Herramientas para una navegación más segura

Los navegadores de Internet son el primer paso para poder acceder a Internet y también lo son para aumentar su privacidad en línea y controlar su información personal. Este documento analiza varias de las herramientas que puede utilizar para llevar a cabo una navegación más segura que sea más allá de la configuración de privacidad de los navegadores. Esta información puede contener lenguaje y terminología que nunca ha escuchado y puede parecerle técnico. Tómese su tiempo para leer este documento, hacer preguntas, probar las herramientas y, lo que es más importante, tenga paciencia. No recomendamos productos, pero a través de pruebas e investigaciones descubrimos que las herramientas aquí mencionadas pueden ser útiles para proteger la privacidad de las personas sobrevivientes. Para obtener más información sobre la configuración del navegador que puede utilizar para aumentar su seguridad y privacidad en línea, consulte el recurso Configuración de privacidad del navegador de Safety Net.

Antes de comenzar: Dé prioridad a su seguridad.

El uso de estas opciones de privacidad puede aumentar, tanto su privacidad como su seguridad, especialmente si le preocupa que alguna persona agresora esté monitoreando físicamente la actividad de su dispositivo. También pueden ayudarle a tener más control sobre su información personal al saber cómo se recopilan y almacenan sus datos cuando está en línea. Sin embargo, es posible que estas opciones no le proporcionen la protección contra el espionaje o monitoreo remoto si una persona agresora está usando stalkerware.

No existe una manera "efectiva" para enfrentar el abuso e inquietudes en cuanto a la seguridad en línea, existen únicamente opciones que pueden adaptarse o no a su situación. Lo que funciona para cierta persona puede no funcionar o ser

seguro para usted. Dele siempre prioridad a la seguridad y confíe en sus instintos. Realizar cambios frecuentes alertará a la otra persona. Es posible que le obligue a desbloquear su teléfono o compartir sus contraseñas. La persona podría volverse más agresiva. En algunas situaciones, hacer cambios también podría borrar la evidencia. Los siguientes pasos de seguridad podrían ser de utilidad para usted:

- Utilice un dispositivo más seguro. Si cree que alguien está monitoreando su teléfono o sus cuentas, use un dispositivo diferente (como una computadora de la biblioteca o el teléfono de alguna amistad) y una cuenta a la que la persona no puede acceder (y a la que no ha tenido acceso en el pasado).
- Obtenga más información. Investigar acerca de la violencia, el abuso y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a encontrar otras opciones y servicios locales y también crear un plan para su seguridad. Puede ponerse en contacto con una línea de ayuda nacional para que le puedan remitir a los servicios locales.
- Para obtener más recomendaciones acerca de la seguridad tecnológica para las personas sobrevivientes, consulte el Conjunto de herramientas de recursos para personas sobrevivientes de Safety Net.

¿Por qué debo preocuparme por las empresas que registran mi historial de navegación?

Puede ser inquietante contemplar la preocupación que tendremos al pensar seriamente en lo que hacen las empresas al estar enteradas de nuestro historial de navegación y, además, si podemos siquiera hacer algo al respecto. Sin embargo, cuando las empresas comparten, compran y/o venden nuestros datos, la información llega hasta los intermediarios de datos, que recopilan y comparten información de identificación personal como nombres, domicilio, dirección de correo electrónico, fecha de nacimiento, información de salud y otros datos de consumidores y registros públicos (para obtener más información sobre los intermediarios de datos, consulte la información de recurso de Safety Net). Las

empresas también pueden usar sus datos de navegación para presentarle anuncios directos o hacerle sugerencias mientras usa las redes sociales. Si le preocupa que una persona agresora revise sus cuentas de redes sociales o controle sus dispositivos, estos anuncios y sugerencias pueden compartir información detallada sobre usted. Por ejemplo, podrían mostrar que ha estado buscando ayuda legal, de servicios de salud reproductiva o información sobre una ciudad a la que planea mudarse.

Bloqueo de rastreadores

Existen numerosas extensiones del navegador gratuitas que pueden utilizarse para bloquear rastreadores de terceros (si no tiene la seguridad de lo que esto significa, consulte el siguiente párrafo). Los sitios web usan rastreadores para monitorear la actividad de los usuarios y recopilar sus datos. Una extensión del navegador, que también se denomina "complemento o add-on" en algunos menús del navegador, es como una aplicación, pero para su navegador (si usa varios navegadores, tendrá que agregar la extensión a cada uno por separado).

