¿Usas siempre la misma contraseña? Conoce los peligros y cómo solucionarlo

03/04/2015

Hoy en día nadie está a salvo de que un ciberdelincuente averigüe algunas de tus contraseñas.

Por lo general el objetivo de estos delincuentes son la extracción y venta de tu información personal almacenada en los servicios que sueles usar en Web (Facebook, Correo electrónico, Banco...) y para ello es necesario averiguar tus contraseñas de diferentes formas. Las formas, mejor las dejamos para una futura entrada, en esta vamos a centrarnos en la importancia, primero, del **porqué no debemos de repetir las contraseñas** y segundo, de que opciones tenemos disponibles para no tener que recordar cada una de ellas. ¿Te imaginas que en vez de llevar un manojo de llaves llevaras una sola que abriera todas las puertas? La de tu casa, el coche, el trastero, etcétera... ¡Qué comodidad! Sí, sería muy cómodo, pero con que alguien malintencionado te quitara esa única llave **tendría acceso a todos tus bienes más preciados**.

Y esto es lo mismo que pasa con tus contraseñas en la red, si siempre utilizas la misma contraseña en todos los lugares, alguien que la descubra podría dedicarse a intentar acceder en diferentes sitios, y lo peor de todo no es que el ciberdelincuente lo vaya a intentar por el mismo, sino que un programa informático, que **puede entrar en miles de páginas** a la vez será quien lo intente y recopile todos los datos más interesantes...

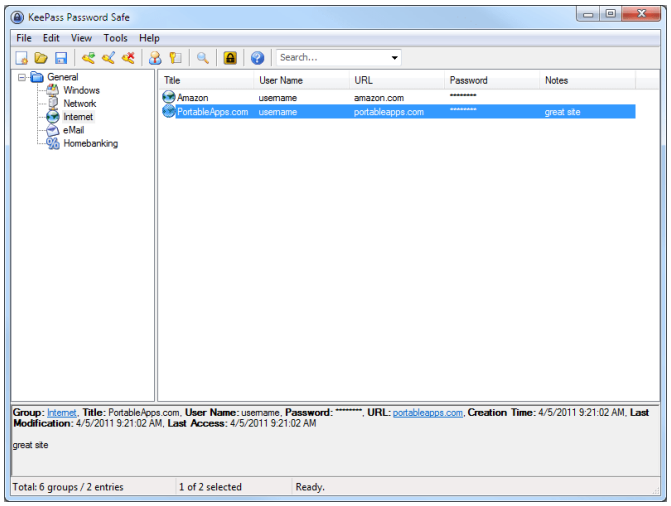
Parece evidente que no es muy seguro utilizar la misma contraseña en todos los sitios, pero resulta complicado recordar una nueva clave para cada sitio donde nos

registramos, por tanto, **¿existe alguna solución?**

Sí, existe, y son los llamados **gestores de contraseñas**. Estos programas constan de un software donde puedes guardar cada clave asociada a un nombre de usuario y el sitio Web donde la has usado. El programa tiene una base de datos encriptada y para acceder a él sí que necesitarás memorizar una contraseña (una única clave maestra) que te pedirá cada vez que lo abras aunque también lo puedes asociar al usuario de tu sistema operativo, pero esto tiene ciertos inconvenientes (si eliminas el usuario del sistema simplemente no podrás acceder a la base de datos) por lo que la mejor forma de usar estos programas definitivamente es con **una contraseña maestra**.

Aunque alguien sustrajera la base de datos del programa, está encriptada y únicamente puede ser abierta con tu contraseña maestra por lo que la base de datos sin la contraseña es inservible.

Mi programa favorito para este fin es **keePass** (para Windows), es un software gratuito pero muy seguro, se puede descargar **desde su página Web**.



Descargar e instalar este programa es muy sencillo, la primera vez que lo abramos nos pedirá crear una base de datos que será nuestro repositorio de contraseñas, a partir de ese momento ya podrás empezar a guardar tus contraseñas dentro del programa.

KeePass tiene características muy interesantes entre las que destaca la posibilidad de crear categorías para guardar las contraseñas, generar contraseñas aleatoriamente y posibilidad abrir y pegar directamente el nombre de usuario y contraseña en el sitio Web con sólo un clic.

Seguridad de tu base de datos.

Si has llegado hasta aquí supongo que ahora se te estará pasando por la cabeza instalarte el programa y quizás te hayas preguntado, ¿Qué pasaría si el equipo donde está instalado el programa se estropea? ¿y si se quema o me lo roban?

Evidentemente, si no tienes una copia de seguridad de la base de datos de las contraseñas simplemente, **¡te has quedado sin ninguna contraseña!** Pero tranquilo, que también hay solución, y consiste en almacenar tu base de datos de contraseñas en un disco duro virtual por ejemplo en **DropBox**, tan sólo tendrás que subir la base de datos de contraseñas a Dropbox y configurar KeePass con la utilidad dedicada para tal fin, para que se conecte a tu DropBox, así podrás leer tu base de datos y guardar nuevas entradas de contraseñas de forma segura en la nube, en contra tiene dos requisitos más, no se te puede olvidar la contraseña de DropBox y necesitarás de acceso a internet para acceder a tu base de datos.

Disponer de la **base de datos en la nube** te permite configurar KeePass en varios equipos que utilices (por ejemplo sobremesa y portátil) y acceder a la misma base de datos desde ambos por lo que des de alta en uno lo verás en otro y viceversa.

Sin lugar a dudas es la solución más segura para **salvaguardar todas tus contraseñas**.

No he querido entrar en más detalles sobre el programa, instalaciones, etcétera… pero si vas a intentar mejorar tu seguridad e instalar el programa y te surge alguna duda, escríbela en los comentarios para que pueda ayudarte a resolverlo.

¡Hasta la próxima entrada!