Diez consejos para escribir contraseñas seguras

"1234". Según revela un estudio, esta es la clave más frecuente que la gran mayoría de usuarios escribimos para proteger nuestros servicios on line, donde guardamos datos privados de gran importancia, e incluso, los números de nuestras cuentas bancarias. Esto significa que cualquier hacker puede entrar en la mayoría de cuentas privadas de plataformas de Internet en pocos segundos.

Por JORDI SABATÉ

11 de julio de 2011

Fuente: eroski consumer

Cuando queremos elaborar un poco más las contraseñas, las basamos, incluso de modo inconsciente, en referencias simbólicas como nuestro cumpleaños, el de nuestros hijos o la fecha de nuestra boda. También así se lo ponemos fácil a los hackers, pues les basta con entrar en sitios como Facebook, ver alguno de estos datos y, a partir de ellos, buscar la combinación de entrada a nuestros servicios. Respecto al nombre de usuario, los profesionales de romper claves saben que casi todos usamos el mismo que tenemos en nuestra dirección de correo electrónico. Conviene, por lo tanto, ser mucho más inteligentes y blindar lo que ahora tenemos casi como un libro abierto.

1. Buscar siempre claves que tengan más de ocho dígitos. Cuantos menos caracteres tenga una clave, más fácil es romperla para un hacker, puesto que el número de combinaciones posibles son menos. Se considera débiles a las combinaciones menores de ocho dígitos, que pueden identificarse con programas generadores de combinaciones aleatorias -llamados robots-, lo que se conoce como "la fuerza bruta".

2. Nunca usar solo números. Aunque pongamos claves de ocho o más dígitos, si usamos solo números, es cuestión de tiempo que un robot encuentre la contraseña y entre en nuestras páginas.

3. Tampoco usar solo letras ni palabras. Las letras se pueden combinar con robots hasta dar con la clave. Respecto a las palabras, siempre tienen una conexión simbólica con nuestro subconsciente, por lo que alguien que nos conozca un poco puede adivinar las claves si piensa en el nombre de nuestra pareja, nuestros hijos o nuestras mascotas.

4. Optar siempre por combinaciones alfanuméricas. Mezclar letras y números es la solución más segura porque se mezclan dos sistemas de clasificación, lo cual amplia mucho las combinaciones. De todos modos, un hacker que tenga algunos datos personales sobre nosotros y mucha psicología puede adivinar las claves si no nos hemos esmerado en confeccionarlas. Debemos ser conscientes de que, de modo automático, siempre buscamos combinaciones fáciles de recordar y relacionadas con personas y fechas importantes. Por lo tanto, lo mejor después de escribir la contraseña es revisar que no contenga señales personales.

5. Intercalar signos de teclado. Un truco que nos permitirá usar letras y números relacionados con nuestra vida sin peligro es intercalar símbolos como "#", "$", "&" o "%" entre los caracteres de la contraseña. La presencia de estos caracteres es mucho más difícil de descubrir para hackers y robots.

6. Lo mejor son las claves aleatorias. Si podemos usar un programa generador de claves aleatorias, estaremos mucho mejor protegidos. La página Clave Segura ofrece de manera gratuita un generador de claves en el que se puede escoger tanto la longitud de la contraseña como la cantidad de caracteres alfanuméricos que usamos. Otros servicios como Passw ordmeter miden el nivel de seguridad de las contraseñas que confeccionamos.

7. No utilizar la misma contraseña para todo. Parece una obviedad, pero es lo que hacemos la mayoría de los usuarios. Hay que tener una contraseña distinta para cada servicio. También es recomendable cambiar las contraseñas cada cierto tiempo.

8. Guardar las claves en un documento de texto. Como las claves seguras son muy difíciles, por no decir imposibles, de recordar, lo lógico es guardarlas escritas en un documento de texto, que utilizaremos para almacenar las contraseñas de todos nuestros servicios. Cada vez que debamos entrar a un servicio, tendremos que recurrir a este documento. Puede que sea pesado, pero es más seguro.

9. Guardar el documento en un lugar seguro. Hay varias opciones para guardar el documento con nuestras claves. La primera es usar una memoria USB separada físicamente del ordenador y que solo enchufemos cuando queramos abrir el documento con nuestras claves. Debemos ser conscientes de que podemos tener el ordenador monitorizado por algún softw are malicioso -ocurre con mucha más frecuencia de la que creemos- o que alguien puede acceder a través de la conexión w ifi si esta no es lo bastante segura. La segunda alternativa es guardar el documento en una copia de seguridad en un servidor de la red, con protocolos de cifrado de 128 bits o más. Podemos guardarlo en plataformas diseñadas para tales usos, como Clipperz. Bastará con abrir este servicio y acceder al documento. Eso sí: la contraseña de acceso a Clipperz tiene que ser altamente compleja, deberemos tenerla escrita en una libreta, guardarla en un cajón y saber que si la perdemos también perderemos el resto de contraseñas.

10. Cerrar la sesión de los servicios a diario. Cuando apaguemos el ordenador por la noche o al salir de casa, la mejor opción es salir de todos los servicios de uso habitual, ya sean el correo electrónico, las distintas redes sociales donde participemos o las plataformas donde guardamos documentos para sincronizarlos, etc. Si alguien encendiera nuestro ordenador y no los hubiéramos cerrado, podría acceder fácilmente a tales servicios, ya que el navegador guarda las contraseñas si no le indicamos lo contrario. Por lo tanto, hay que indicar en el apartado de "Seguridad" de nuestro navegador que no recuerde ninguna contraseña. Al volver a usar el ordenador habrá que introducir todas las claves, pero evitaremos disgustos.