Dispositivos domésticos inteligentes: Privacidad y seguridad de las personas sobrevivientes para el hogar "inteligente" (Internet de las cosas)

Muchos dispositivos, como timbres, termostatos, televisores y altavoces, están ahora conectados al Internet. Esto puede proporcionar acceso a entretenimiento o información sin necesidad de utilizar un teléfono o computadora, y puede permitir que los dispositivos en el hogar sean controlados remotamente. Estos dispositivos suelen denominarse "inteligentes", como los altavoces o televisores inteligentes. También se conocen como dispositivos por Internet de las Cosas (IoT por sus siglas en inglés).

Aunque los dispositivos conectados a Internet pueden resultar cómodos y aumentar el acceso de las personas con discapacidad, también pueden ser utilizados indebidamente por personas agresoras. Algunos de estos dispositivos pueden utilizarse para vigilar lo que ocurre a distancia o para controlar funciones del hogar como la calefacción, la alarma, las cerraduras y las luces.

Este recurso está dirigido a las personas sobrevivientes que quieren entender la forma en que esta tecnología puede ser utilizada en su contra y explorar las opciones para aumentar la privacidad y la seguridad.

Para obtener más información lea las evidencias de la IoT y las cuestiones legales (escrito para profesionales y abogados).

La seguridad es lo primero. Antes de tomar las siguientes medidas, piense en su seguridad. Algunas personas pueden intensificar su comportamiento abusivo cuando los dispositivos o las cuentas están protegidos, o cuando se

interrumpe la supervisión. Hable con una persona intercesora sobre la planificación de la seguridad.

Confíe en sus instintos. Si parece que alguien sabe demasiado sobre usted, es posible que esté vigilando sus dispositivos, accediendo a sus cuentas en línea, rastreando su ubicación o recopilando información sobre usted en Internet. Si sospecha que alguien le está vigilando, considere la posibilidad de utilizar otro teléfono o dispositivo al que nunca haya tenido acceso, como el teléfono de una amistad o una computadora de la biblioteca, la escuela o el trabajo. Para obtener más información, lea la seguridad telefónica y la privacidad.

Obtenga más información. Enfrentarse a la violencia, los malos tratos y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a descubrir opciones y recursos locales y a crear un plan para su seguridad. Puede llamar a un teléfono de ayuda nacional para que le pongan en contacto con los recursos locales.

Mapa de dispositivos inteligentes en su hogar

El primer paso es intentar crear una lista de todos los dispositivos conectados en su casa. Esto puede ser útil si está tratando de aumentar su privacidad o averiguar si una persona agresora puede tener acceso a un dispositivo. Por ejemplo, si ha comentado algo que usted ha hecho o dicho cuando no estaba allí. A lo mejor podría estar ocurriendo algo inexplicable en su casa, como que suba o baje la calefacción cuando no ha cambiado el termostato, que se enciendan o apaguen las luces, que cambie el volumen del televisor o que se activen las alarmas. Tenga en cuenta que su teléfono también podría proporcionar a la otra persona mucho acceso e información, y podría ser una explicación más sencilla de lo que está

ocurriendo. Para obtener más información lea seguridad telefónica y privacidad.

Importante: Antes de emprender cualquier acción para cambiar el acceso de otra persona o retirar los dispositivos, es aconsejable que considere si siente la seguridad de hacerlo y si desea documentar lo que ha estado sucediendo. Para obtener ayuda, hable con una persona intercesora.

