VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Junio 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Qué es el cifrado?
- ¿Qué se puede cifrar?
- ¿Cómo hacerlo bien?

Cifrado

¿Qué es el cifrado?

Es posible que escuches a la gente usando el término "cifrado" y cómo deberías utilizarlo para protegerte a ti y asegurar tu información. Sin embargo, el cifrado puede ser confuso y debes entender sus limitaciones. En este boletín se explica en términos sencillos qué es el cifrado, cómo funciona y cómo implementarlo correctamente.

Editor Invitado
Francesca Bosco (**@francibosco**) es investigadora y directora de proyectos relacionados con el ciberdelito, la seguridad cibernética y el mal uso de la tecnología. Actualmente trabaja en el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia y es cofundadora del Tech and Law Center.

En tus dispositivos tienes una gran cantidad de información sensible tales como documentos personales, fotos y correos electrónicos; si perdieras uno de tus dispositivos o te lo robaran, quien lo posea podría acceder a toda esa información sensible. Además, si realizas transacciones en línea, tales como compras o banca electrónica, alguien podría monitorear estas actividades y robar tu información personal, como tu cuenta financiera o números de tarjetas de crédito. El cifrado te protege de estas situaciones, ayudando a asegurar que personas no autorizadas no accedan o modifiquen tu información.

El cifrado ha existido desde hace miles de años. Hoy en día es mucho más sofisticado, pero tiene el mismo propósito: se utiliza para pasar un mensaje secreto de un lugar a otro asegurando que solamente las personas autorizadas podrán acceder y leer el mensaje. Cuando la información no está cifrada se le llama texto sin formato, esto significa que cualquiera puede leer fácilmente o acceder a dicha información. El cifrado convierte esta información en un formato no legible denominado texto cifrado. En la actualidad, el cifrado funciona mediante el uso de operaciones matemáticas complejas y una clave única para convertir la información en texto cifrado. La clave es qué bloquea o desbloquea tu información, en la mayoría de los casos es una contraseña o código de acceso.

¿Qué se puede cifrar?

En general, hay dos tipos de datos para cifrar: los datos en reposo (por ejemplo, los datos almacenados en el dispositivo móvil) y los datos en movimiento (como la recuperación de correo electrónico o mensajería a un amigo).

Cifrado

El cifrado de datos en reposo es vital para proteger tu información en caso de que pierdas o te roben tu equipo. Hoy en día, los dispositivos son extremadamente potentes y poseen una enorme cantidad de información, pero son muy fáciles de perder. Además, otro tipo de medios de comunicación móviles pueden contener información sensible, como una memoria USB o discos duros externos. El Cifrado de Disco Completo (FDE, por sus siglas en inglés) es una técnica ampliamente utilizada que cifra toda la unidad de disco del sistema. Esto significa que todo el sistema será cifrado automáticamente para ti, no tienes que decidir qué cifrar. La mayoría de las computadoras vienen con FDE, pero puede que tengas que habilitarlo manualmente o activarlo. En los equipos Mac se llama FileVault, mientras que en los equipos Windows, dependiendo de la versión, puedes usar Bitlocker o Device Encryption; la mayoría de los dispositivos móviles también soportan FDE. En los iPhone y los iPad se habilita automáticamente el FDE una vez que se establece un código de acceso. A partir de la versión 6.0 de Android (Marshmallow), Google requiere que FDE esté activado por defecto, siempre que el hardware cumpla con ciertos estándares mínimos.

El cifrado es una forma poderosa para proteger tu información, pero sólo es tan fuerte como tu clave.

La información también es vulnerable cuando está en tránsito. Si los datos no se cifran pueden ser monitoreados, modificados y capturados en línea. Esta es la razón por la cual debes asegurar que todas tus transacciones y comunicaciones en línea estén cifradas. Un tipo común de cifrado en línea es HTTPS, esto significa que todo el tráfico entre el navegador y un sitio web está cifrado; sabrás que usas cifrado en línea cuando aparezca https:// en la URL, el icono de candado en tu navegador o la barra de navegación de la URL se vuelve verde. Otro ejemplo es cuando envías o recibes correo electrónico, la mayoría de los clientes proporcionan funciones de cifrado que se pueden habilitar. Un tercer ejemplo es el cifrado de datos en tránsito entre dos usuarios de chat, como iMessage, Wickr, Signal, WhatsApp o Telegram; aplicaciones como estas utilizan el cifrado de extremo a extremo que impide que terceras personas accedan a los datos mientras se realizan transferencias desde un extremo del sistema o dispositivo a otro, esto significa que sólo tú y la persona con la que te estás comunicando pueden leer lo que se envía.

¿Cómo hacerlo bien?

Para asegurarte de que está protegido cuando utilizas el cifrado, es fundamental que lo uses correctamente.

Cifrado

- El cifrado es sólo tan fuerte como tu clave. Si alguien adivina u obtiene acceso a tu clave lo tendrán también a tus datos. Protege tu clave, si estás utilizando una clave de acceso o contraseña asegúrate que es segura y única. Cuanto más larga sea la contraseña, más difícil es para un atacante adivinar o usar fuerza bruta sobre ella. No olvides tu contraseña, ya que sin ella no se puede descifrar la información; si no puedes recordar todas tus contraseñas, se recomienda el uso de un gestor de contraseñas.
- El cifrado es sólo tan fuerte como la seguridad de tus dispositivos. Si se ha visto comprometido o está infectado por malware de ciberatacantes, puede pasar por alto el cifrado. Por esto es importante tomar otras medidas para asegurar tu dispositivo, incluyendo el uso de antivirus, contraseñas seguras y mantenerlo actualizado.
- Muchas apps móviles y aplicaciones de computadora ahora ofrecen un fuerte cifrado para proteger tus datos y comunicaciones. Si la app o la aplicación no utiliza cifrado, considera otra alternativa.

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

La criptografía: http://revista.seguridad.unam.mx/numero-11/la-criptograf%C3%AD-el-secreto-de-las-comunicaciones-seguras

¿Qué es el cifrado y cómo funciona?: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

Uso de cifrado en bases de datos: http://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos

El cifrado web: http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

El hombre de en medio y el cifrado electrónico:

http://revista.seguridad.unam.mx/numero-03/privacidad-el-hombre-de-en-medio-y-el-cifrado-electr%C3%B3nico

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