Los rastreadores de terceros envían información sobre su historial de navegación a otras empresas, además del sitio web que está visitando. Esto les permite realizar un seguimiento de su actividad en Internet y crear un perfil detallado sobre usted a través de su historial de navegación. Pueden recopilar no solo lo que usted consulta en la página web que está visitando, sino también el historial de su navegador, informándole a las empresas en dónde hace clic cuando está en ese sitio y además qué sitios visitó antes y después.

Muchas extensiones de navegador, destinadas a proteger a los usuarios de los rastreadores, se enfocan principalmente en bloquear solo los anuncios (que a menudo, pero no siempre, son la fuente de información de los rastreadores). Una excepción es Privacy Badger, que se enfoca en bloquear el seguimiento de actividades en línea. Su sitio web tiene explicaciones detalladas y fáciles de usar. Desafortunadamente por el momento no funciona con Safari, iOS o Chrome para

Android, pero sí funciona con la mayoría de los demás navegadores de escritorio (Google Chrome, Microsoft Edge, Mozilla Firefox), así como con Firefox para Android (que también puede descargar de forma gratuita).

Si usa un navegador que es incompatible con Privacy Badger y no quiere cambiar, o simplemente quiere obtener la protección adicional de los bloqueadores que usan diferentes métodos, puede probar un bloqueador de anuncios como uBlockOrigin o AdGuard.

Técnicas para separar su identidad en línea en diferentes compartimentos

Los distintos navegadores cuentan con diversos mecanismos a través de los cuales usted puede separar la información de su historial en línea en varios "compartimentos". Por ejemplo, si tiene que usar los mismos dispositivos para la vida personal y laboral, es posible que desee evitar iniciar sesión en los mismos sitios o tener el mismo historial de navegación en cada "compartimento". Por ejemplo, si usa un compartimento para buscar servicios para la planificación de seguridad y también lo usa para navegar por Facebook (o cualquier plataforma de redes sociales), es posible que aparezcan anuncios relacionados con su búsqueda de planificación de seguridad en su *feed* de Facebook. La persona que está monitoreando sus redes sociales puede adivinar, basándose en los anuncios, que está buscando información sobre una posible mudanza a una nueva ciudad específica, soluciones legales, buscar un refugio o cualquier cosa relacionada con su búsqueda. Esto podría suceder incluso en el caso de que usted, por ejemplo, hubiera estado consultando en su computadora mientras que la persona que monitorea sus redes sociales solo tiene acceso a su Facebook a través de su teléfono.

Contenedores del navegador

El navegador Mozilla Firefox tiene una extensión disponible llamada contenedores de cuentas múltiples, que le permite separar su actividad de navegación en compartimentos llamados contenedores. Por ejemplo, podría tener un

contenedor titulado "Personal", otro "Trabajo", otro "Compras" y uno más denominado "Escuela" (la extensión viene con algunos contenedores incorporados, pero puede agregar y eliminar contenedores a su gusto). Si ha iniciado sesión en una cuenta en un contenedor, no iniciará sesión en ningún otro contenedor.

Contenedor de Facebook

Hay otra extensión que se integra con la extensión contenedores de cuentas múltiples mencionada en el párrafo anterior y esta se llama Contenedor de Facebook. Esta extensión gestiona la actividad de Facebook e Instagram, incluido el bloqueo del píxel de seguimiento de Facebook, que se encuentra en aproximadamente un tercio de los sitios web y que la compañía lo utiliza para realizar un seguimiento de su actividad en línea y personalizar anuncios y sugerencias para usted. Al utilizar el contenedor de Facebook, aumenta su privacidad al evitar que la compañía conozca su actividad de búsqueda y navegación fuera de Facebook e Instagram.