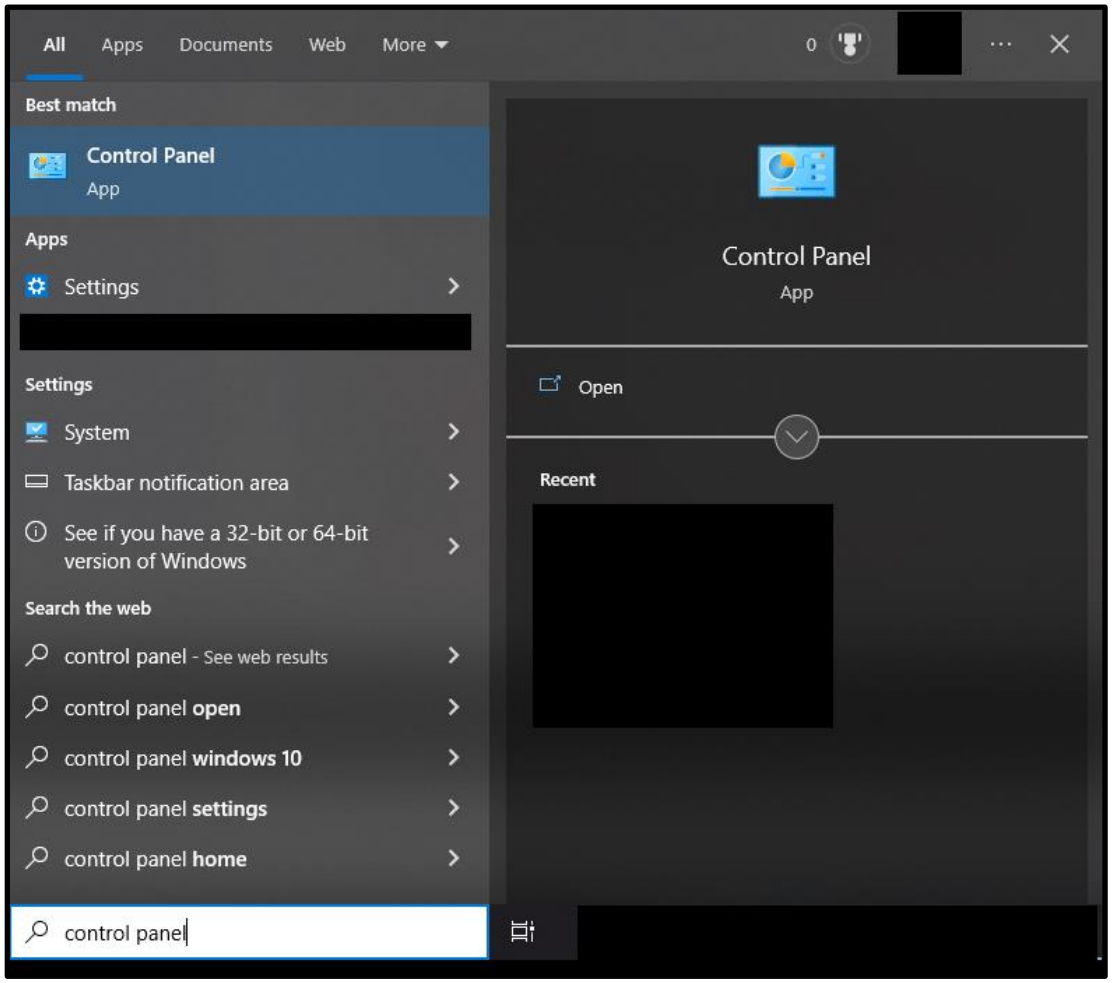
Algunas cosas, como televisores, timbres y termostatos, pueden ser más fáciles de identificar. Si usted u otra persona pueden cambiar los ajustes o manejar un dispositivo a través de una aplicación, entonces es casi seguro que está conectado a Internet. Cosas como refrigeradores, detectores de humo o enchufes pueden ser menos obvias. Si tiene dudas, puede intentar buscar el dispositivo en Internet, utilizando la marca y el nombre o número del modelo para ver si se comercializa como "inteligente" o conectado. Recuerde que si le preocupa que la otra persona esté vigilando su teléfono o computadora, puede utilizar un dispositivo al que no tenga acceso. Otros dispositivos conectados, como las cámaras, podrían estar ocultos y requerir más trabajo o la ayuda de un experto para encontrarlos.

Cómo crear una lista de dispositivos con el router
Puede disponer de la información de inicio de sesión del router inalámbrico doméstico (el dispositivo que proporciona acceso WiFi doméstico), otra opción para crear la lista de dispositivos es iniciar sesión en la cuenta del router para ver la lista de dispositivos conectados.

