Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Mantente actualizado**
- **Plugins y Add-Ons**
- **Características de seguridad**
- **Privacidad**

Privacidad y seguridad en el navegador

EDITOR INVITADO

Mike Poor es el editor invitado para esta edición. Mike es un analista sénior de seguridad en la empresa consultora InGuardians Inc. (www.inguardians.com). También, es instructor sénior en el Instituto SANS, donde imparte uno de los cursos más importantes, el *SEC503: Intrusion Detection In-Depth*.

RESUMEN

Tu navegador, ya sea Internet Explorer, Fireforx, Chrome o Safari, es una de las principales herramientas que utilizas para interactuar con Internet. Los atacantes cibernéticos lo saben, por lo que tu navegador es uno de sus principales objetivos. Tu navegador puede recolectar una gran cantidad de información sobre ti sin que lo sepas. En este boletín, mencionaremos los pasos que puedes dar para proteger tu computadora y tu privacidad.

MANTÉN TU NAVEGADOR ACTUALIZADO

El primer paso para protegerte es utilizar siempre la última versión de tu navegador. No importa qué navegador uses, siempre que sea la versión más reciente. Los atacantes cibernéticos buscan y encuentran constantemente, errores de programación y otros defectos en los navegadores. Una vez que encuentran estos errores (a menudo llamados vulnerabilidades), pueden explotarlos, dando a los atacantes el acceso y, algunas veces, el control de tu sistema. Las empresas que desarrollan tu navegador (como Microsoft, Google o Apple) liberan parches de seguridad para reparar estas vulnerabilidades. Cuando instales la última versión, asegúrate de que tu navegador tenga estos problemas solucionados. Para garantizar que tu navegador esté actualizado, cerciórate que la característica de actualización automática, tanto de tu navegador como de tu sistema operativo, siempre esté activada. Algunos navegadores, como Chrome, se actualizan automáticamente cada vez que los usas.

PLUGINS Y ADD-ONS

Los plugins (algunas veces llamados complementos) son programas adicionales que pueden instalarse en tu navegador. El problema con estos programas adicionales, es que te exponen a ti y a tu sistema a un mayor riesgo. Cada programa que agregues a tu navegador tiene sus propias vulnerabilidades o debilidades únicas. Instala sólo los plugins que sean absolutamente necesarios y asegúrate de descargarlos desde un sitio de confianza reconocido. A veces, un sitio web puede solicitar la instalación de un plugin. Sé cuidadoso, puede tratarse de un truco para engañarte y que instales software infectado. Cuando te sea posible, siempre descarga e instala un

Privacidad y seguridad en el navegador

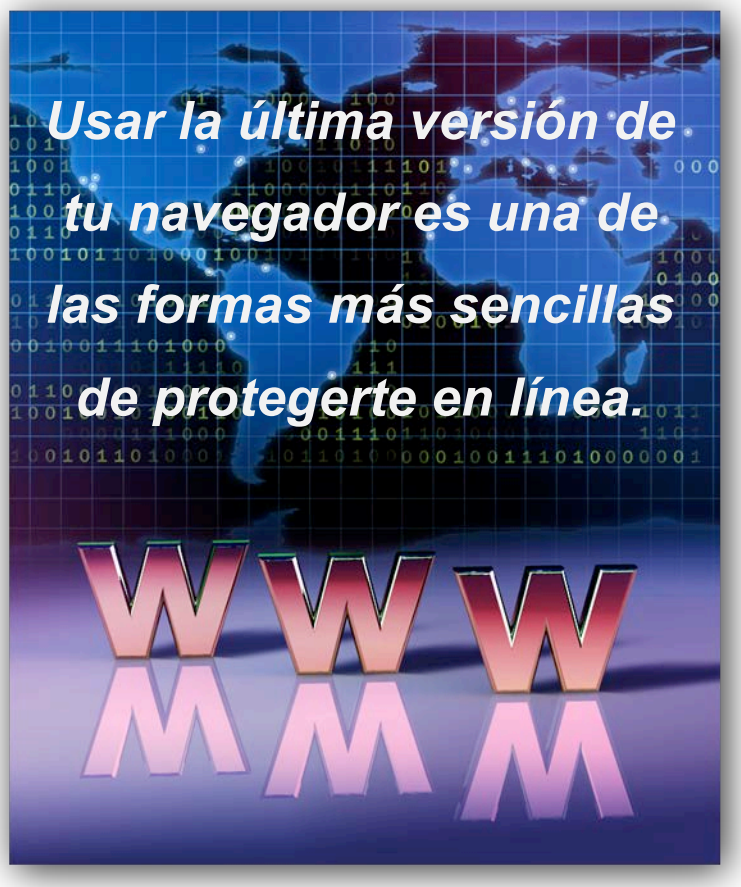
plugin desde el sitio original de su proveedor. Por ejemplo, siempre descarga o actualiza tu Flash Player desde el sitio de Adobe (www.adobe.com). Cuando hayas instalado un plugin, asegúrate de mantenerlo actualizado, así como tu navegador. Esto puede ser complicado, ya que muchos plugins no tienen la capacidad de actualizarse automáticamente; por lo que tienes que verificarlos manualmente y actualizarlos. Si este es el caso, te recomendamos verificar el estado de los plugins de tu navegador al menos una vez al mes. En la sección de recursos, hay varios sitios web de confianza que te ayudarán a hacer esto.

