# Stalkerware: Vigilancia telefónica y seguridad para las personas sobrevivientes

## ¿Qué son los programas de acoso (Stalkerware)?

El stalkerware se refiere a las herramientas – aplicaciones (apps), programas de software y dispositivos – que permiten que otra persona vigile secretamente la actividad de su teléfono.

El stalkerware puede controlar casi todo lo que usted hace en su teléfono, incluyendo las fotos y los vídeos que toma, los sitios web que visita, los mensajes que envía y recibe, su historial de llamadas y su ubicación. El programa stalkerware puede permitir a alguien encender la cámara web o el micrófono, hacer capturas de pantalla, ver la actividad en aplicaciones de terceros (como Snapchat o WhatsApp) e interceptar, reenviar o grabar llamadas telefónicas.

Casi todos los programas de stalkerware telefónico requiere que la persona tenga acceso físico al dispositivo para ser instalado. Una vez instalado, el programa funciona de forma sigilosa, sin ninguna notificación o actividad característica y son difíciles de detectar o eliminar. Para acceder a la actividad de su teléfono, la persona que controla el dispositivo ingresa a un sitio web o aplicación en un dispositivo diferente. También puede recibir notificaciones de alguna actividad, como copias de mensajes de texto o una alerta que indica que usted está en una llamada para poder unirse en secreto y escuchar.

## ¿Cómo puedo saber si hay un programa de stalkerware en mi dispositivo?

Podría ser difícil detectar un programa de stalkerware. Algunos indicios podrían ser que su batería se agote rápidamente, que el dispositivo se apague y se encienda, o una rápida elevación en el uso de datos. Sin embargo, la señal más común de que su actividad está siendo controlada será el comportamiento sospechoso de la otra persona. Por ejemplo, la persona podría saber demasiado sobre sus actividades telefónicas. Confíe en sus instintos, busque señales y para asegurarse, es posible que una persona profesional capacitada tenga que revisar el dispositivo.

**Responder a un programa de stalkerware**

**La seguridad es lo primero**. Antes de realizar alguna acción para encontrar o eliminar el programa de stalkerware, es importante considerar su seguridad. Algunas personas pueden intensificar su comportamiento abusivo cuando se enteran que el stalkerware se ha eliminado. Hable con una persona intercesora acerca de un plan de seguridad.

Si sospecha de la existencia de un programa de stalkerware, eso quiere decir que una persona podría estar viendo lo que usted hace en su teléfono. Para realizar las llamadas o una actividad en línea que requiera mayor privacidad, utilice un teléfono u otro dispositivo que no esté siendo vigilado. Puede ser el teléfono de una amistad o la computadora de una biblioteca pública, de la escuela o del trabajo.

**Recolección de evidencia** del programa de stalkerware. Puede tomar notas sobre lo que le está sucediendo. Además, la policía o un perito forense pueden buscar evidencia. Obtenga más información sobre este tema aquí, Evidencia de stalkerware .

**Eliminar un programa de stalkerware.** En la mayoría de los casos, un reinicio total del dispositivo podría eliminar el programa de stalkerware. Sin embargo, cuando se vuelven a instalar las aplicaciones o archivos desde una copia de seguridad podría volver a descargarse. Para eliminar cualquier riesgo de que el programa stalkerware se reinstale, además de hacer el reinicio total para que inicie el dispositivo desde cero, también podría crear una nueva cuenta de iCloud o Google.

**Cómo prevenir el programa de stalkerware.**

**Considere el acceso.** Tenga cuidado si alguien quiere actualizar o utilizar su teléfono. La instalación del programa de stalkerware es sencilla y rápida. Confíe en sus instintos.  Desconfíe si la persona agresora le regala un teléfono inteligente o una tableta a usted o a sus hijos.

**Actualice las cuentas.** Cambie las contraseñas y configure la autenticación de dos factores. Lea más sobre Seguridad de las Contraseñas.

**Bloquee su teléfono.** Debido a que la mayoría de los programas de stalkerware requieren el acceso físico al teléfono para instalarlo, para minimizar el riesgo, configure una contraseña en su teléfono (y no la comparta). Muchos dispositivos permiten elegir entre una contraseña numérica, una figura o patrón, la huella digital y otras funciones de seguridad. Obtenga más información aquí, Consejos de seguridad para su teléfono.

**Utilice una protección antivirus y software anti-stalkerware.** Descargue aplicaciones de seguridad en su teléfono; estas aplicaciones pueden ayudar a evitar que se instale un programa stalkerware y pueden escanear su teléfono en búsqueda de aplicaciones de stalkerware o malware.

**Use las funciones de seguridad.** Revise las funciones de seguridad en su configuración para saber qué es lo que está disponible en sus dispositivos. Los teléfonos Android tienen una configuración que permite la instalación desde "fuentes desconocidas"; asegúrese de que esté desactivada. Además, instale siempre las últimas actualizaciones para su teléfono y sus aplicaciones. Si no lo hace, puede hacer que su teléfono sea más vulnerable a los problemas de seguridad y privacidad.

**No realice *rooteo* (para Android) o el jailbreak (para iPhone) en su teléfono.** *Rootear* o hacer *jailbreak* a un dispositivo significa eliminar las limitaciones del sistema operativo para permitir instalaciones de terceros (aquellas que no están disponibles en las tiendas de aplicaciones). Esto afecta a las funciones de seguridad integradas diseñadas para proteger el dispositivo y lo hace vulnerable. Muchas de las funciones del programa de stalkerware más invasivas no funcionan a menos que se desactiven las protecciones establecidas por el fabricante. En los teléfonos iPhone, la mayoría de los programas de stalkerware no pueden ser instalados salvo que el dispositivo tenga jailbreak. Un teléfono con *rooteo* o con

jailbreak será más vulnerable a los virus y programas malware o maliciosos y facilitará la instalación de programas de stalkerware.

**Cuando no se trata de un programa de stalkerware.**
Existen muchos otros métodos que alguna persona podría emplear para acceder a la información contenida en su teléfono o para enterarse de sus actividades sin tener que instalar un programa de stalkerware. Si la persona agresora tiene acceso físico al teléfono o a sus cuentas en la nube, es posible que no necesite instalar un programa de stalkerware para vigilarle.

A veces, una persona agresora reúne información sobre usted a través de sus amistades y familiares. Para que usted pueda detectar las posibilidades, busque patrones estudiando lo que sabe la persona y piense de dónde pudo haber obtenido esa información. Una persona intercesora puede ayudarle a descubrir lo que está sucediendo y planificar los siguientes pasos a seguir.

 Financiado por la Oficina Federal de Víctimas de Delitos del Departamento de Justicia (OVW, DOJ, por sus siglas en inglés). Subvención n.º. 15JOVW-21-GK-02255-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente la opinión de DOJ. Actualizamos nuestros materiales con

frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.