Cómo administrar sus contraseñas en línea

“En la nube!” dijo Microsoft en su campaña publicitaria de Windows 7. Nos encantaría poner nuestra información personal en cuentas en toda la web, recibiendo a cambio los servicios en la nube con la facilidad y comodidad de esta. En este punto, es probable que haya muy poco acerca de usted que no está conectado a alguna parte.

Los hackers se han dado cuenta de que nuestros valiosos (y lucrativos) datos están ahí fuera, esperando a ser vulnerados o abiertos. ¿entonces Cómo vamos a proteger las cuentas en línea de la intrusión?

En primer lugar, usted debe comenzar con una pequeña pieza de software conocido como un administrador de contraseñas. No sólo todos le ayudarán a bloquear sus cuentas, pero te salvará de tener que introducir sus credenciales de inicio de sesión cada vez que ingrese a su equipo (todos los nombres de usuario y las contraseñas se almacenan dentro de estas herramientas). Algunos incluso extienden esta funcionalidad en sus dispositivos móviles también.

Un gestor de contraseñas mantiene sus datos seguros ya que le permite usar contraseñas que sean difíciles de descifrar como lo son para recordar. En lugar de una contraseña como “lumia920fan”, el director me sugieren algo en la línea de “50P3HofuvzDL”. Ahora imagine que usted está utilizando una contraseña complicada como el que para cada sitio web que conectarse. Que tenga buena suerte.

El uso de contraseñas para sus cuentas en línea que son a la vez fuertes y únicas, es importante para un par de razones. Los hackers han penetrado las defensas de incluso los mayores servicios de nube, como iCloud y los sistemas de Gawker, y

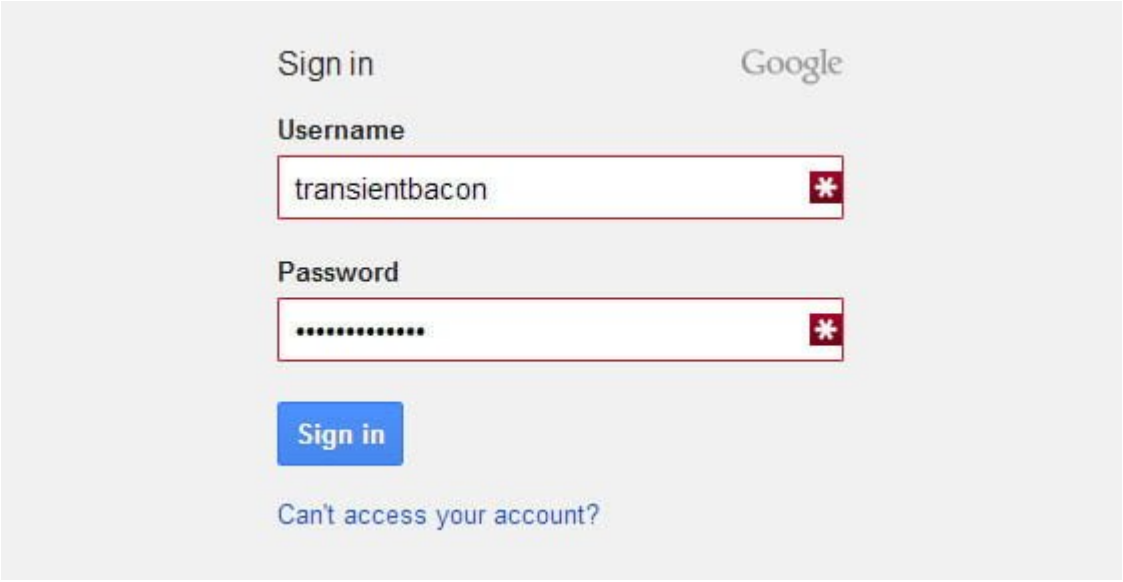
cuando lo hacen, suelen descargar los datos sensibles tanto como sea posible para que se pueda desmenuzar a su discreción. Entonces es sólo una cuestión de tiempo hasta que se puedan descifrar sus credenciales de cuenta, obteniendo un acceso completo a su información.

Los hackers intentarán comprometer su nombre de usuario y contraseña en cientos de otros sitios, con la esperanza de que usted tambien los utiliza en más de un punto. Muchos de nosotros somos culpables de este paso en falso y la información contenida en otros sitios pueden ayudar a los hackers a entrar en las cuentas aún más. Uno sólo tiene que mirar la historia con moraleja de Mat Honan para un ejemplo aterrador, donde el número de tarjeta de crédito que figura en su cuenta de Amazon permite a los hackers entrar en sus cuentas de Google. Las contraseñas seguras también aumentan drásticamente la cantidad de tiempo que tarda un ordenador para romper esta, haciendo que su cuenta sea mucho más propensa a ser pasado por alto en lugar de las personas con contraseñas débiles.

