Passwords (contraseñas)

Uno de los elementos de la seguridad informática que se utilizan con mayor frecuencia en los sistemas de cómputo es el llamado *password* o contraseña. De hecho, cuando accedemos al correo electrónico, al sistema operativo de nuestra computadora o algún sistema del Instituto, como la Base de Datos Académica (SDBAII), el Sistema de Control de Estudiantes (SICOE) o quizá el sistema de reservaciones, aparte de requerir el nombre de usuario, se nos solicita la contraseña. Pero como es bien sabido, si alguno de estos dos elementos no es proporcionado o se teclea incorrectamente, simplemente se niega el acceso.

Scarfone (2009) define la contraseña como una secuencia de caracteres secretos (combinación de letras, dígitos o signos) que el usuario utiliza para autentificar su identidad en un sistema informático. El término "autentificar" o "autenticar" es el proceso de validación que se lleva a cabo para garantizar el acceso a los recursos de dicho sistema, y que involucra algo que el usuario "conoce" (la misma contraseña), el usuario "es" (huella digital, geometría de la mano, reconocimiento facial) o el usuario "posee" (tarjeta de acceso). Sin embargo, muchas veces el usuario no vislumbra la importancia que tiene lo secreto de una contraseña y, por comodidad, desconocimiento o descuido, la evidencia lo expone ante personas no autorizadas para ingresar a los sistemas, y así vulnera la seguridad y provoca problemas potencialmente peligrosos no solo para el usuario mismo, sino para toda la organización. Ya desde 1985 el National Institute of Standards and Technology (NIST) publicó el estándar Password Usage, donde cuestiona la efectividad de las contraseñas, fundamentalmente porque los usuarios la olvidaban fácilmente o porque se la proporcionaban a otras personas sin el menor reparo. Esto lleva a pensar que gran parte del trabajo debe centrarse en hacer conciencia de la importancia que tiene la contraseña para un usuario. Pero no es tan sencillo; por ejemplo, qué posibilidades hay de recordar una contraseña como la siguiente: Mo9YT-5FB1aab@54. Aunque por la longitud y la combinación de caracteres se consideraría altamente efectiva (se recomienda que la longitud sea de al menos 8 caracteres y se combinen letras, dígitos y signos), lo más seguro es que por su complejidad, el usuario la escribirá en un papel y lo guardará en un lugar de fácil acceso (en el cajón, debajo del teclado o incluso en la misma pantalla de la computadora); entonces, la efectividad y la seguridad se vulneran. Aún más, la seguridad se compromete severamente cuando existen ciertos usuarios malintencionados que buscan obtener esas claves, pues su acceso representará la obtención de información que podría ser altamente valiosa y rentable para sí mismos o para intereses ajenos.

Normalmente, al crear una contraseña es común emplear palabras fáciles de recordar, como nombres de familiares, deportes, RFC, placas del automóvil, fechas de cumpleaños o nombres de mascotas, lo que aumenta la seguridad si se escriben al revés. Sin embargo, los usuarios expertos y malintencionados (generalmente llamados "*hackers* de sombrero negro" o "*crackers*") tienen métodos, como el denominado "fuerza bruta", que permite detectar contraseñas mediante el intento continuo de múltiples combinaciones de letras y números. Es por ello que a lo largo del tiempo se han desarrollado diversas técnicas que permiten al usuario crear contraseñas que sean de fácil memorización y altamente seguras.

Algunas técnicas son las siguientes:

Texto modificado. La primera de ellas es el empleo de nombres sencillos pero sustituyendo algunas letras por números o caracteres especiales. Por ejemplo, para convertir la palabra "instituto" en una contraseña más segura, se sustituyen los caracteres "i" por el número "1" (1nst1tuto), se modifica la letra "s" por el número "5" (1n5t1tuto), después se cambia la letra "o" por el "0" (1n5t1tut0) y las letras "n" y "u" se invierten (1u5t1tnt0). Si además la contraseña se refuerza al agregar un número de la suerte, por ejemplo el 9 y 6, y al colocarlos al principio y al final (91u5t1t-nt06), en posiciones pares (19u5t61tnt0) o impares (1u95t1tn6t0), se obtendrá una contraseña segura y fácil de memorizar. Es obvio que estas técnicas son conocidas por los *hackers*, pero si se sustituyen algunas letras y otras no, la complejidad será mayor y la posibilidad de adivinarla será mínima.

Mnemónicos. Otra técnica para crear contraseñas seguras es recordar una frase, como un poema, la letra de alguna canción o alguna frase célebre, preferentemente no muy conocida; por ejemplo: "Puedo escribir los versos más tristes esta noche", y tomar la primera letra de cada palabra (Pelvmten), o la primera y última letras (Poerlsvsmstseane) y aplicar la técnica anterior, sustituyendo caracteres por números (POer15v5m5t5eane), y se obtiene como resultado una contraseña altamente poderosa de 16 caracteres de longitud.

Combinación de palabras modificadas. Consiste en seleccionar dos o tres palabras inconexas y sustituir los caracteres por números o símbolos. Esta técnica es muy parecida al texto modificado, con la diferencia de que utiliza dos o más palabras sin relación alguna. Por ejemplo, las palabras "corre" y "pelota" se utilizarían como *password* así: c0rrEPe10t@; o las palabras "agua" y "computadora" quedarían como @gu@c0mput@ d0r@.

Estas técnicas, aunque útiles, también podrían representar ciertas dificultades para el usuario al intentar recordarlas. Una alternativa es emplear una sola palabra fácil de recordar y modificarla creando derivaciones, como agregar una serie de números o símbolos en distintas posiciones. Esto es útil sobre todo cuando se emplea la misma contraseña en distintos sistemas. Por ejemplo, la palabra "Eficiencia" se escribiría como contraseña base "Ef1c1enc1@" y sus respectivas derivaciones: al agregar el número 47 "47Ef1c1enc1@", el * "*Ef1c1enc1@47" o el número 51 "51Ef1c1enc1@". Claro está que las reglas deberán almacenarse para que no se olviden, pero la contraseña base queda en la mente del usuario.

Finalmente, e independientemente de aplicar las técnicas anteriores que permiten al usuario crear contraseñas más seguras, es conveniente tomar en cuenta las siguientes recomendaciones:

1. Nunca escribir una contraseña, en lugares muy evidentes y de fácil acceso (Post-it, agendas, cuadernos, etc.)
2. No darla a conocer. Recordar que el uso es personal y que si bien el propietario puede ser cuidadoso y seguir estas reglas, a quien se le otorga quizá no.
3. Cambiarla frecuentemente. Es muy saludable esta recomendación, ya que su renovación minimiza la probabilidad de caer en manos de usuarios indeseables.
4. Utilizar palabras extensas o frases con más de cuatro palabras de tal manera que se formen contraseñas de al menos ocho caracteres. Esto disminuye el riesgo de ser detectada por fuerza bruta.
5. Al crearla, siempre combinar letras, números y símbolos.
6. Nunca reutilizar contraseñas.
7. Evitar que haya gente viendo el teclado al ingresarla a un sistema.

Es importante recordar que las contraseñas son las puertas de acceso a información o recursos, las cuales podrían ser altamente sensibles para la organización y para el mismo usuario y que, al no concientizar sobre su importancia, su seguridad se verá gravemente comprometida.