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 que password utilizamos en cada caso y terminamos con el acceso bloqueado.

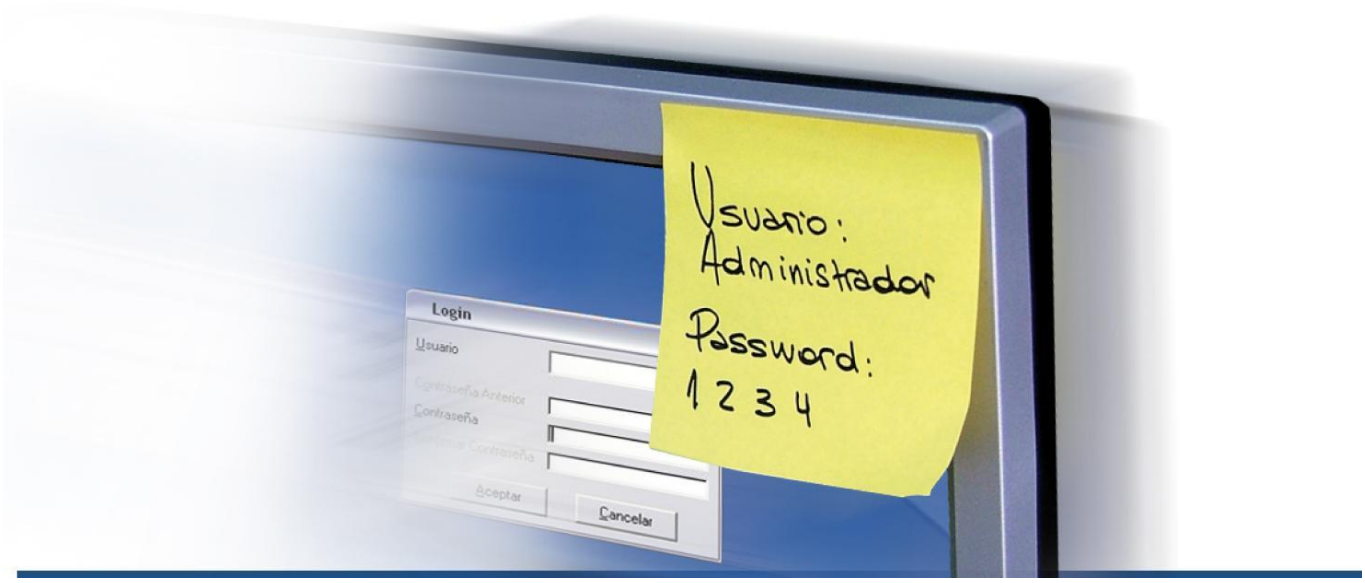
Existen numerosas pautas y consejos para evitar que los “hackers” se apoderen de nuestras passwords, pero “prolijamente” los ignoramos por ser muy complejas de implementar o directamente “incumplibles”.

Nos piden que usemos passwords o “palabras claves” que no tengan ninguna referencia a datos personales, 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.

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 apropiarse 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 que passwords usamos en cada sitio, o bloqueando el acceso al 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 papelitos sueltos que van a parar a un cajón del escritorio, en un sticker pegado al monitor, o utilizamos en forma reiterada para todos las aplicaciones passwords "obvias" o fáciles de adivinar, saboteando nosotros mismos la seguridad que se pretende implementar con estos mecanismos de "usuario y password" para proteger nuestra información.



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 celadas, 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 contraseñas 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 en contra nuestra, ya que los “hackers” conocen estas soluciones y pueden llegar fácilmente a donde se almacenan nuestras contraseñas, y “hurtarlas” todas juntas !!!

Por suerte existen otras soluciones mejores que permiten almacenar y transportar en forma segura todas nuestras passwords 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. Además permite almacenar y transportar en forma segura datos personales, de cuentas bancarias, y las "Tarjetas de Coordenadas" de los bancos. Se pueden almacenar hasta 100 cuentas con diversos datos.

Toda la información almacenada en el **ADMINISTRADOR DE PASSWORDS HARDkey MIO**, está cifrada y protegida con un PIN o clave de acceso que el usuario puede definir y cambiar tantas veces como quiera.

Esta solución tiene un interesante mecanismo para "automatizar" el acceso a sitios web, sólo la primera vez se deben ingresar el usuario y password (hay un tercer dato opcional por si es necesario) que se utilizarán para cada sitio y se deben "asociar" estos datos con los lugares en la página donde se deben completar. La próxima vez que ingresemos a un sitio "automatizado" nos pedirá que ingresemos el PIN de acceso y completará automáticamente los datos solicitados para el LOGIN.

Se dispone también de un "Asistente para cambio de passwords" que permite cambiar las passwords en los sitios y almacenarlas simultáneamente dentro de la memoria del dispositivo USB.

Además ofrece una modalidad que permite mediante unos atajos de teclado, "arrastrar" y "pegar" en los lugares que lo soliciten passwords y otros datos como números de cuentas bancarias, CBU, tarjetas de crédito, etc.

De esta forma se facilita la utilización de "passwords fuertes" y distintas para cada aplicación, al no tener que recordarlas ni tipearlas nunca, pues sólo se deberá recordar un PIN para acceder a la memoria de su llave, y allí tendrá todas las passwords y datos confidenciales que necesite para moverse en este "mundo cibernético" que exige utilizar usuario y password para todo lo que hacemos diariamente.

HARDkey MIO ADMINISTRADOR DE PASSWORDS:

- Almacene y transporte sus password de dentro de una llave HARDkey MIO .
- Utilice password "fuertes" difíciles de adivinar, pues no tendrá que tipearlas ni recordarlas.
- Evite ser engañado con "falsos sitios de Home Banking" accediendo solo a los que tiene almacenados y "automatizado" con su llave HARDkey MIO.
- Guarde y proteja los datos de su "Tarjeta de Coordenadas"
- Coloque passwords fuertes en sus archivos Office y adminístrelas en forma segura.
- Tenga siempre a mano números de cuentas bancarias, tarjetas de crédito, números impositivos, claves de accesos, y datos personales suyos y de familiares.
- Arrastre y péquelos fácilmente por medio "atajos de teclado" cuando se los pidan.
- Realice una copia de seguridad de todas sus passwords en forma fácil y segura.

Proteja y transporte todas sus passwords y datos sensibles con el **ADMINISTRADOR DE PASSWORDS HARDkey MIO**