CLAVES DE ACCESO

Las claves de acceso son contraseñas que un usuario emplea para acceder a un servicio, sistema o programa. Generalmente la clave de acceso está asociada a un nombre de usuario.

¿CÓMO CREAR CLAVES SEGURAS?

1. **Nada de información personal**. Incluso un hacker novato puede dar con nuestro nombre completo, el nombre de nuestro esposo o hijos, mascotas o equipo de fútbol favorito. Nunca se debe escoger una contraseña que tenga algo que ver con nuestra personalidad.

2. **Palabras inventadas**. No solo no debemos utilizar el nombre de nuestra mascota o el nuestro propio, sino que tampoco deberíamos utilizar cualquier palabra actual que pueda encontrarse en un diccionario. Este tipo de contraseñas pueden ser fácilmente rompibles por un software preparado para robarlas.

3. **Mezcla de caracteres**. Las contraseñas suelen reconocer todo tipo de caracteres, por lo que se debe emplear mayúsculas y minúsculas para hacerlas más complicadas. Para hacerlas aún más complejas, no se debe elegir como mayúscula la primera letra (deberíamos optar, por ejemplo, por “coNtraSeña” en lugar de “Contraseña”). Mejor aún, debemos intercalar algunos números y caracteres especiales para sustituir algunas letras (“c0NtraSeñ@”).

4. **Emplee acrónimos**. Algunas utilidades para dar con las contraseñas pueden ser lo suficientemente inteligentes como para sustituir algunas letras por caracteres en palabras corrientes. Así, dar con “c0ntraseñ@” puede llevar más tiempo que hackear “contraseña”, pero sigue siendo relativamente fácil dar con ella porque, con caracteres especiales o no, la contraseña sigue siendo tan obvia como “contraseña”. Por eso, la recomendación en este caso es, en lugar de escoger la frase favorita de una canción o película, convertirla en un acrónimo. Por ejemplo, en la película Algunos hombres buenos, Jack Nicholson dice “¿Quiere la verdad? ¡No puede manejarla!”, el acrónimo (y la contraseña) seria “¿Qlv?¡Npm!”, combinando mayúsculas y minúsculas, así como caracteres especiales. Es una palabra que no aparece en los diccionarios, pero puede ser fácil para recordar.

5. **Use una herramienta**. La principal razón por la que los usuarios escogen contraseñas que son fáciles de romper es que, cuando tienen que elegir una, siempre escogen la que resulte sencilla de recordar. Evidentemente, es mucho más fácil acordarse del nombre del perro o de pulsar teclas tal y como

aparecen en el teclado (1234567 que una del tipo “a5$jgFD118@Kle45@”. Pero, ¿cuál es más segura? Existen herramientas de gestión de contraseñas que permiten guardar complejas contraseñas, aunque también conllevan su riesgo puesto que, si se accede a este software, se tendrá acceso a todas las contraseñas del usuario. Sin embargo, estas aplicaciones ayudan al usuario a utilizar contraseñas más robustas sin necesidad de recordarlas todas.

NOTA: Si presenta dificultades con el procedimiento descrito en este documento, por favor repórtelo a través de la plataforma **SUSI.**