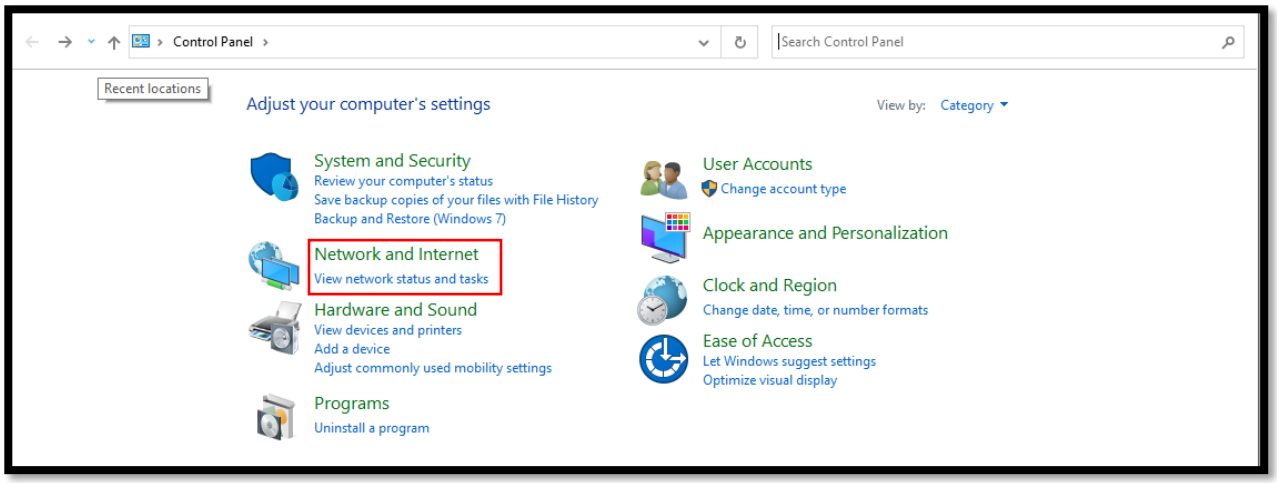
Antes de poder conectarse a su router, necesitará conocer su dirección IP. En muchos casos, es 192.168.1.1. Si utiliza un Mac, un teléfono Android o un iPhone, puede seguir las instrucciones que aparecen aquí (su teléfono deberá estar conectado a su red inalámbrica para que esto funcione). Si

utiliza un PC, puede encontrarlo siguiendo las instrucciones que aparecen a continuación. Si ya conoce la dirección IP de su router, o sabe cómo encontrarla por su cuenta, puede saltar al párrafo que comienza de la siguiente manera: "Para realizar el siguiente paso, necesitará la información de inicio de sesión de su proveedor de servicios de Internet (ISP)".

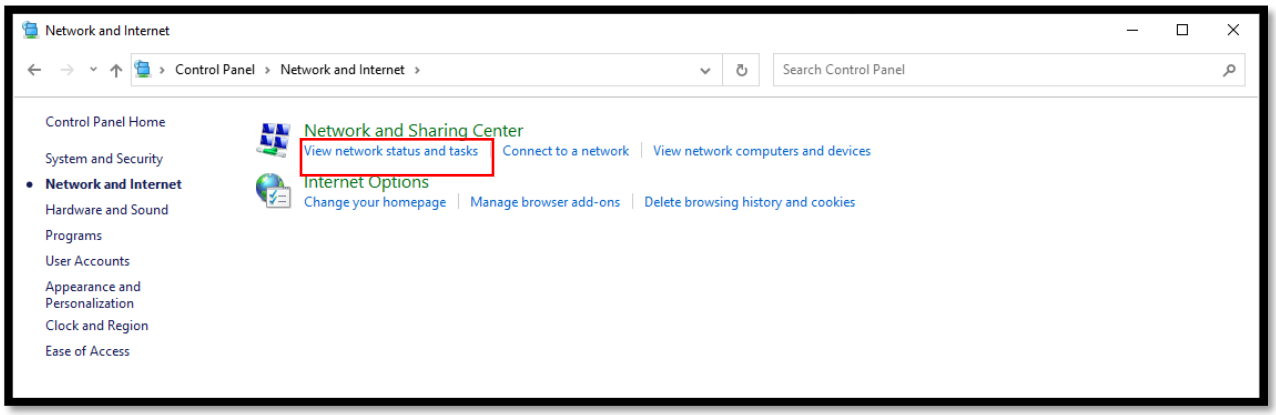
1. En la parte inferior izquierda o central de su barra de tareas, escriba "Panel de control" en el menú de Inicio.