Perfiles del navegador

Google Chrome, Microsoft Edge y Mozilla Firefox permiten la creación de múltiples perfiles, o personas compartimentadas, en el mismo dispositivo y navegador. Cada perfil tiene sus propias cookies e historial de navegación por separado. La configuración de diferentes perfiles puede aumentar la privacidad de manera similar que en los contenedores al mantener su historial de navegación de manera separada. Es posible que solo inicie sesión en ciertas cuentas mientras usa un perfil determinado, y puede cerrar la sesión de ese perfil cuando termine de navegar. Esta puede ser una característica útil de navegación más segura, pero es importante no verla como una solución instantánea sin inconvenientes. Si alguien tiene acceso a su dispositivo, aún puede acceder a cualquier perfil en el que haya iniciado sesión, no solo al que esté usando en este momento. Por ejemplo: si usted inició sesión en su cuenta de Google en el trabajo y busca servicios de reubicación, y si también inició sesión en su cuenta de Google

en su teléfono celular o computadora en casa, una persona que está monitoreando la actividad de su navegador en su computadora en casa o su teléfono celular verá que estaba buscando dichos servicios. Al iniciar sesión en un perfil lo iniciará también en otros dispositivos conectados a esa cuenta; lo que podría exponer accidentalmente un perfil que usted estaba usando en un dispositivo más seguro a la persona que está vigilando su actividad en un dispositivo menos seguro.

Navegación encriptada o cifrada

El uso de HTTPS (en lugar de HTTP) hace que sea más difícil para una persona que monitorea su actividad, ya sea una persona agresora, pirata informático o cualquier otro, leer su tráfico de Internet de forma remota, ya que está completamente encriptado. HTTPS Everywhere es una extensión de navegador gratuita que se asegurará de que su comunicación con todos los sitios web utilice HTTPS, siempre que eso sea tecnológicamente posible. Esto es más útil para protegerse contra alguien que está tratando de usar la tecnología para espiar su historial de navegación. Sin embargo, no oculta su actividad en línea cuando alguien puede acceder físicamente a sus dispositivos, o tiene sus contraseñas u otros medios para iniciar sesión en sus cuentas o dispositivos.

Servidores VPN

Cuando accede a un sitio web o envía un correo electrónico, su dirección IP única se comparte y se puede usar para obtener su ubicación aproximada. Un servidor VPN (red privada virtual) oculta su dirección IP de los sitios web que visita y le brinda una dirección IP pública diferente para aumentar la privacidad, además de proporcionar cierto nivel de encriptado para evitar espionaje durante su navegación por Internet. Esto puede protegerle si un sitio web, en el que tiene una cuenta, es pirateado y el pirata informático publica datos del usuario (algo que sucede con relativa frecuencia).

¿Cómo puedo elegir un VPN?

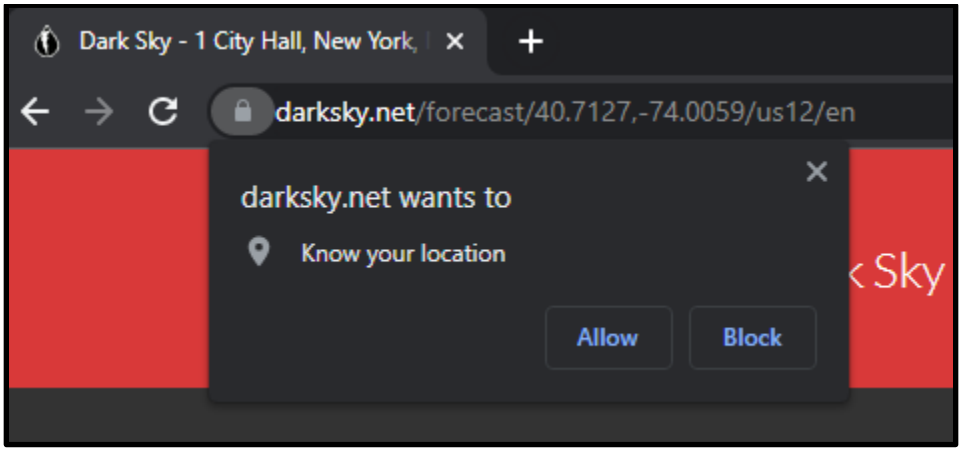
Hay muchas opciones para los servicios de VPN. En general, los servicios de VPN de pago funcionarán mejor que los gratuitos y es menos probable que se conviertan en aplicaciones fraudulentas que puedan aparentar ser un servicio de VPN (aunque tenga en cuenta que existen opciones gratuitas acreditadas, como ProtonVPN). La mayoría de los servicios VPN de pago le permiten agregar más de un dispositivo a un plan, por lo que una opción para ahorrar costos es juntar dinero con algunas amistades y comprar un plan que todos puedan utilizar. Por ejemplo, si un plan le permite proteger hasta seis dispositivos, y tres de ustedes lo compran juntos, cada uno de ustedes puede proteger un teléfono y una computadora portátil y solo tiene que pagar un tercio del costo. En general, los servicios sin registros, que no mantienen registros de su actividad en Internet, como NordVPN, ProtonVPN o Private Internet Access, son más seguros que los servicios que mantienen registros.