Teniendo en cuenta estos peligros, no es ninguna sorpresa que hay bastantes gestores de contraseña hacia fuera allí, tanto para plataformas PC y móviles. Aquí están algunos de los mejores.

Administradores de Contraseñas

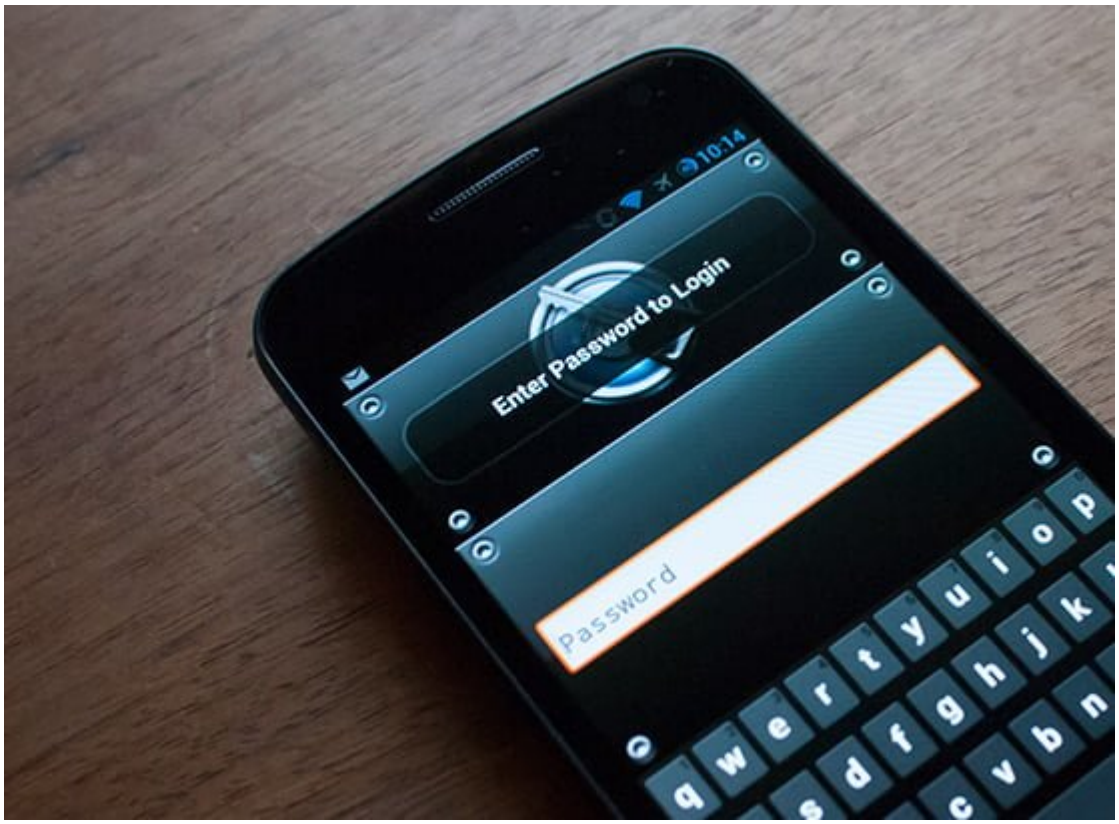
El administrador de contraseñas primero que vamos a estar buscando en un servicio llamado LastPass. Inicialmente lanzado en 2008, LastPass vive casi en su totalidad dentro de un plugin para el navegador. Detectará automáticamente formularios de contraseña, generará contraseñas seguras, y rellenar las credenciales guardadas a medida que viajas alrededor de la web. Es gratuito para uso de escritorio, pero las personas que quieran usarlo en sus dispositivos móviles tienen que comprar la compañía de $ 12 Servicio / año Premium.



