



Carlos Muller
HARD KEY / SITEPRO

¿Qué hacer con nuestras Passwords?



En nuestro “mundo informatizado” cualquiera que utilice una computadora debe lidiar con innumerables sitios Web donde debe autenticarse mediante un nombre de usuario y una password. En general manejamos de 12 a 17 passwords entre cuentas de correo, banca electrónica, redes sociales, sitios de

compra-venta on-line, chat, sitios para revelado de fotos, contraseñas de planillas, Web de supermercados, etc.

Hay que sumarle a esto el hecho de que por razones de seguridad en muchos sitios nos obligan a cambiar la password periódicamente, con lo cual en determinado momento olvidamos

cuál utilizamos en cada caso y terminamos con el acceso bloqueado. Existen numerosas pautas y consejos para evitar que los “hackers” se apoderen de nuestras claves de acceso, pero “prolijamente” los ignoramos por ser muy complejas de implementar o directamente “incumplibles”. Nos piden que usemos passwords o “palabras claves” que no tengan ninguna referencia a datos personales,

Con esto haremos más difícil el hecho de que un “hacker” pueda acceder a nuestras cuentas en sitios Web o aplicaciones al descubrir las passwords que utilizamos por medio de “ingeniería social” (averiguando datos personales para con ellos deducir nuestras contraseñas) o por “fuerza bruta”, es decir probando con todas las combinaciones posibles hasta encontrar la correcta para acceder y lograr apro-



que sean “passwords fuertes” es decir largas, de 15 o más caracteres, que tengan mayúsculas, minúsculas, números, caracteres especiales como @ \$ % # intercalados entre sí, tampoco deberían utilizarse palabras legibles en ningún idioma, además nos sugieren que usemos una clave distinta para cada cuenta y que la cambiemos frecuentemente.

piarse de nuestra “identidad”, datos, información y hasta el dinero de nuestras cuentas bancarias. Sin embargo, cumpliendo con todos estos recaudos de seguridad, es muy probable que nosotros tampoco podamos acceder a nuestras cuentas, porque terminaremos olvidando qué passwords usamos en cada sitio o bloqueando el acceso por equivocarnos

al tipear las “engorrosas contraseñas” que engendramos para protegernos de los “hackers”, y deberemos realizar tediosos trámites para recuperar nuestro propio acceso.

Al final terminamos anotando nuestras passwords en una agenda, en papelititos sueltos que van a parar a un cajón del escritorio, en un sticker pegado al monitor o utilizamos en forma reiterada para todas las aplicaciones passwords “obvias” o fáciles de adivinar saboteando nosotros mismos la seguridad que se pretende implementar con estos mecanismos de “usuario y password”.

Incluso, para complicar más las cosas, algunos bancos además de pedir “passwords fuertes” están utilizando unas “TARJETAS DE COORDENADAS”, una especie de matriz con filas y columnas y números en cada celdas, que se piden al azar para hacer transacciones por Internet, obligándonos a tener esta tarjeta a mano con el riesgo que alguien la pueda copiar fácilmente, o robárnosla con la contraseña escrita justamente en esa tarjeta para tenerla a mano.

Existen soluciones estándares o de uso frecuente, como permitir que Windows recuerde nuestras contraseñas o programas para almacenar todas nuestras claves en un archivo que se graba en el disco de nuestra PC.

Esto parece ser mejor que dejar todas las contraseñas en un sticker pegadas en el monitor, pero puede volverse nuestra en contra ya que los “hackers” conocen estas soluciones y pueden acceder a ellas y “hurtarlas”

¡todas juntas!

Por suerte existen otras soluciones mejores que permiten almacenar y transportar en forma segura todas nuestras claves sin tener que dejarlas “expuestas a ataques” en el disco de nuestra PC.

Una de estas soluciones es un desarrollo argentino denominado Administrador de Passwords HARDkey MIO (www.HARDkeyMIO.com) que valiéndose de un dispositivo USB especial (llave electrónica con memoria cifrada) permite proteger y transportar en forma segura todas nuestras contraseñas. Las passwords nunca se graban en el disco de la computadora por lo cual no pueden ser “capturadas” fácilmente por los “hackers”.

El Administrador de Passwords HARDkey MIO es un producto pensado para solucionar el manejo de todas nuestras contraseñas de sitios Web, aplicaciones y archivos Office.