VPN para enrutadores y dispositivos inteligentes

Si tiene dispositivos inteligentes (objetos de uso cotidiano que se pueden conectar a Internet y controlar de forma remota) como Google Home o Alexa, un termostato inteligente, un refrigerador inteligente o un timbre con cámara conectado a Internet, estos también tienen direcciones IP. Como se mencionó anteriormente, las direcciones IP indican su ubicación aproximada y las empresas de tecnología a menudo almacenan su dirección IP en los datos de su cuenta. Si le preocupa que una persona acosadora encuentre su dirección IP, también puede ocultar las direcciones IP públicas de estos dispositivos con un servicio VPN. Esto es posible utilizando un enrutador compatible con VPN y protegiéndolo con un servicio VPN, que luego protegerá los dispositivos conectados a él. Muchos servicios de VPN se pueden usar con enrutadores compatibles con VPN, aunque al momento de escribir este artículo, ExpressVPN tiene la reputación de tener la configuración más fácil entre las opciones de VPN con enrutador.

Datos de ubicación precisos: ¿qué son y qué significan para mí?

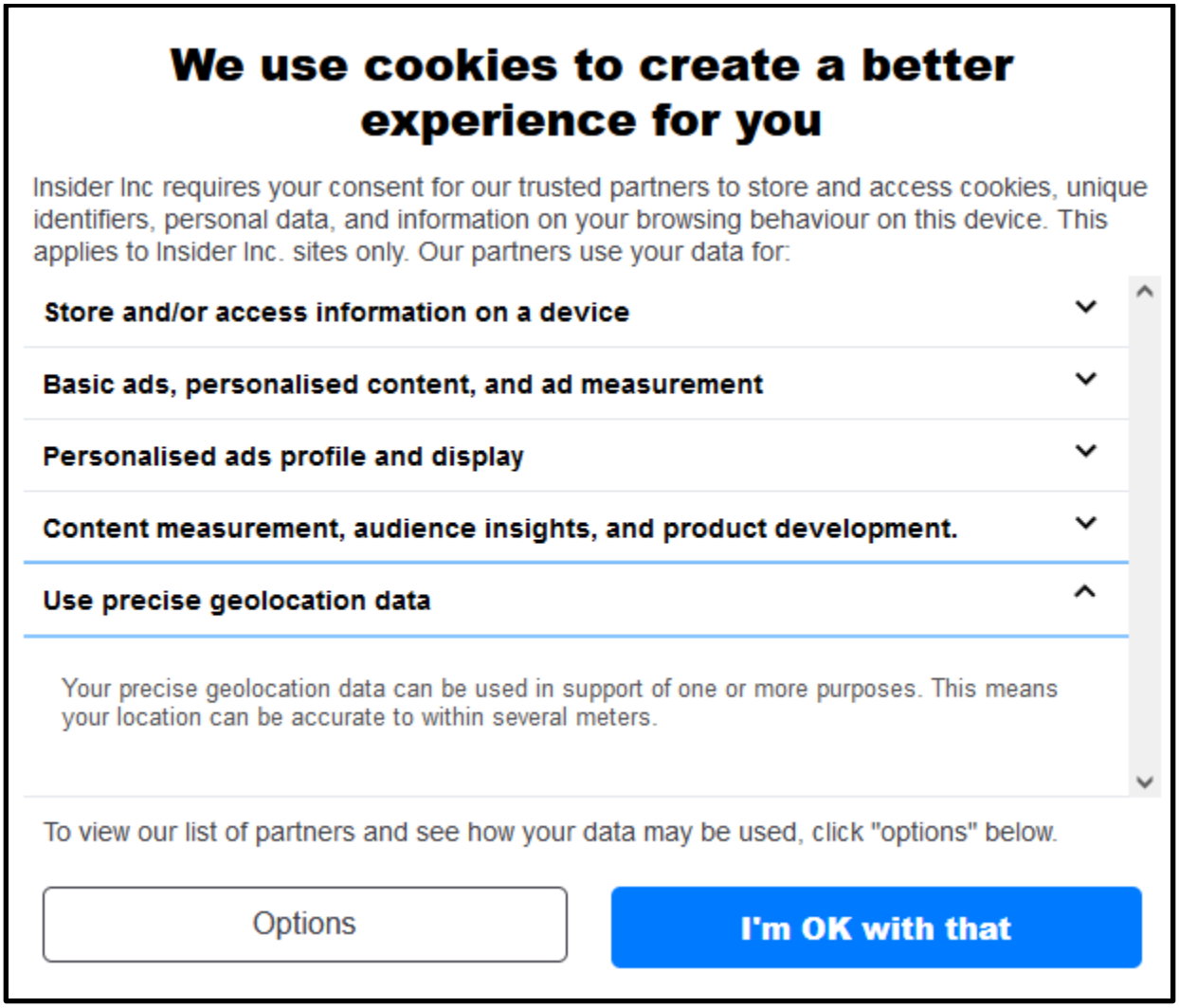
En ocasiones, mientras navega, los sitios web pueden solicitar su permiso para ver su ubicación. Por lo general parece una solicitud emergente (pop-up).