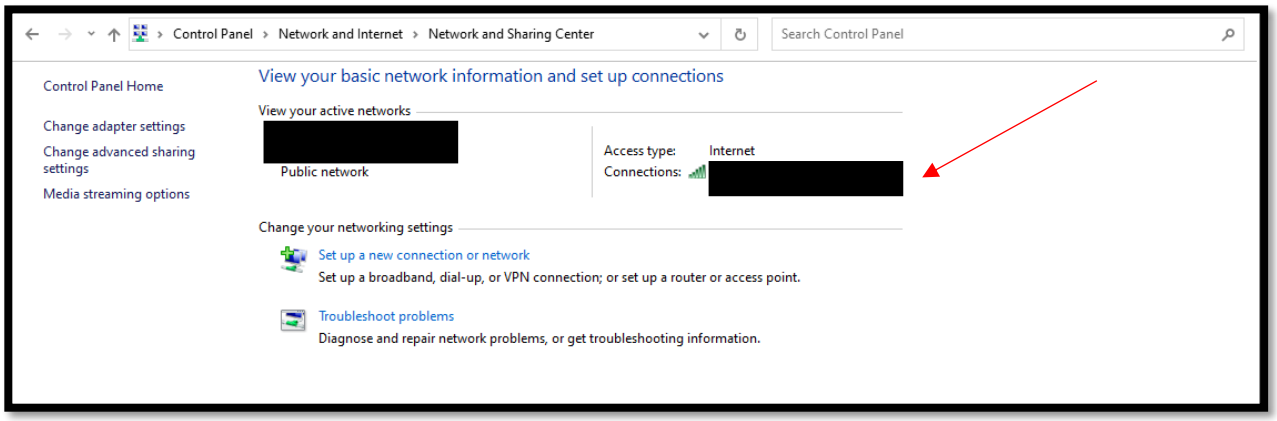
2. Haga clic en Red e Internet.



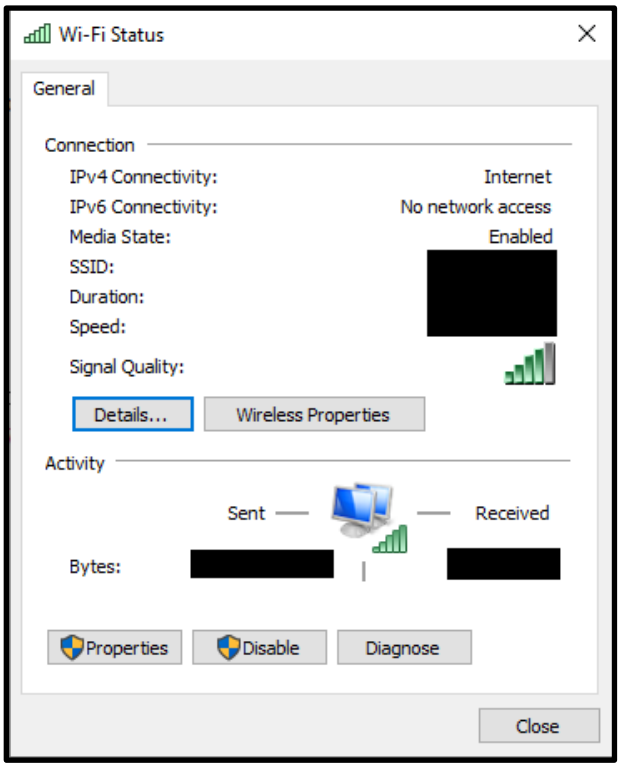
3. Haga clic en “Ver estado y tareas de la red”.

