VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Septiembre 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Verificación en dos pasos

Resumen

El proceso de probar quién eres (llamado autenticación) es clave para proteger tu información. Una autenticación fuerte intenta garantizar que sólo tú puedes acceder a tu información personal, como tu correo electrónico, fotos o cuentas bancarias. Existen tres formas diferentes para confirmar quién eres: algo que sabes (como una contraseña), algo que tienes (como la licencia de conducir), y algo que eres (como tu huella digital). Cada uno de estos métodos tiene sus ventajas y desventajas. El método más común son las contraseñas, algo que sabes. En este boletín vamos a enseñarte cómo protegerte usando la verificación en dos pasos, algo mucho más seguro que utilizar sólo contraseñas y a la vez muy fácil de implementar. Para entender mejor la verificación en dos pasos, tenemos que empezar con las contraseñas.

Editor Invitado

Keith Palmgren tiene más de 30 años de experiencia en seguridad de la información. Él es instructor certificado por el Instituto SANS y autor de SANS SEC301, un curso de cinco días de Introducción a la Seguridad de la Información. Cuando no está enseñando, Keith se dedica a la consultoría y proyectos de escritura. Sigue a Keith en su Twitter **@kpalmgren**.

Contraseñas

Las contraseñas prueban quién eres basado en algo que sabes. El peligro de éstas es que son un punto único de fallo. Si alguien adivina o tiene acceso a tu contraseña, puede pretender ser tú y acceder a toda la información que está asegurada por la misma. Es por esto que se enseñan buenas prácticas para protegerla, como el uso de contraseñas seguras que son difíciles de adivinar, utilizar una contraseña diferente para cada cuenta o no compartir nunca tus contraseñas con otras personas. Aunque estos consejos siguen siendo válidos, las contraseñas han sido utilizadas más de lo planeado y ya no son eficaces en estos días. Las últimas tecnologías hacen que sea demasiado fácil para los atacantes cibernéticos robar contraseñas. Lo que necesitamos es una solución fácil de usar y más segura para obtener una autenticación fuerte. Afortunadamente, esa opción está disponible en algo que se llama verificación en dos pasos.

Verificación en dos pasos

La verificación en dos pasos (a veces llamada autenticación de dos factores o 2FA) es una solución más segura que utilizar sólo contraseñas. Funciona al no requerir uno, sino dos métodos diferentes para autenticarse; un ejemplo es la tarjeta

Verificación en dos pasos

del cajero automático. Cuando retiras dinero de un cajero automático, en realidad se utiliza una forma de verificación en dos pasos. Para acceder al dinero se necesitan dos cosas: tu tarjeta (algo que tienes) y tu número de PIN (algo que sabes). Si pierdes tu tarjeta, el dinero está a salvo ya que quien la encuentre no puede retirar dinero al desconocer tu PIN (a menos que hayas escrito el PIN en la tarjeta, que es una muy mala idea). Lo mismo ocurre cuando sólo tienen tu PIN y no la tarjeta. Un atacante debe tener ambos para comprometer tu cuenta bancaria. Esto es lo que hace mucho más segura la verificación en dos pasos, ya que tiene dos capas de seguridad.

Usa la verificación en dos pasos siempre que sea posible, es una de las medidas más fuertes para proteger tu información.

Usando la verificación en dos pasos

La verificación en dos pasos es algo que configuras individualmente para cada una de sus cuentas, afortunadamente muchos servicios en línea ahora lo ofrecen. Uno de los líderes en la verificación en dos pasos es Google. Las cuentas de Google son un objetivo prioritario para los atacantes cibernéticos, ya que la compañía ofrece una variedad de servicios gratuitos en línea a millones de personas en todo el mundo. Así fue como Google necesitó proporcionar una autenticación fuerte, además fue de las primeras organizaciones en implementar la verificación en dos pasos para la mayoría de sus servicios en línea. Si entiendes cómo funciona la verificación en dos pasos de Google, entenderás cómo funciona en otros sitios como Twitter, Facebook, Apple, Instagram y muchos bancos.

En primer lugar, se habilita la verificación en dos pasos en tu cuenta de Google y se registra tu número de teléfono móvil. Una vez completado, la verificación en dos pasos funciona como sigue. Ingresas a tu cuenta igual que antes con tu nombre de usuario y contraseña; éste es el primero de los dos factores (algo que sabes). Google envía un mensaje de texto a tu teléfono móvil que contiene un código único, específicamente una serie de seis números. Al igual que la contraseña, a continuación se deben ingresar esos seis números en el sitio web; éste es el segundo de los dos factores. Así que para acceder con éxito a la cuenta, es necesario saber tanto la contraseña y tener tu teléfono móvil para recibir los códigos únicos. Incluso si un atacante tiene la contraseña, no pueden acceder a tu cuenta de Google a menos que también tenga tu teléfono. Para asegurarte de que tu cuenta está realmente segura, Google enviará un nuevo código único cada vez que se conecte.

Verificación en dos pasos

Hay otra opción para la verificación en dos pasos con Google y muchos otros sitios. En lugar de recibir el código único a través de mensajes de texto SMS, puedes instalar una aplicación de autenticación en tu teléfono inteligente. La aplicación genera un código único para ti cada vez que quieras ingresar. La ventaja con el uso de una aplicación móvil es que no es necesario estar conectado a un servicio telefónico para recibir el código único, el teléfono lo genera por ti. Además, ya que se genera el código de forma local en el teléfono y no es enviado, no puede ser interceptado.

Recuerda, si la verificación en dos pasos no está activada por defecto, tienes que habilitarla. Aunque puede parecer al principio que trae más trabajo, te recomendamos utilizarla siempre que sea posible, especialmente para los servicios críticos como cuentas de correo electrónico, banca en línea o almacenamiento de archivos en línea. La verificación en dos pasos va mucho más allá para proteger tu información que una simple contraseña.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Frases de acceso:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_sp.pdf
Cómo crear contraseñas seguras:	http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=185
Clave de seguridad para la verificación en dos pasos:	https://support.google.com/accounts/answer/6103523?hl=es
Sitios con verificación en dos pasos:	https://twofactorauth.org
Verificación en dos pasos de Google:	http://www.google.com/landing/2step/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: José Carmen Hernández, Xocoyotzin Carlos Zamora, Katia Rodríguez

