Ajustadores Ltda.

NOTI-AJUSTES

NUMERO 192 SEPTIEMBRE DE 2011

LA SEGURIDAD INFORMÁTICA: ¿QUÉ TAN SEGURA ES? (2)

Si bien no existen precauciones 100% seguras, las principales recomendaciones en cuanto a la seguridad de las contraseñas son las siguientes:

- Nunca use una misma clave o nombre de usuario para acceder a varias cuentas o páginas, ello hace que quien acceda a su clave pueda ingresar a la totalidad de sus sitios;

- No caiga en la tentación de tener dos claves, las cuales siempre rote de tiempo en tiempo. Ello lo convierte en una víctima demasiado predecible;

- No utilice palabras que se encuentren en un diccionario. Los hackers pueden identificarlas usando herramientas del tipo Blunt Force;

- Dedique un tiempo a encontrar una contraseña que no sea obvia ni sencilla de descubrir. En el siguiente cuadro se muestran los tiempos que tarda un hacker, con un equipo modesto, en descifrar su clave:

Número de caracteres	Letras, números y símbolos	Sólo en minúsculas
3	0,86 segundos	0,02 segundos
4	1,36 minutos	0,046 segundos
5	2,15 horas	11,9 segundos
6	8,51 días	5,15 minutos
7	2,21 años	2,23 horas
8	210 años	2,42 días
9	200 siglos	2,07 meses
10	18.990 siglos	4,48 años
11	180 millones de años	116 años
12	Más	Más
13	Mucho más	Mucho más
14	Muchísimo más	Muchísimo más

Fuente: Duo Security Group

Si su contraseña solo tiene letras y números, y ninguna letra en mayúsculas, usted es una víctima fácil de los hackers;

- Considere la implementación de un programa de administración de Contraseñas, el cual encripta y almacena todas sus claves en una base de datos, de tal

manera que usted no tenga que recordar una larga y compleja lista de ellas. Basta con una sola contraseña maestra (esta sí, totalmente secreta), para acceder a sus sitios escogidos. Algunos de los más populares de estos administradores se encuentran en la dirección http//lifehacker.com/5529133/five-best-password-managers;

- Haga suya la rutina de cambiar todas sus claves de manera periódica, especialmente aquellas que correspondan a cuentas financieras;

- Cuando ingrese al banco o entidad financiera, tómese el trabajo de digitar toda la dirección, en lugar de seleccionarla del histórico de páginas visitadas. Es más largo tener que escribir www.mibanco.com, pero mucho más seguro;

- Revise su estatus crediticio, al menos dos veces al año. Verifique si ha sido reportado a las centrales de riesgo, por transacciones que no sean suyas pero que lo involucren de alguna manera;

- Evite caer en los esquemas clásicos de fraude, como el Phishing. Nunca responda a este tipo de correos. Proceda a borrarlos sin abrirlos;

- Limite al mínimo indispensable la información personal que usted suministra en las redes sociales. Son sitios muy vulnerables;

- Verifique los saldos de sus cuentas financieras al menos una vez por semana. Los extractos de tarjeta de crédito al menos una vez al mes;

- Las empresas deberían contar con sistemas que evalúen la seguridad de los passwords utilizados por sus empleados, negándose a activar aquellos que no contengan símbolos, números y algunas letras en mayúsculas;

- Educar, Educar, Educar. Campañas en contra del préstamo de claves entre empleados, en contra de tener libretas de contraseñas al alcance de todos y acerca de la importancia de la seguridad en las claves de acceso, mejorarán la percepción de la importancia de la seguridad.

asr@une.net.co