CARACTERÍSTICAS DE SEGURIDAD

Cada navegador tiene sus propias características de seguridad. Tómate un momento, y revisa las preferencias u opciones de seguridad del navegador. Una característica clave que casi todos los navegadores brindan, es la de advertir cuando se está a punto de visitar sitios web potencialmente maliciosos. El navegador mantiene una lista actualizada de miles de sitios web clasificados como maliciosos, o que intentan hacer algún daño a las personas. Si intentas visitar alguno de estos sitios maliciosos, el navegador se detendrá y presentará un aviso de advertencia. Cuando te aparezca un mensaje de advertencia, no vayas a ese sitio. Sé precavido con todos los sitios web que visites. El navegador no puede seguirles el paso a los intrusos; por lo tanto, no puede conocer todos los sitios maliciosos.

PRIVACIDAD

Tal vez no lo notes, pero tu navegador puede almacenar mucha información de tu actividad en línea, incluyendo “Cookies”, “Páginas en caché” y el “Historial”. Las cookies son pequeños archivos de datos que envían los sitios web



al navegador para hacer más fácil el uso de la Web; por ejemplo, almacenar preferencias. Sin embargo, las cookies también permiten a las compañías seguir tus movimientos a través de la Web. Las páginas en caché son copias almacenadas de sitios web que se visitaron recientemente. Las páginas en caché se utilizan para mejorar el rendimiento del sistema; sin embargo, también podrían ser accedidas por usuarios no autorizados. Finalmente, algunos navegadores guardan el historial de todos los sitios web visitados. A menudo, esta característica permite al navegador llevarnos rápidamente a los sitios web más visitados.

Para proteger la privacidad, es posible deshabilitar alguna o todas estas características. Algunos navegadores tienen la capacidad de eliminar manualmente los datos

Privacidad y seguridad en el navegador

almacenados, o hacerlo automáticamente cada vez que se cierre el navegador. Finalmente, la mayoría de los navegadores cuentan con un 'modo protegido', en donde se desactiva la recolección de datos, incluyendo el caché, las cookies y el historial. De esta manera, no se almacena información de nuestra actividad al navegar; no obstante, esto también limitará la capacidad de interactuar con algunos sitos. Revisa las configuraciones de seguridad de tu navegador para cambiar alguna de estas características. En conclusión, cuando sea posible, asegúrate de que las conexiones del navegador estén cifradas. Esto contribuye a que la actividad en línea no pueda ser monitoreada o capturada. Las conexiones cifradas se conocen como HTTPS. Por ejemplo, sitios como Twitter, Facebook y Google te permiten cambiar tu configuración personal para usar siempre el cifrado HTTPS cuando te comuniques con ellos. También, cuando realices una operación bancaria o compra en línea, asegúrate de que las conexiones estén cifradas. Esto lo puedes confirmar al ver 'https://' en el navegador y con la aparición de un candado.

RECURSOS

Los enlaces mostrados en este boletín han sido reducidos para mejorar la legibilidad a través del servicio TinyURL. A fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando permiso antes de abrirlo

Browser Plugin Check:
http://preview.tinyurl.com/3m9gjr5

Firefox Plugin Check:
http://preview.tinyurl.com/3vesv9b

Chrome Browser Security:
http://preview.tinyurl.com/3brxaok

Internet Explorer 9 Security:
http://preview.tinyurl.com/44w6hyv

Safari Browser Security:
http://preview.tinyurl.com/3q8h8q7

Firefox Browser Security:
http://preview.tinyurl.com/3uwy86f

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Mayra Villeda, Francisco Martínez, Galvy Cruz, Mauricio Andrade, Rubén Aquino