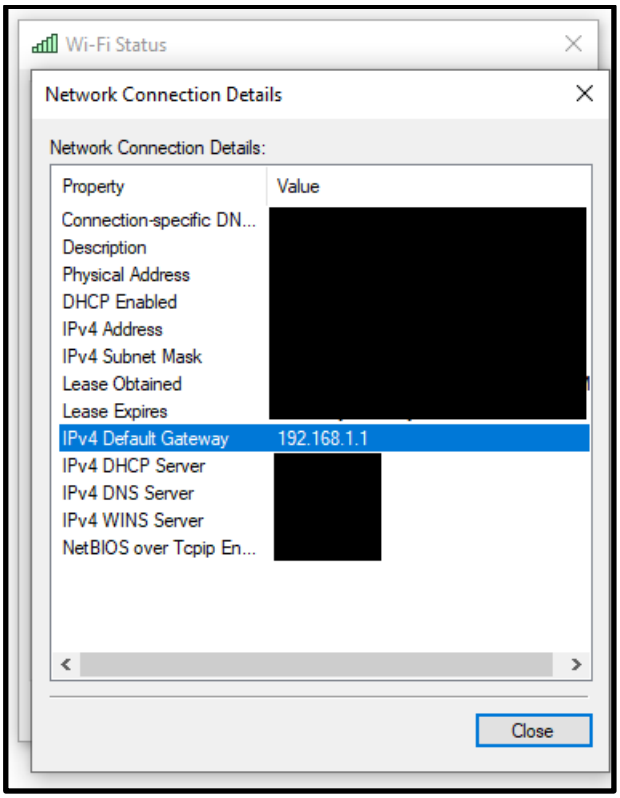


4. Seleccione su conexión WiFi (indicada por la flecha roja de abajo).



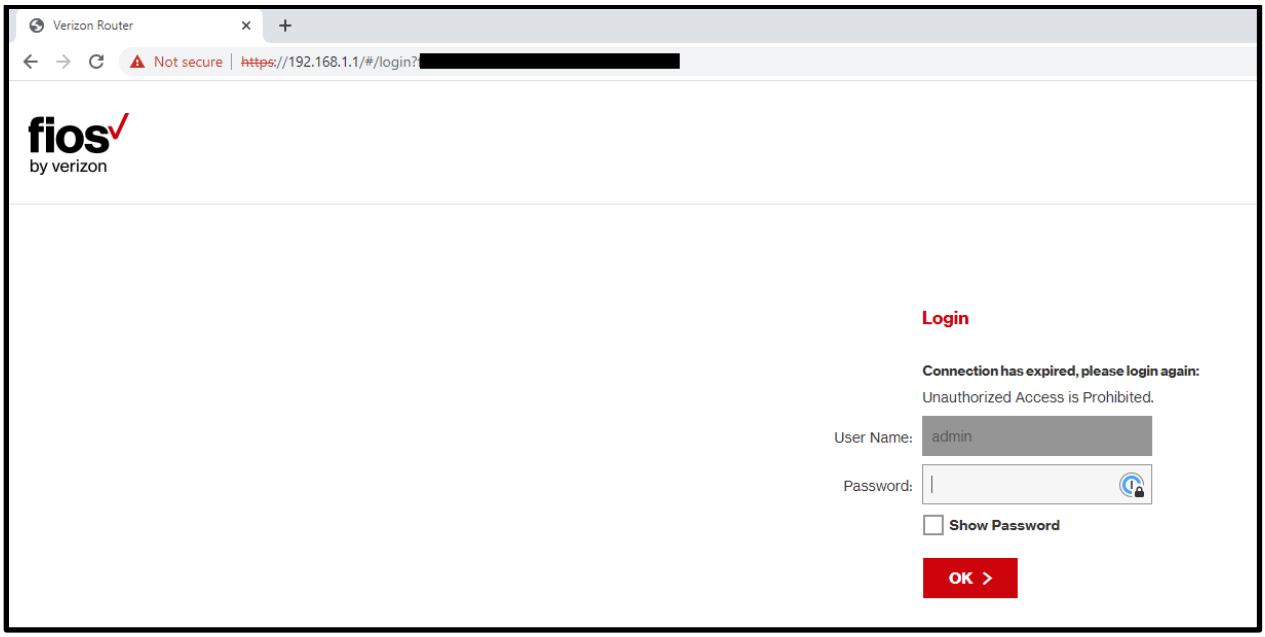
5. Una vez que haya seleccionado su conexión WiFi, verá una pantalla denominada "Estado WiFi" (abajo a la izquierda). Haga clic en el botón "Detalles", y verá una pantalla llamada "Detalles de la conexión de red" (abajo a la derecha), que tiene una lista de "Propiedades" y una lista de "Valores". La dirección IP de su router es el valor de la propiedad "IPv4 Default Gateway". Una vez que haya hecho esto, puede pasar a los siguientes pasos - conectarse a su router.



