aunque sea en parte los perjuicios causados a la historia crediticia del afectado. En otros casos, bastante frecuentes, los bancos se rehúsan a responder por las pérdidas y daños debido a que el causante del problema ha sido el propio usuario. Pese a lo indignante que resulta la situación de ver rechazadas nuestras pretensiones de

resarcimiento de daños, a veces es necesario aceptar que hemos sido nosotros mismos los causantes de las pérdidas que nos hayan ocurrido. No se puede culpar a la entidad financiera o crediticia de nuestra propia falta de cuidado en el manejo de las claves y los nombres de usuario.

Algunas recomendaciones prácticas y de fácil aplicación para mejorar la seguridad de nuestro dinero y nuestro historial crediticio contra los ataques, provengan de donde provengan, son las siguientes:

Nombre de usuario: el nombre de usuario (username en Inglés) debe ser lo suficientemente largo e imaginativo como para que no sea obvio ni fácil de adivinar. Nombres como Admin, Miusuario o el nombre de la persona son tan obvios que no resulta para nada difícil suponerlos.

Clave: el password es la pieza fundamental y crítica de la seguridad informática. Se nos ha dicho hasta el cansancio que se debe cambiar a intervalos y que no se debe compartir con nadie. Lo que a veces se olvida advertir es lo que más nos puede dejar en situación de vulnerabilidad. Expliquemos primero de manera sencilla cómo funciona un password.

Al momento de ingresar a un sitio específico, se le pedirá su nombre de usuario y su password. Cuando usted lo digita, un programa de encriptación lo convierte en algo como esto: 929g0m5cck76l3j0o7g3b4. Su nombre de usuario y este nuevo password son guardados en un administrador de seguridad de cuentas (SAM en Inglés). Cada vez que usted digite de nuevo su password normal, éste será encriptado y comparado con el que está almacenado. Si no coinciden, le será comunicado que la contraseña no es correcta. Estos password encriptados son los que persiguen los hackers externos, para compararlos utilizando potentes motores de búsqueda, hasta hallar aquellos que corresponden a los que ellos han obtenido por otros medios.

La otra forma de obtener las contraseñas, la más fácil, consiste en ser descuidado o ingenuo con ellas. En un estudio realizado sobre 200.000 contraseñas obtenidas de manera fraudulenta por hackers, se evidenció que más del 99% de las contraseñas eran simplemente alfanumércias, sin contener siquiera algunos de sus caracteres en mayúsculas o incluyendo un símbolo.

Las contraseñas más empleadas son, en su orden:

123456
12345678
Abc123
12345
111111
mipass

En la siguiente entrega nos referiremos a las maneras más prácticas para crear y mantener contraseñas, de forma segura.

asr@une.net.co