SANS SECURITY AWARENESS
VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Diciembre 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- **Las contraseñas ya no son suficiente**
- **¿Qué es la autenticación de doble factor?**
- **Cómo funciona**

Protege tu inicio de sesión

Resumen

El proceso de autenticación, o prueba de identidad, es primordial para proteger tu información, como tu dirección de correo electrónico, cuentas bancarias o de redes sociales. Puede que no te des cuenta de esto, pero existen tres formas diferentes de demostrar quién eres: algo que sabes (como una contraseña), algo que tienes (como una licencia de conducir) y algo que eres (como tu huella digital). Cada uno de estos métodos tiene ventajas y desventajas. El método más común de autenticación es la contraseña, algo que sabes. Desafortunadamente, se está demostrando que usar solo contraseñas es cada vez más inseguro. En este nuevo boletín te enseñamos cómo proteger tu identidad y tu inicio de sesión con algo mejor que solo contraseñas. Esto se llama autenticación de doble factor.

Editor Invitado

Tiffany Schoenike es la directora de la campaña e iniciativa de la Alianza Nacional de Ciberseguridad (**@staysafeonline**). En 2016, Tiffany trabajó con la Casa Blanca, el gobierno y la industria para desarrollar y presentar "Protege tu inicio de sesión", una campaña sobre la autenticación de doble factor llamada: Para. Piensa. Conéctate.™

Las contraseñas ya no son suficiente

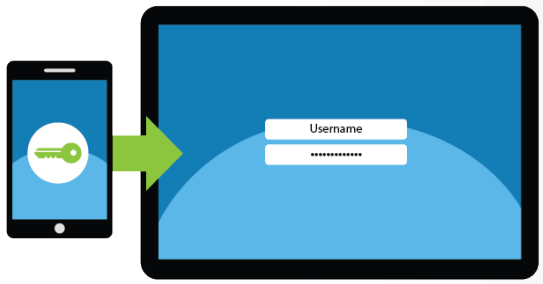
Las contraseñas demuestran quién eres basado en algo que sabes. Pero si alguien adivina u obtiene tu contraseña, puede fingir ser tú y acceder a toda tu información. Las contraseñas comprometidas se han convertido en una de las principales causas de cuentas robadas. Es por esto que se recomienda usar contraseñas difíciles de adivinar, una contraseña diferente para cada cuenta y nunca compartir tus contraseñas con otros. Si bien este consejo sigue siendo válido, las contraseñas no son muy efectivas. Afortunadamente, hay una simple y rápida forma de tener el control y mantener tu información personal a salvo, llamada autenticación de doble factor.

¿Qué es la autenticación de doble factor?

La autenticación de doble factor (también llamada verificación de dos pasos, autenticación multifactor, o 2FA) es más

Protege tu inicio de sesión

segura que solo usar contraseñas. Esto funciona al requerir no uno, sino dos métodos de autenticación para demostrar que eres quien dices ser. Un buen ejemplo es tu tarjeta ATM. Cuando retiras dinero de un cajero ATM, estás usando en realidad autenticación de doble factor. Para tener acceso a tu dinero necesitas dos cosas, tu tarjeta ATM (algo que tienes) y tu número PIN (algo que sabes). Si tu tarjeta ATM se pierde o es robada, otros no podrán retirar tu dinero sin saber además tu PIN. Un ladrón debe tener ambos, tu tarjeta ATM y tu PIN para hacer un retiro. La autenticación de doble factor usa el mismo concepto.



Protege tu inicio de sesión mediante el uso de autenticación de doble factor siempre que sea posible, esta es una de las medidas más fuertes que puedes tomar para protegerte en línea.

Cómo funciona

La autenticación de doble factor está ampliamente disponible en la mayoría de los bancos, correos, redes sociales y otros sitios. Adicionalmente, muchos de estos sitios ofrecen instrucciones paso a paso de cómo habilitar la autenticación de doble factor (para más información, ve los recursos de la sección final). Una vez que habilitas la autenticación de doble factor puedes contar con que funcione. Primero, ingresas a tu cuenta usando tu nombre de usuario y tu contraseña, tal como lo has hecho siempre. Éste es el primero de los dos factores (algo que sabes). Entonces recibirás un código único, a menudo por mensaje de texto en tu teléfono. Entonces ingresas el código en la pantalla de acceso. Éste es el segundo de los dos factores (debes tener tu teléfono para recibir el código). Ahora tu cuenta está realmente desbloqueada. Incluso si un cibercriminal roba tu contraseña, no podrá acceder a tu cuenta a no ser que además tenga tu teléfono.

En vez de recibir el código único vía mensaje de texto, puedes instalar una aplicación especial en tu teléfono. Esta aplicación móvil genera un código único para ti cada vez que quieras iniciar sesión. La ventaja de usar una aplicación móvil es que es aún más seguro, ya que el código se genera a través de la aplicación y no es enviado vía mensaje de texto. Adicionalmente, es más conveniente ya que no necesitas conectarte a tu servicio telefónico para recibir el código único. La aplicación genera constantemente nuevos códigos que puedes usar para iniciar sesión en tu cuenta.

Protege tu inicio de sesión

Si bien la autenticación de dos factores puede parecer más complicada al principio, tu información personal estará sustancialmente más segura. No esperes hasta que tus cuentas sean comprometidas, protege tu inicio de sesión habilitando la autenticación de doble factor en tus cuentas, como correo, banco o redes sociales y disfruta de una mayor tranquilidad sabiendo que estás más seguro.

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: securingthehuman.sans.org/ouch/archives

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

Frase de contraseña: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_sp.pdf

Sitios que soportan la autenticación de dos factores: https://twofactorauth.org

Para. Piensa. Conéctate: https://www.stopthinkconnect.org/tips-advice/spanish-tips-and-advice

Verificación en dos pasos: https://www.google.com/intl/es_419/landing/2step/

Una contraseña para gobernarlos a todos:
https://revista.seguridad.unam.mx/numero30/una-contrasena-para-gobernarlos-todos

Consejo editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: Jorge Alberto Hernández Cuecuecha y Diana Laura Arrieta Jiménez

