VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Agosto de 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Quién eres?
- Contraseñas
- Verificación en dos pasos
- Usando la verificación en dos pasos

Verificación en dos pasos

¿Quién eres?

El proceso de probar quién eres (llamado autenticación) es un paso clave para proteger tu información en línea. Si deseas estar seguro de que eres la única persona que tiene acceso a tu información privada, entonces necesitas un método seguro para demostrar quién eres, como cuando verificas tu correo electrónico, compras algo en línea o accedes a tus cuentas bancarias. Puedes demostrar que eres quien dices ser de tres diferentes maneras: con algo que sabes, como una contraseña; con algo que tienes, como tu pasaporte; y con algo que eres, como tu huella digital. Cada uno de estos métodos tiene sus ventajas y sus desventajas. El método más común, es usar algo que sabes: las contraseñas.

Editor Invitado

James Tarala es el editor invitado para esta edición. Es conferencista, autor e instructor en el SANS Institute. James es consultor en Enclave Security y colaborador en Critical Security Controls y **AuditScripts.com**. Encuentra a James en Twitter como **@isaudit** o conócelo en persona en uno de sus próximos cursos.

Contraseñas

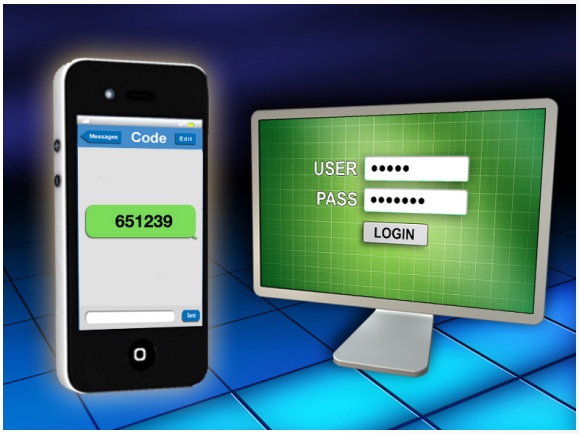
Lo más probable es que utilices contraseñas casi todos los días de tu vida. El propósito de una contraseña es demostrar que eres quien dices ser. El peligro con las contraseñas es que si alguien puede adivinarla u obtener acceso a ella, entonces, se pueden hacer pasar por ti y acceder a toda la información que tienes asegurada. Es por ello que se enseñan algunos pasos para proteger las contraseñas, como el uso de contraseñas fuertes, que son difíciles de adivinar por los atacantes. El problema de las contraseñas es que se están volviendo anticuadas rápidamente. Con las nuevas tecnologías, cada vez se vuelve más fácil para los cibercriminales realizar ataques de fuerza bruta y, eventualmente, adivinar contraseñas o recolectarlas con tecnologías que capturan lo que se escribe en el teclado (keyloggers). Afortunadamente, existe una opción que cada vez es más común, se llama verificación en dos pasos. Te recomendamos utilizar esta opción para protegerte siempre que sea posible.

Verificación en dos pasos

La verificación en dos pasos (a veces llamada autenticación de dos factores) es una forma más segura para probar tu identidad. En lugar de usar solamente un paso para la autenticación, tal como una contraseña (algo que sabes), se requieren de dos pasos. Tu tarjeta del banco es un ejemplo. Cuando retiras dinero de un cajero

Verificación en dos pasos

automático, en realidad estás usando una forma de verificación en dos pasos. Para demostrar quién eres al acceder a tu dinero, necesitas dos cosas: la tarjeta del banco (algo que tienes) y tu número de identificación personal o PIN (algo que sabes). Si pierdes la tarjeta que usas en el cajero automático, tu dinero sigue a salvo, cualquier persona que encuentre la tarjeta no puede retirar tu dinero, ya que no conoce tu número de identificación personal (a menos que hayas escrito el número en tu tarjeta, lo cual es una mala idea). Se cumple lo mismo si solo tienen tu PIN y no la tarjeta. Un atacante debe tener ambos para poder comprometer tu cuenta. Esto es lo que hace que la verificación en dos pasos sea mucho más segura: cuentas con dos capas de seguridad.



Usa la verificación en dos pasos siempre que sea posible, es una solución mucho más segura que usar solo contraseñas.

Usando la verificación en dos pasos

Uno de los líderes de la verificación en dos pasos en línea es Google. Con una variedad de servicios libres en línea tales como Gmail, Google necesitaba proporcionar una solución de autenticación más fuerte para sus millones de usuarios, por lo que implementó la verificación en dos pasos en la mayoría de sus servicios en línea. La verificación en dos pasos de Google no solo es un servicio gratuito en el que cualquiera de sus usuarios puede inscribirse, sino que otros proveedores en línea están utilizando una tecnología similar para sus servicios, tales como Dropbox, Facebook, LinkedIn y Twitter. Al entender el funcionamiento de la verificación en dos pasos de Google, podrás entender cómo funcionan otros servicios de verificación en dos pasos en línea.

La verificación en dos pasos de Google funciona de la siguiente forma. Primero necesitarás tu nombre de usuario y contraseña, igual que antes. Éste es el primer factor, algo que sabes. Sin embargo, Google requiere un segundo factor, algo que tienes, en concreto, tu smartphone. Hay dos maneras en las que puedes utilizar tu smartphone como parte del proceso de inicio de sesión. La primera es registrar tu número de teléfono con Google. Cuando intentes autenticarte con tu nombre de usuario y contraseña, Google te enviará un mensaje de texto (SMS) con un código único para tu smartphone, después, deberás introducir este número al iniciar sesión. La otra opción es instalar un software de autenticación de Google en tu smartphone. El software genera un código único para ti. La ventaja de este segundo método es que no necesitas estar conectado a un proveedor de servicios, ya que el teléfono genera el código para ti.

Verificación en dos pasos

La verificación en dos pasos no está habilitada, por lo general, es algo que tienes que habilitar por ti mismo. Además, la mayoría de las aplicaciones móviles aún no son compatibles con la verificación en dos pasos. Para la mayoría de las aplicaciones móviles tendrás que utilizar aplicaciones específicas de contraseñas, que puedes generar una vez que hayas habilitado la verificación en dos pasos. Por último, tienes la opción de crear claves de recuperación en caso de que pierdas tu smartphone. Recomendamos imprimir estas claves y guardarlas en un lugar seguro, bajo llave.

Te recomendamos ampliamente que utilices la verificación en dos pasos siempre que sea posible, especialmente para servicios críticos, tales como correo electrónico o almacenamiento de archivos. La verificación en dos pasos va mucho más allá para proteger tu información, por lo que los delincuentes tienen que esforzarse mucho más para comprometer tus cuentas.

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

Donde se puede utilizar verificación en dos pasos:	http://preview.tinyurl.com/mv6da8m
Verificación en dos pasos de Google:	http://www.google.com/landing/2step/
Términos comunes de seguridad:	http://www.viruslist.com/sp/glossary
Consejos de seguridad de UNAM-CERT:	http://www.seguridad.unam.mx/usuario-casero/consejos/
Tip del día de seguridad del SANS:	https://www.sans.org/tip_of_the_day.php

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Paulo Contreras, Jonathan Banfi, Nora Cozaya, Célica Martínez