A pesar de que existen claves predecibles y otras difíciles de adivinar, ninguna es 100% segura, por lo que se recomienda ser muy cuidadoso con la información que se entrega en internet y tomar algunas consideraciones a la hora de crearlas.

RNB > GSD 2.0 > 06.11.10

Técnicamente hablando, una clave es una secuencia secreta de letras, números y símbolos de puntuación, y debido a su carácter de "secreta", debería ser conocida sólo por su dueño.

"Las claves se usan para demostrar que 'yo soy quien digo ser', pues se supone que sólo el dueño las conoce. Por ejemplo, al visitar mi banco por internet, yo le digo 'Hola, soy Juan'. El banco entonces me solicita mi clave para compararla con la guardada de Juan. Si son iguales, me deja entrar", explica Alejandro Hevia, académico del Departamento de Ciencias de la Computación de la Universidad de Chile.

A pesar de lo íntima que puede ser una clave, no existe ninguna que sea 100% segura, puesto que todas tienen una debilidad inevitable y es que, en principio, toda clave puede ser adivinada, ya sea que esto resulte fácil o difícil. "La dificultad de adivinarlas depende de dos cosas: el largo de la clave (mientras más larga mejor) y si la clave es 'fácil' o no (una clave es fácil si es una palabra conocida o simplemente deducible a partir de información conocida de su dueño). Si mi clave es larga (ocho letras o más) y contiene letras y símbolos que no signifiquen nada concreto, entonces adivinarla será difícil y será segura", especifica el profesor.

Si, por ejemplo, contiene menos de ocho letras será fácil de adivinar, ya que a pesar de que el número de combinaciones de claves de cinco o seis letras parece demasiado, existen computadores que pueden intentar todas las combinaciones posibles en sólo cosa de minutos u horas. En tanto, a partir de ocho caracteres se hace más difícil para estas máquinas y posibles "adivinadores".

Pero tampoco basta con que sea larga, sino que, como dice Alejandro Hevia, ésta debe ser "impredecible". ¿Qué significa esto? Que no debe contener ninguna palabra, concepto o número que se relacione con su dueño. Por el contrario, es mejor que no signifique nada. "Por ejemplo, si la clave de Juan es 'juan', entonces es predecible (¡mala!). Lo mismo, la clave 'campana' es mas predecible que 'xb7ui*2a'. Claramente, esta última es más segura, pues no es fácil de deducir a partir de datos de Juan, como su nombre, dirección, nombre de la polola, etc.", recomienda.

Entonces, ¿cuáles serían las claves "típicas"? Hay muchas: '1234', 'abcd', 'soyyo', 'abc123' o 'superman' son sólo algunos ejemplos de las fácilmente adivinables. Tan obvias son que forman parte de los diccionarios de claves que están disponibles en internet, donde se reúnen las palabras comunes de diccionario y otras típicas usadas en claves. Por ende, "mi clave será más segura si no está en esos diccionarios; probablemente una como 'xb7ui*2ª' no lo estará", señala el especialista.

Algunas recomendaciones

En resumen, para crear una clave segura, ésta debe cumplir con una serie de requisitos: por una parte, debe ser suficientemente larga (ocho letras o más) e impredecible (no debe "significar" nada), y por la otra, debe mezclar letras, números y símbolos de manera arbitraria. Por ejemplo, "ax*2,3Bo" es una clave más segura que "juan1234".

"Pero ojo, hoy los criminales en internet no sólo intentan adivinar las claves usando diccionarios, sino que también usan información pública de su potencial víctima para apurar el proceso. Por ejemplo, un criminal mirando Facebook o Twitter puede saber dónde vive Juan, el nombre de su perro, polola, qué bandas de música le gustan, etc. Y con eso, puede intentar deducir su clave, usando combinaciones de estos datos (nombres, fechas de cumpleaños, por ejemplo) y claves típicas de diccionario de claves. Por eso, nunca se debe usar como clave una fecha de cumpleaños, nombre de polola/pololo o familiar o de la mascota, o la numeración de la casa o el teléfono. Todas esas son fácilmente adivinables", precisa Alejandro Hevia.

El profesor también asegura que una clave formada por letras "al azar" y sin orden aparente es segura, el problema está en que ésta debe ser recordable también; de lo contrario, la olvidaremos inmediatamente y no servirá para nada.

Por ello, "una buena recomendación para producir una clave segura es elegir una frase preferida o letra de una canción que le guste y crearla escogiendo las primeras letras de cada palabra y agregarle números o símbolos. Por ejemplo, si tomo la frase 'Puro, Chile, es tu cielo azulado' y saco las primeras letras, pero dejo las comas, tengo 'P,C,etca'. Para recordar la clave sólo tengo que acordarme de la frase, lo cual lo hace mucho más fácil", puntualiza.

Tener ojo con…

Alejandro Hevia da una serie de consejos sobre cómo comportarse en relación con las claves.

- Lo primero es usar una clave larga y difícil de adivinar.
- Luego, no se debe usar una misma clave para lugares o servicios distintos. Por ejemplo, no usar la misma clave para el banco que para Facebook.
- Asimismo, las claves no deben compartirse, aún con un amigo, pues se corre el riesgo que mi amigo la revele por accidente sin yo saberlo.

Sin embargo, "aún haciendo todo lo anterior una clave puede ser 'robable' si uno no es cuidadoso", asegura el académico. Por ello, "jamás se debe hacer 'click' en enlaces ('links') recibidos por email, pues éstos pueden ser parte de una estafa llamada 'phishing'", sostiene.

Y agrega: "Un phishing consiste en un correo fraudulento que aparenta venir de mi banco, o de un amigo, o de Facebook, Gmail o alguna institución en que confío y me pide que 'urgentemente' vaya a visitar un sitio web. Este sitio web aparenta ser 'oficial', pero, en realidad, es falso y malicioso, y su propósito es robarme mis claves. También, si no tengo actualizado mi computador (sistema operativo y antivirus), entonces un virus o programa espía puede robarme mis claves, ¡Aún si ellas son largas y difíciles de adivinar!".

Cuidado con almacenarlas

Cada vez que se habla sobre la creación de claves, se menciona a algunos sitios web que se ofrecen como especies de bancos de las claves de los usuarios. Sin embargo, Alejandro Hevia aconseja no confiar en ellos, puesto que si bien hay algunos que son honestos, "lamentablemente hay muchos otros que no, que son fraudulentos y sólo quieren robarme mis claves".

En general, se recomienda usar los servicios de navegadores como “Firefox”, por ejemplo, el cual tiene una opción para guardar contraseñas para todos los sitios que visito en forma segura, protegidas por una contraseña maestra.

“Si se usa esto, optar por una contraseña maestra larga y difícil de adivinar, pero recordable. Aun así, siempre las contraseñas deben ser largas e impredecibles; lo bueno es que sistemas como el de Firefox me ayudará a recordarlas”, señala el académico.

Programa de Alfabetización Digital y Mediática 2.0 PADM 2.0 – GSD 2.0 – www.serdigital.cl

Compartir este Artículo

Etiquetas: Clave, contraseña, login, password, seguridad, Usuario

Deja un comentario

Nombre (requerido)

E-mail (no se publicará) (requerido)

Sitio Web

Enviar comentario

Diseñado por El Rey del Diseño | Consultora Divergente