Este tipo de solicitud no pide una dirección IP: los sitios web no tienen que pedir permiso para registrarla. Lo que solicita es información de una ubicación mucho más precisa que la que proporciona su navegador (a menudo a metros de su ubicación real). Los sitios web deben solicitar permiso a los usuarios para leer datos de ubicación tan precisos.

En ocasiones la solicitud aparece de una manera diferente, como en el siguiente ejemplo que damos a continuación. En este caso es parte de la solicitud general del sitio web, usar sus datos para que puedan recopilar, almacenar y, en ocasiones, vender información sobre usted. A menudo, por privacidad, es conveniente rechazar estas solicitudes tanto como sea posible, pero debido a que muchos sitios web lo hacen más difícil o lento, es comprensible que muchas personas hagan clic en el botón "Aceptar todo". Cualquier sitio web determinado puede o no solicitar datos de geolocalización precisos, pero los usuarios normalmente no ven los tipos de permisos que están otorgando si hacen clic en "Aceptar todo", sin hacer clic para averiguar la información que pueda estar disponible para consultarla primero. Por ejemplo, es posible que muchas personas que visitan el sitio del que se tomó esta captura de pantalla (un sitio de noticias), si no hacen clic en un botón para ver esta información antes de hacer

clic en "Aceptar todo", no se den cuenta de que podrían estar dando permiso al sitio para registrar exactamente dónde están.



Denegar permisos tanto como sea posible es una forma de controlar quién almacena o comparte su ubicación precisa. Sin embargo, puede haber ocasiones en los que desee utilizar las funciones del sitio web basadas en la ubicación; por ejemplo, cuando desee ver rápidamente las noticias locales o el clima, y no desea que el sitio almacene su ubicación precisa, pero no importa si almacena el área en general. Las herramientas como la extensión del navegador Location Guard se pueden usar estratégicamente para aumentar la privacidad de la ubicación. Location Guard le permite establecer una ubicación fija para usted, por lo que si

desea otorgar permiso a un sitio meteorológico para conocer el área general pero no su ubicación precisa, puede fijar su ubicación en la ciudad más cercana.

Información adicional.

Estas herramientas no son el único medio para aumentar su privacidad mientras navega. Los navegadores también tienen muchas configuraciones de privacidad integradas. Para obtener información sobre la configuración del navegador y cómo puede usarla estratégicamente, consulte nuestro recurso llamado "configuración de privacidad del navegador".

Financiado por la subvención US DOJ-OVW #15JOVW-21-GK-02216-MUMU. Las opiniones, hallazgos y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para consultar la última versión de este y otros materiales.