

Cómo Configurar La Autenticación De Dos Pasos Para Facebook, Google, Microsoft Y Más

Cómo Configurar La Autenticación De Dos Pasos Para Facebook, Google, Microsoft Y Más,

La autenticación de dos pasos puede no ser tan atractivo como el último teléfono Android, pero la tecnología está capturando titulares de noticias, y con razón. La semana pasada, Microsoft comenzó el despliegue de esta herramienta de seguridad para sus cerca de 700 millones de usuarios de cuentas de Microsoft. El Martes, la revista Wired informó en Twitter, que está trabajando en la autenticación de dos factores también.

Es una característica de seguridad que podrían haber dejado de hackers en la puerta de entrada antes de que se hicieran con el control de la cuenta de Associated Press Twitter, y es algo que usted debe utilizar para proteger sus propias cuentas en línea, donde esté disponible.

Entonces, ¿cómo funciona la autenticación en dos pasos? En pocas palabras, se requiere no uno, sino dos pedazos de información privilegiada antes de conceder el acceso a una cuenta en línea.

Digamos que usted ya ha configurado la autenticación de dos pasos para su cuenta de Google, y ahora un hacker otro lado del mundo está tratando de entrar en su cuenta de Gmail. Él

tiene su dirección de correo electrónico e incluso la contraseña, pero no tiene el segundo elemento del proceso de autenticación. En el caso de las cuentas de Google, el segundo elemento es un código de seguridad único que se envía directamente a su teléfono celular a través de mensajes de texto.

En esencia, la autenticación de dos factores requiere de algo que has aprendido de memoria (la contraseña) y algo que tiene en su bolsillo (su teléfono).

Si la autenticación de dos pasos suena como una especie de dolor, bueno, lo es. Activar esta función es una manera muy fácil de hacer la vida más difícil para usted, ya que tendrá que pasar más tiempo para probar su identidad cada vez que inicie sesión en una cuenta protegida de una nueva pieza de hardware. Sin embargo, este nivel de autenticación hace que sea mucho más difícil para los hackers tomar el control de sus cuentas.



¿Tiene una cuenta de Google y un teléfono inteligente? Entonces usted debe tener la autenticación de dos pasos activada.

Empezar también requiere un poco de trabajo de campo de su parte. La mayoría de los sitios y servicios que ofrecen autenticación de dos pasos como una característica opcional de seguridad, por lo que se necesita para iniciar sesión en sus diversas cuentas y cavar en torno a la configuración de seguridad para encontrarlo.

Google y Facebook han ofrecido autenticación de dos pasos, como medida de seguridad opcional desde 2011. Dropbox comenzó a ofrecer el año pasado y Apple iCloud tiene autenticación de dos pasos en marzo. Microsoft está llegando tarde a la fiesta, pero ahora lo tiene, y la versión de Twitter de la tecnología

no puede llegar lo suficientemente pronto.

En aras de la brevedad, voy a correr por el proceso de configuración de dos pasos para las tres grandes redes sociales, así como los servicios de almacenamiento remoto favoritos. Pero usted debe duplicar este proceso a través de todos los sitios y servicios que ofrece se utiliza la autenticación de dos pasos. Y si parece que una gran cantidad de sistemas de gestión, no se preocupe, hay una aplicación para eso.

Comience con Google

Google hace autenticación de dos factores bastante simple, pero puede ser muy frustrante para configurar si inicia sesión en Google a través de múltiples dispositivos. Para comenzar, ingrese a su cuenta de Google y vaya a la sección Seguridad de la página Configuración de la cuenta.

Pop hasta la sección de verificación de 2 pasos y darle la vuelta haciendo clic en el botón Configuración grande y siguiendo la guía de Google paso a paso para vincular su cuenta con el número de un teléfono celular o teléfono fijo. Google o bien texto o robocall en ese número para proporcionar un código de seis dígitos cada vez que intente acceder a su cuenta de Google desde un dispositivo «no confiable», por lo que asegúrese de usar el número de un teléfono que tenga a mano.



También puede generar códigos de un solo uso que puede anotar y guardar para los momentos en que desee iniciar sesión en Google, en ausencia del servicio de celular y generar cinco o diez de estos códigos, y mantenerlos en su cartera en caso de emergencia. Tenga en cuenta también la descarga de la aplicación Google Authenticator para iOS y Android para los usuarios del sistema operativo iOS, si no quieres que Google envíe más mensajes de texto cada vez que revise su correo desde un equipo nuevo.