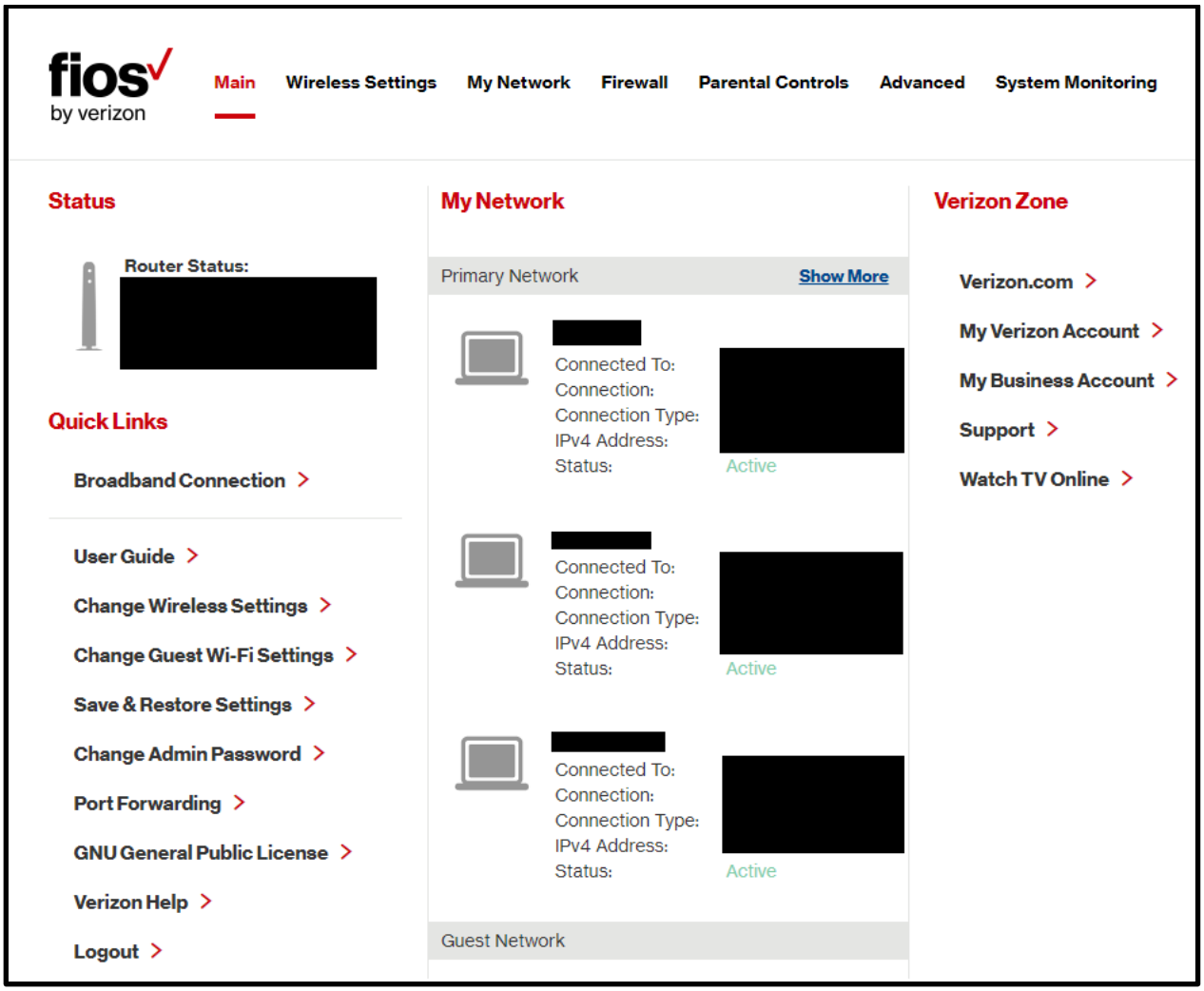


Para realizar el siguiente paso, necesitará la información de inicio de sesión de su proveedor de servicios de Internet (ISP). Una vez que haya conseguido esta información de inicio de sesión:

1. Vaya a la dirección IP de su router en su navegador, escribiendo la dirección IP del router en la barra de direcciones, y conéctese.



