La fuga de datos por culpa de contraseñas poco seguras alimenta un lucrativo mercado negro de información Contraseñas.

[29/01/2014]

Expertos de la UOC recomiendan seguir algunos principios básicos a la hora de construir la contraseña para diferentes servicios web y evitar ser víctimas de hackers malintencionados. Los expertos en seguridad informática advierten sobre las malas prácticas en que a menudo caen los usuarios al crear contraseñas poco seguras y los problemas que esto puede ocasionar a la hora de preservar la seguridad de sus sistemas y la información personal. En muchos casos, esa información puede acabar en mercados negros de hackers que ganan mucho dinero con los datos o con redes de ordenadores zombis.

Por Joan Antoni Guerrero

Las 10 recomendaciones de expertos para una contraseña segura

1. Las contraseñas deben tener una longitud de entre ocho y diez caracteres como mínimo.
2. Se debe combinar el uso de mayúsculas y minúsculas, incluir algún número y un símbolo.
3. Se recomienda no repetir contraseñas para diferentes servicios o, en todo caso, tener variantes con pequeños cambios.
4. No se deben utilizar como contraseña palabras de diccionario porque hacen más vulnerable el sistema.
5. Evitar el uso de contraseñas que hagan referencia a datos fácilmente deducibles como son las fechas de cumpleaños.
6. Se puede construir una contraseña a partir de las primeras letras de las palabras que componen el título de una canción favorita.
7. Si se escriben las contraseñas en un papel hay que ser prudente y no dejarlo en un lugar visible ni cerca del ordenador.
8. Se pueden guardar las contraseñas para recordar en un documento de Word que esté cifrado o también en servicios online que ofrezcan la posibilidad de cifrar el contenido.
9. A las preguntas planteadas en el proceso de recuperación de contraseñas se debe evitar dar información personal conocida por muchas personas.
10. Hay que evitar el uso de contramedidas forzadas y ampliamente utilizadas como cambiar algunas letras por números similares. El hecho de utilizar simbología similar hace las contraseñas más vulnerables.

La opinión de los expertos

Los profesores de la UOC Robert Clarisó, director del máster universitario de Ingeniería informática, y Helena Rifà, directora del máster interuniversitario de Seguridad TIC, coinciden en que lo más importante es que las claves «sean difíciles de adivinar y fáciles de recordar». Un objetivo que no siempre resulta sencillo. En primer lugar, hay que evitar información deducible, como son las fechas de aniversario o caer en el error de usar el mismo nombre de usuario, un hecho muy habitual que hace muy frágil la protección del sistema.

No usar palabras de diccionario

Pese a que resulte en un principio complicado, los expertos están de acuerdo en destacar que habría que utilizar siempre combinaciones de letras y números, mayúsculas y minúsculas, y emplear también algún símbolo especial. De esta manera se evita elegir una palabra simple que hace mucho más vulnerable el sistema.

Helena Rifà considera no usar palabras de diccionario como regla básica, porque en caso contrario se facilitaría mucho el trabajo de los hackers si se hace un ataque de diccionario. Asimismo, la profesora de la UOC recomienda tener diferentes contraseñas, o con ligeros cambios, para los diferentes servicios en los que se está registrado y, además, remarca, es necesario que todos tengan una longitud mínima entre ocho y diez caracteres.

El reto de recordar contraseñas

Ahora bien, el hecho de que por razones de seguridad se tengan que generar tantas contraseñas diferentes también le hace difícil al usuario recordarlas, cuando en general se trata de claves que queremos tener presentes fácilmente para acceder rápido al web. Tanto Clarisó como Rifà piensan que las contraseñas se pueden apuntar en algún papel pero, en este caso, advierten que hay que ser prudente. Se pueden escribir en un papel, pero este se debe mantener lejos del ordenador y escondido.

Los usuarios que tienen un gran volumen de contraseñas pueden guardarlas en un documento cifrado en el ordenador, o bien, también cifradas, en servicios en línea como puede ser el Dropbox o en programas comerciales.

Protegerse de ataques

Una buena contraseña nos protege de ataques que son más comunes de lo que podemos pensar. Todo el que tenga un servidor accesible desde el exterior se puede encontrar con algún caso de ataque. En una institución como la UOC, por ejemplo, según explica Clarisó, «cada día hay decenas de miles de intentos de conexión malintencionados» al sistema. «A veces las contraseñas de los usuarios son fáciles de adivinar y si alguien descubre tu contraseña puede hacer auténticas barrabasadas», comenta. Por ejemplo, se puede acceder a la información personal del usuario, enviar correo basura o bien hacer ataques contra otras máquinas. «Normalmente estos ataques –explica Clarisó– no se hacen directamente desde las máquinas del atacante sino por medio de otros usuarios, de manera que es más complicado identificar su origen».

Los expertos consideran que a menudo los usuarios no son conscientes de la importancia que tienen los datos que facilitan. Señalan que detrás de este fenómeno se mueve un negocio importante alimentado por los datos obtenidos fraudulentamente. Cuando se trata de robar contraseñas, «originalmente había quien lo hacía como reto intelectual, pero hoy en día ya hay auténticos "profesionales" que se ganan la vida de esta manera», comenta Clarisó. Existe un mercado negro detrás de tal fenómeno y páginas web donde los hackers ponen a la venta información, como por ejemplo números de tarjetas de crédito, entre otros datos de valor comercial.

Webs «gánster»

Del mismo modo, algunos ataques informáticos consiguen tener una red de ordenadores infectados (con software malicioso y de troyanos, la mayoría procedentes de China, Rusia o los Estados Unidos) y algunos hackers alquilan estas redes a terceros que buscan hacer ataques en páginas web para que dejen de funcionar por un tiempo, por ejemplo. «Todo lo que pasa en la vida real también se da en la informática», advierte Clarisó. Tanto es así que incluso se pueden encontrar «webs gánster» que se dedican a «la extorsión» usando información obtenida fraudulentamente.