Es muy sencillo de usar, y puede generar códigos para cualquier servicio de autenticación que utiliza el algoritmo TOTP (basado en el tiempo One-Time Password), incluyendo Facebook y Dropbox. Recomiendo hacer la configuración si vas a estar habilitando la autenticación de dos pasos en otros servicios, pero ten en cuenta que esto hará que sea muy difícil para que acceda a estos servicios sin su teléfono. Si su teléfono se pierde o es robado, o si simplemente elimina accidentalmente el app autenticador, es posible descargar una versión actualizada y volver a autenticar a través de todos los servicios que utiliza, pero es un dolor real.

Facebook **es**
fácil **en**

comparación

Facebook se unió a la este proceso de verificación de dos pasos un poco tarde, pero al menos se tomó el tiempo extra para suavizar el proceso de instalación. La activación de la autenticación de dos pasos para su cuenta de Facebook es muy fácil. Sólo tiene que acceder a Facebook y haga clic en el icono configuracion(icono) en la esquina superior derecha, haga clic en el menú de Ajustes de Cuenta.

A continuación, seleccione la sección Seguridad en la barra de navegación en el lado izquierdo de la pantalla y activar la función Aprobaciones Login (término de Facebook para la autenticación de dos factores) haciendo clic en la casilla correspondiente. Facebook le guiará a través del proceso, explicando cómo recibir y escribir en un código alfanumérico único cada vez que desee acceder a su cuenta.



Para conseguir el código tendrá que o bien descargar una aplicación de Mobile Authenticator que genera códigos cada vez que inicia sesión, o dar su número de teléfono móvil de Facebook, así que usted puede enviar los códigos de autenticación a través de SMS. Recomendando ir por la ruta aplicación autenticador. Es muy sencillo de usar, y usted no tiene que esperar a que los servidores de Facebook para el envío de su código. Además, usted también puede agregar un número de teléfono móvil como una copia de seguridad adicional si la aplicación no funciona.



En su aplicación móvil, Facebook construido en una característica Generador de código que genera códigos TOTP para su cuenta, pero se puede utilizar cualquier aplicación

autenticador TOTP antigua si usted está dispuesto a saltar el proceso de configuración de Facebook.

Si está utilizando aplicaciones Mobile Authenticator de Google para gestionar la autenticación de dos pasos a través de múltiples servicios, por ejemplo, que es una idea genial que se puede configurar para proporcionar códigos autenticador de su cuenta de Facebook también.

Sólo debe iniciar el proceso de configuración del generador de código, haga clic en el vínculo Configurar Generador de código en Aprobaciones sesión en tu configuración de seguridad de Facebook, y cuando llegue el momento de abrir la aplicación móvil de Facebook, haz clic en el enlace – Tienes problemas?.

Facebook le pedirá que haga clic en un botón azul grande para obtener la clave e introduzca la clave de 16 caracteres proporcionada en su aplicación móvil de Facebook, pero se puede entrar en casi cualquier autenticador app incluyendo la de Google y seguirá funcionando.

Microsoft finalmente está

participando

Su cuenta de Microsoft cubre su buzón de Outlook, su perfil de Xbox Live, Windows Phone, y mucho más. Mejorar la seguridad en todos los ámbitos por el cambio en la autenticación de dos factores en la sección de seguridad de la página de resumen de cuenta de Microsoft.

Usted puede configurarlo de modo Microsoft enviará códigos de seguridad ya sea una dirección de correo electrónico alternativa o su teléfono inteligente a través de SMS, a menos que prefiera para descargar una aplicación para el autenticador que va a generar códigos de seguridad para usted.

Los usuarios de Windows Phone pueden descargar propia aplicación autenticador de Microsoft en la tienda de Windows, pero todos los demás sólo pueden usar cualquier aplicación autenticador que soporta el algoritmo de contraseña de una sola vez (One-Time Password algorithm.).



Para simplificar, le recomiendo usar la mencionada aplicación Google Authenticator en iOS y Android. Utilice la aplicación para escanear el código de barras que le proporciona Microsoft durante el proceso de autenticación de dos pasos y generará los códigos para su cuenta de Microsoft también.

Y usted no tiene que parar allí, esperar a Twitter que tendrá su sistema de autenticación de dos pasos, y hay un montón de otros sitios y servicios que ya ofrecen sistemas de seguridad similares. Dropbox, LastPass, Box, e incluso Amazon Web Services soporta la autenticación de dos pasos, al igual que muchos de los servicios bancarios. El bloqueo de estas cuentas con autenticación de dos factores añade otra capa de seguridad a su vida digital, que puede ser desbloqueada sólo con el

teléfono inteligente en su bolsillo.