Esto le proporcionará una lista de dispositivos conectados a su red WiFi, como se muestra en la siguiente imagen en "Mi red".



2. Haga clic en un dispositivo para ver más detalles sobre él. En la imagen de arriba, hemos ocultado detalles sobre el dispositivo por motivos de privacidad, pero podrá verlos. La dirección MAC le permite buscar el fabricante del dispositivo, y el nombre del dispositivo también puede darle pistas sobre cuál es, lo que le ayudará a crear su lista.

Uso de la lista de dispositivos

Una vez que tenga una lista de dispositivos, añada información sobre quién compró o configuró cada dispositivo. Si una persona agresora añadió estos aparatos a su casa, aunque ahora no viva en ella, es posible que haya

configurado las cuentas para poder vigilar o controlar los dispositivos a distancia. Incluso si usted compró los dispositivos, pero la otra persona le ayudó a configurarlos o alguna vez compartió el acceso, es posible que aún pueda hacerlo.

Para cada dispositivo, busque información sobre cómo puede manejar o cambiar los ajustes. ¿Hay un panel de visualización a través del cual puede cambiar las opciones, o necesita una aplicación o una dirección web para realizar los cambios? Si no encuentra información sobre cómo realizar cambios, puede buscar en Internet la marca y el modelo. De momento, simplemente tome nota de estos ajustes. A continuación hablaremos de otras consideraciones antes de realizar cambios.

Por último, añada información sobre lo que la otra persona podría hacer o averiguar sobre usted o sus actividades a través del dispositivo. ¿Captura vídeo o audio? ¿Crea un registro de actividades? ¿Puede anular o cambiar a distancia los ajustes programados? Una vez más, puede que tenga que utilizar Internet para buscar información sobre el dispositivo.

Si hay dispositivos conectados a su router que no puede identificar, puede intentar buscar el dispositivo en Internet. Sin embargo, dependiendo del dispositivo esto puede ser útil o no. También puede buscar la dirección MAC, que le proporcionará información sobre el fabricante, lo que a su vez podría darle pistas sobre cuál es el dispositivo. Si siente que es seguro hacerlo, podría desconectarlo. Si resulta ser un dispositivo que quería, puede volver a conectarlo.

Estrategias para aumentar la privacidad y la seguridad

Ahora que ya tiene una lista de dispositivos conectados, puede elegir qué pasos seguir a continuación. Si desea documentar lo que está sucediendo,

ya sea para sus propios registros o para compartirlo con otra persona, sería bueno hacerlo antes de tomar cualquier medida para cambiar la configuración, desconectar el acceso o eliminar dispositivos. Dependiendo del dispositivo, puede tomar fotos del dispositivo tal y como lo encontró, hacer capturas de pantalla de aplicaciones o información que investigue sobre los dispositivos en línea, o tomar notas sobre lo que ha encontrado. También puede ser útil tomar notas sobre cualquier cosa que la otra persona haya hecho con el dispositivo, o sobre cualquier cosa extraña que usted haya notado en la casa, incluyendo la fecha y la hora. Para obtener más información, lea cómo documentar los malos tratos.

Puede tomar medidas para impedir que la otra persona tenga acceso a los dispositivos, cambiar otros ajustes o retirarlos por completo. En algunos casos, las personas agresoras intensifican el abuso cuando se corta el acceso o se realizan cambios. Puede hablar con una persona intercesora para elaborar un plan de seguridad. También puede optar por dejar la configuración o los dispositivos durante un tiempo para reunir evidencias o porque eso le proporciona más seguridad.

La forma de eliminar el acceso o cambiar la configuración variará en función del dispositivo. Si hay una pantalla, es posible que pueda utilizarla para realizar cambios. Si no, es posible que tenga que utilizar una aplicación o un sitio web. En algunos casos, es posible que tenga que ponerse en contacto con la empresa que fabricó el dispositivo para cambiar la cuenta.