LastPass es a veces criticado por los aficionados acérrimos de seguridad para el almacenamiento de sus datos en sus servidores, poniéndolo en riesgo de ser extraído por los piratas informáticos. Esto es cierto, pero los datos son encriptados antes de ser enviados, asi que puede poner su mente a descansar siempre y cuando la contraseña maestra de LastPass es en sí misma sea segura – usted tendrá que recordar eso. La compañía ha detectado una intrusión en realidad el año pasado que puso a "decenas de usuarios" en situación de riesgo, pero sólo porque tenían contraseñas maestras débiles. Después de trabajar con rapidez para restablecer y obtener las cuentas de los afectados, el representante de LastPass Joe Siegrist confirmó que los usuarios con contraseñas maestras fuertes no tenía nada de qué preocuparse.

A pesar de su torpeza seguridad antes, LastPass ofrece varias funciones que sus competidores no lo hacen. En primer lugar, es compatible con Google Authenticator. Esta aplicación multiplataforma hace imposible que las contraseñas de su cuenta de LastPass ser hackeado sin acceso físico al teléfono. LastPass también ofrece algunos de los mejores teléfonos inteligentes integración de cualquier administrador de contraseñas, y puede integrarse con Firefox y el navegador Dolphin en Android casi a la perfección. También puede instalar un bookmarklet personalizado que se llene nombre de

usuario y las contraseñas en páginas web con sólo unos toques.



1Password es uno de los mas importantes competidores para LastPass, y a pesar de interfaz de su diseño al estilo de interfaz Apple, el administrador de contraseñas es compatible con Mac, Windows, iOS y Android. 1Password no tiene las mismas caaracteristicas como LastPass, pero su estrategia basada en sincronización con Dropbox, significa que tiene completamente el control de todos sus datos. En lugar de sincronizar con los servidores de la empresa, 1Password puede colocar su contraseña en una base de datos dentro de una cuenta de Dropbox, que puede ser sincronizada con un teléfono. La compañía tiene una versión reciente con actualización para iOS 4 que cuesta $ 7.99 y ofrece sincronización iCloud.

En el pasado, 1Password puede integrarse con el navegador de iOS usando un bookmarklet, pero la compañía abandonó esa funcionalidad hace algún tiempo. En su lugar, usted tiene que utilizar el navegador web integrado en la aplicación. La versión de Android es notablemente inferior a la de : puede ver las contraseñas, pero no los cambia, y hay un botón de

“Autologin”, pero en las pruebas no logra hacer nada más que levantar una pantalla en blanco en dos diferentes dispositivos Android.

La elección de un servicio de pago como estos dos es sin duda su opción más sencilla, pero se puede reproducir la mayoría de sus capacidades y herramientas gratis – si usted está dispuesto a ser creativo con su software. Se puede usar un gestor de contraseñas gratuito como KeePass para generar contraseñas seguras en el escritorio, o tambien utilizar Firefox Sync en conjunto con Firefox para Android para sincronizar su dispositivo móvil. Desafortunadamente, Chrome para Android y iOS no sincroniza las contraseñas guardadas en tu ordenador o portátil, y no hay ninguna versión de Firefox para iOS en este momento.

Otras opciones

Los Administradores de Contraseñas no son la única manera de proteger su identidad en línea, por supuesto. Los fieles usuarios de Google deberían considerar el uso de esta herramienta que se realizan en 2 etapas de verificación.

Puede habilitar esta configuración de seguridad en su cuenta de Google, y aunque es un poco incómodo a veces, los 2 pasos de verificación hace que sea mucho más difícil para alguien que desea tener acceso a su cuenta de Google.

Cada vez que inicie sesión en Google desde un dispositivo nuevo, se realizaran los 2 pasos de verificación que requiere con un código enviado a su teléfono a través de mensaje de texto. (También puede crear e imprimir las contraseñas de un solo uso, para cuando usted no tiene su teléfono a mano.) Después de introducir el código en el navegador, puede optar por activar la máquina o dispositivo durante un máximo de 30 días. Si usted utiliza su cuenta de Google para acceder a servicios en línea, estos 2 pasos de verificación es una de las maneras más fáciles de aumentar drásticamente su seguridad

en línea.

Con la Autenticación y acceso al Smartphone por medio de claves, es una de las maneras de añadir un segundo elemento a su esquema de seguridad, pero algunos usuarios no estarán satisfechos hasta que sus ordenadores se parecen algo sacado de una película de espías. Afortunadamente, LastPass es compatible con dispositivos como lectores de huellas digitales y tarjetas inteligentes, siempre que puedan interactuar con el navegador web. Al igual que el YubiKey, tales capas de seguridad física puede llegar a ser una molestia para las personas con dispositivos móviles, pero si estás pensando en las características de seguridad en este nivel, esto probablemente no te molestará mucho.