Descripción general de los programa espía (spyware) y de acoso

ALERTA DE SEGURIDAD: Los programa espía (spyware) y de acoso han facilitado que los/las delincuentes acosen, rastreen, controlen y hostiguen a víctimas con una facilidad sin precedente. Los/las agresores/as, acosadores/as y demás delincuentes pueden utilizar los programa espía (spyware) para controlar secretamente lo que hace con su dispositivo móvil, como un teléfono inteligente o una tableta. Si usted sospecha que está siendo acechado/a o vigilado/a:

- Tenga en consideración que todo lo que haga en el dispositivo puede ser visto por el/la agresor/a, incluyendo tratar de buscar el programa espía (spyware) o buscar si pidió ayuda.
- Utilice un dispositivo que la persona agresora no utilice.
- Confíe en sus instintos. Busque patrones que le ayuden a descifrar qué está haciendo la persona.

¿Qué es un programa espía (spyware) o programa de acoso (stalkerware)?

Un programa espía (spyware) o un programa de acoso es una aplicación, software o dispositivo que permite que otra persona (como un/a agresor/a) controle secretamente y registre la actividad del teléfono o la computadora de otra persona. El término "stalkerware" (programa de acoso) es un término más reciente que refiere al uso indebido invasivo, intrusivo y peligroso de estas herramientas. Un programa espía (spyware) activa un control a distancia que facilita la vigilancia, el acoso, el maltrato, el acecho y/o la violencia, sin el consentimiento del/de la usuario/a. El software puede estar "escondido" en el dispositivo, y no dar aviso específico ni notificaciones constantes de que el programa está instalado. Un programa espía (spyware) o de acoso puede ser instalado en una computadora o teléfono inteligente. Suelen ser difíciles de detectar y eliminar.

¿Son legales los programas espía o de acoso?

En general, es ilegal controlar o vigilar el dispositivo de otra persona sin su permiso o conocimiento. Esto aplica tanto a los comportamientos personales como a través del empleo de la tecnología. Dependiendo de la circunstancia y del contexto, instalar programas espía (spyware) puede violar una amplia cantidad de leyes que van desde el acecho o el acoso hasta el uso no autorizado de una computadora, la instalación de micrófonos y las escuchas a escondidas. Para obtener más información acerca de las leyes relacionadas con la vigilancia electrónica, visite WomensLaw.org.

¿Qué puedo hacer si tengo sospechas sobre un programa espía?

Si sospecha que tiene un programa espía (spyware) en su(s) dispositivo(s), lea los recursos a continuación y conozca más acerca de los programa espía (spyware), las señales para determinar si está instalado, las opciones para eliminarlo y cómo documentar lo que sucede mientras se mantiene seguro/a. También puede considerar consultar a la policía sobre qué pueden hacer para investigar el programa espía (spyware) en su dispositivo.

Sea consciente de que todo lo que haga en el dispositivo con el programa espía (spyware) instalado puede ser revelado a la persona que lo controla, así que considere utilizar un dispositivo que no esté siendo controlado. También considere otras formas en las que alguien podría conocer las actividades de su dispositivo, como tener acceso directo al dispositivo, a sus cuentas en línea e incluso preguntando a personas que tengan información sobre usted.

- Programas Espía (spyware) y de Acoso: Vigilancia de Dispositivos y Seguridad para Sobrevivientes
- Programas Espía (spyware) y de Acoso: Vigilancia de Computadoras y Seguridad para Sobrevivientes
- Consejos de Documentación para Sobrevivientes
- 12 Consejos para la Seguridad y la Privacidad de su Teléfono Celular
- Consejos para la Seguridad de su Computadora Portátil (en Inglés)

- Programas Espía (spyware) en la Telefonía Celular: Serie de Recolección de Evidencia (para profesionales del sistema judicial)

 Financiado por la Oficina de Víctimas de Crímenes del Departamento de Justicia (OVW, DOJ, por sus siglas en inglés) de los Estados Unidos. Subvención n.º 2016-TA-AX-K069. Las opiniones, hallazgos, conclusiones o recomendaciones aquí expresados pertenecen a el/la autor/a y no necesariamente reflejan los puntos de vista del Departamento de Justicia (DOJ, por sus siglas en inglés).

Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.