1. En primer lugar, averigüe quién tiene acceso al dispositivo, la aplicación o la cuenta. Si la persona agresora todavía tiene acceso, cualquier cambio que haga podría anularse, o la persona podría intensificar su abuso. Si considera que es seguro hacerlo, elimine el acceso cerrando la sesión de otros dispositivos o eliminando los usuarios.

2. A continuación, cambie las contraseñas y añada opciones de seguridad como la autenticación multifactorial. Para obtener más información, lea contraseñas y autenticación multifactorial.
3. Por último, si lo desea, realice cambios en la configuración del dispositivo.

Si no es capaz de recuperar el control del dispositivo y no le parece seguro tenerlo funcionando en su casa, puede considerar desconectar el *feed* o retirar el dispositivo por completo. Otra posibilidad, si no reconoce un dispositivo, es desconectarlo de la red WiFi conectándose al router como se describe en la sección anterior, desconectándolo a través del panel que aparece al conectarse y cambiando después la contraseña de la red WiFi para que el dispositivo sólo pueda volver a conectarlo alguien que conozca la nueva contraseña. Tenga en cuenta que si hace esto, una persona agresora puede darse cuenta de lo que ha hecho - confíe en sus instintos para saber lo que es seguro.

Dispositivos inteligentes y direcciones IP

Si utiliza un dispositivo, como un teléfono, para crear cuentas o conectarse a ellas, es posible que la dirección IP del dispositivo se haga pública a través de una filtración de datos (cuando alguien roba y vende o publica datos de una empresa), y una persona agresora o acechadora podría utilizar esta información para averiguar dónde vive usted. Una dirección IP puede utilizarse normalmente para rastrear el dispositivo hasta un área metropolitana o una zona rural de tamaño similar. Además, si alguien tiene acceso a una de sus principales cuentas en la nube, como su cuenta de Google o iCloud, es posible que pueda ver las direcciones IP de todos los dispositivos que se hayan conectado a esa cuenta. Si le preocupa que alguien le localice de esta forma, puede ocultar las direcciones IP de sus dispositivos a través de un servicio VPN, que envía su actividad en Internet

a través de una de las computadoras del servicio y hace que para el público (fuera de su red doméstica), su dirección IP parezca ser la dirección de esa computadora. De este modo, la dirección IP asociada a sus cuentas no será la suya y, si se produce una filtración de datos, su dirección IP real no se robará ni se publicará.

Puede proteger las direcciones IP públicas de dispositivos individuales a través de un servicio VPN como Proton VPN, NordVPN o Private Internet Access. Las versiones de pago de estos servicios le permiten proteger varios dispositivos a la vez, y si no puede permitirse pagar un servicio VPN por su cuenta, puede reunir dinero con amistades (por ejemplo, si usted y dos amistades de confianza reúnen dinero para un servicio VPN que le permite proteger hasta seis dispositivos con la misma cuenta, cada uno puede proteger dos dispositivos). Si quiere proteger las direcciones IP públicas de muchos dispositivos, puede añadir un servicio VPN a muchos tipos de routers, que protegerán la dirección IP pública de todos los dispositivos conectados a su red. Muchos servicios VPN admiten esta opción, pero su configuración puede requerir ciertos conocimientos técnicos. En el momento de escribir este artículo, la protección Express VPN para routers es conocida por ser relativamente fácil de usar.

Resumen

Controlar nuestra privacidad puede ser un reto, puesto que gran parte de nuestra vida es digital y está conectada. Desgraciadamente, las personas agresoras suelen abusar de los dispositivos conectados como táctica para acosar, controlar o vigilar. Si usted sufre este tipo de abuso y necesita más ayuda, póngase en contacto con una línea de atención telefónica o con un programa local contra la violencia doméstica. Si algo de este contenido es difícil de entender, puede discutirlo con una persona intercesora que podrá

ponerse en contacto con el Safety Net Project de NNEDV para obtener ayuda.

 Financiado por US DOJ-OVW Grant No. 15JOVW-21-GK-02216-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del DOJ.

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