El Boletín Mensual de Concientización en Seguridad para ti

Navegadores

Resumen

Los navegadores como Google Chrome, Microsoft Edge, Safari de Apple o Mozilla Firefox son una de las formas más comunes en que las personas interactúan con Internet. Los usamos para leer las noticias, revisar el correo electrónico, comprar en línea, mirar videos y jugar. Como resultado, los navegadores también son un objetivo para los atacantes cibernéticos.
Muchas personas asumen que navegar en línea es seguro si solo visitas sitios conocidos y confiables. Sin embargo, es bastante fácil hacer clic accidentalmente y visitar una página web maliciosa, a veces sin siquiera saberlo. Además, los mismos sitios web que conoces y en los que confías pueden ser hackeados y los atacantes cibernéticos instalarán malware en ellos. Finalmente, los navegadores actuales tienen muchas funciones nuevas, que a menudo pueden ser confusas y, si se configuran incorrectamente, te exponen a aún más peligros.

Aprovechando de forma segura el navegador

Estos son los pasos clave para protegerte:

Actualizaciones: Utiliza siempre la última versión del navegador. Los navegadores actualizados cuentan con las últimas correcciones de seguridad y son mucho más seguros. Con las computadoras de hoy, esto se ha vuelto mucho más fácil, ya que simplemente puedes habilitar las actualizaciones automáticas del sistema. O para algunos navegadores, simplemente hay que reiniciar cada vez que te indique que hay una nueva actualización. Después de una actualización, busca nuevas características de seguridad de las que puedas beneficiarte.

Advertencias: Los navegadores actuales frecuentemente pueden reconocer ciertos sitios maliciosos diseñados para causarte daño. Si tu navegador te advierte que el sitio web que estás a punto de visitar es peligroso, cierra la pestaña y busca lo que necesitas en un sitio diferente.

Sincronización: Nunca sincronices tu navegador de trabajo con tu navegador personal o con cualquier cuenta personal. La sincronización es cuando permites que los navegadores en diferentes dispositivos se comuniquen entre sí y compartan tu información de navegación, como tu historial, marcadores y contenido guardado.

Contraseñas: Muchos navegadores admiten la opción de guardar tus contraseñas para diferentes sitios. En lugar de almacenar tus contraseñas en el navegador, te recomendamos que utilices un gestor de contraseñas independiente. Los gestores de contraseñas son aplicaciones de seguridad separadas que tienen muchas más características y funciones de seguridad.

Complementos: Los complementos o extensiones son pequeñas piezas de software agregadas a los navegadores que pueden añadir funcionalidad. Sin embargo, cada nuevo complemento que agregues también puede incorporar más vulnerabilidades. Para la computadora de tu trabajo, solo agrega complementos que estén autorizados y aprobados, y al igual que el navegador, mantenlos actualizados. Elimina los complementos que ya no necesites o uses.

Modo incógnito: La mayoría de los navegadores ofrecen una opción de privacidad (también conocida como "modo incógnito"). Esto significa que cuando abres una pestaña del navegador en modo incógnito limitas la información que se recopila sobre ti. Por ejemplo, tu navegador no recopila cookies, no rastrea el historial de navegación y no almacenará ni distribuirá información confidencial tuya.

Chat en vivo: Algunos sitios web ahora ofrecen una función de chat en vivo donde puedes hacer preguntas. Solo participa en estos chats en línea en sitios conocidos y confiables. Además, limita la información que compartes durante una sesión de chat, ya que no tienes idea de quién recopila tu información, qué hacen con ella y a quién se la pueden vender o compartir.

Cuidado con otorgar permisos de control remoto: Algunos sitios web fraudulentos intentarán vulnerar tu computadora publicando una advertencia emergente de seguridad falsa en el navegador diciendo que tu computadora está infectada y presionándote para que inicies una sesión de chat en línea para reparar tu equipo. Luego, te solicitarán con urgencia que les permitas instalar un agente remoto para poder reparar tu computadora. En realidad, tu computadora está bien. En vez de eso, intentan engañarte para que instales software malicioso para poder robar tus contraseñas, tus datos y rastrear toda tu actividad en línea.

Cerrar sesión: Cuando termines de visitar un sitio web, asegúrate de cerrar sesión para eliminar la información confidencial de inicio de sesión y contraseña antes de cerrar el navegador.

Editor invitado

Dean Parsons es el CEO de ICS Defense Force, con más de 20 años de experiencia en ciberdefensa de TI/ICS. También es instructor certificado del SANS para ICS515 y coautor/instructor de ICS418; enseña ciberdefensa activa, respuesta a incidentes, liderazgo y gestión de riesgos para sistemas de control industrial. www.linkedin.com/in/dean-parsons-cybersecurity.

Recursos

Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/
Actualizaciones: https://www.sans.org/security-awareness-training/resources/power-updating/
Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Protegiendo tu huella digital: **https://www.sans.org/newsletters/ouch/privacy/**

Traducido para la comunidad por: Célica Martínez Aponte and Iván Galindo, UNAM-CERT