Guía de Teléfonos para Sobrevivientes: Aumentar la Privacidad y Responder al Maltrato

Nuestros teléfonos inteligentes almacenan información sensible, rastrean nuestra ubicación y son la manera en la que accedemos a nuestras cuentas personales. Es increíblemente importante que los/las sobrevivientes de maltrato tengan las herramientas para mejorar su privacidad y responder al maltrato tecnológico. Estos son algunos pasos y consideraciones para los/las sobrevivientes.

Priorice la Seguridad

Use un dispositivo más seguro. Si usted piensa que alguien está controlando su teléfono, use un dispositivo distinto al que la persona no pueda acceder (y al que la persona no haya tenido acceso en el pasado) como una computadora en la biblioteca o el teléfono de un/a amigo/a.

Obtener más Información. Vivir situaciones de violencia, de maltrato y de acecho puede resultar complicado y peligroso. Los/as intercesores/as de víctimas en su área pueden informarlo/a acerca de las opciones y recursos locales y ayudarlo/a a crear un plan para su seguridad. Puede contactar a la línea de ayuda nacional para conectarse con los recursos locales.

Parte 1: ¿Su Teléfono se Está Usando en su Contra?

Lamentablemente, las conversaciones y la información contenida en los teléfonos se puede usar indebidamente para perseguir, controlar, acechar o intimidar. *Confíe en sus instintos.* Si usted sospecha que alguien está controlando su teléfono, pero no está seguro/a, puede buscar más información sobre cómo descubrir lo que está sucediendo. Mientras tanto, aquí hay algunas preguntas a considerar.

¿Hay un patrón?

¿La persona parece saber todo (con quién habló, el contenido de conversaciones que tuvo por teléfono o cerca de su teléfono, mensajes de texto que escribió o recibió, a dónde va) o solo parte de esa información? Reducir las posibilidades de las maneras en que se rastrean sus actividades le ayudará a determinar cómo usted está siendo controlado/a y qué estrategias debería considerar.

¿Qué parece saber la persona?

Si la persona sabe que usted tuvo una conversación, pero no sabe específicamente lo que se dijo, escribió o compartió, esa persona podría observar el registro de llamadas, los expedientes de facturación u otra clase de información de cuenta. También podría haber hablado con la persona con la que usted se estuvo comunicando.

Si la persona conoce el contenido de sus mensajes, entonces puede estar utilizando otros dispositivos que estén asociados a sus cuentas, puede estar controlando su dispositivo o la otra persona le compartió o reenvió los mensajes.

Si la persona conoce el contenido de conversaciones de voz o video, pero no estuvo cerca para simplemente escuchar la conversación, y si la persona con la que usted habló no le contó sobre la conversación, esa persona podría estar utilizando un software de acecho. **Precaución:** cualquier cosa que usted haga en su teléfono, incluyendo las búsquedas de información o la búsqueda del software de acecho, podría ser visto. Busque información sobre los programas de acoso desde un dispositivo más seguro.

¿La persona que lo/la está controlando tuvo acceso a su teléfono?

La mayoría de los controles requieren acceso físico a los teléfonos. La persona podría revisar su teléfono regularmente para ver a quién llamó o envió mensajes o podría haber instalado programas de acoso en su teléfono que le permiten ver su actividad desde otro teléfono o computadora. Con acceso físico a su teléfono,

la persona también podría descargar aplicaciones o cambiar los ajustes de cuenta y de seguridad para que su teléfono sea más vulnerable.

¿La persona tiene acceso a su cuenta en línea o en la nube?
Otra forma en la que alguien podría revisar su teléfono es si esa persona tiene acceso a su cuenta mediante la compañía de teléfono y/o una cuenta en la nube con la que su teléfono esté asociado (Google o Apple). Si el nombre de la persona figura en la cuenta telefónica o si logra convencer a la compañía telefónica de que es usted o alguien autorizado, esa persona podría tener la posibilidad de activar funciones de ubicación o acceder a sus expedientes de facturación en línea y ver sus registros de llamadas y más información.

¿Conoce su ubicación?
Los teléfonos y las aplicaciones pueden compartir su ubicación. Revise los ajustes de su teléfono y de las aplicaciones para limitar como se comparte la ubicación. La mayoría de los teléfonos también tienen una función que ayuda a que usted localice un teléfono que no encuentra, lo que puede desvelar su ubicación si la otra persona tiene acceso a su teléfono o cuenta. Conozca más acerca de Rastrear la Ubicación más allá de los teléfonos.

¿Le preocupan los programa espía (spyware)?
Busque información sobre los programas de acoso desde un dispositivo más seguro.

Parte 2: Si su teléfono está siendo controlado

Hay pasos que usted puede seguir para proteger su teléfono, sus aplicaciones y cuentas. No hay una forma “correcta” de actuar. Lo que funciona para otras personas podría no darle resultado o no ser seguro para usted.
PRECAUCIÓN: Los cambios con frecuencia alertan a la otra persona. Esa persona podría forzarlo/a a usted a que desbloquee su teléfono o le comparta sus

contraseñas. La persona podría volverse más agresiva. Hacer cambios también podría eliminar evidencia.

1. **Restaurar el Teléfono y las Cuentas.**
    - Realizar una restauración de fábrica del teléfono podría desinstalar cualquier programa de acoso que se haya instalado sin su permiso o conocimiento. Sin embargo, es importante no volver a conectar el dispositivo con una copia de respaldo para que el programa de acoso no se vuelva a instalar.
    - También puede desinstalar toda aplicación que no le resulte conocida y revisar qué aplicaciones y ajustes actuales permiten que se comparta la ubicación. Llame a su proveedor de celular para asegurarse de que no haya otro servicio de ubicación habilitado.
    - Restaure las contraseñas de las facturas telefónicas, las cuentas en la nube y demás cuentas conectadas para eliminar cualquier posible acceso que la persona pueda tener.
2. **Cambie su teléfono actual.** Si tiene la posibilidad y siente seguridad al respecto, usted podría cambiar su teléfono o configurar un segundo teléfono. Estos son algunas opciones:
    - Compre un nuevo teléfono y considere cambiar de compañía telefónica y obtener un nuevo número. Consulte si hay medidas de seguridad adicionales que usted pueda configurar para su cuenta, como pedirle a la compañía que registre que solo usted será quien posee la cuenta de forma autorizada o pedir que se generen notificaciones ante cambios en su cuenta, incluyendo si se agregan o quitan funciones.
    - Compre un teléfono prepago con efectivo.
    - Dependiendo de sus ingresos o circunstancias, usted podría tener descuentos en teléfonos o servicios. Un ejemplo es el programa LifeLine,

que ofrece descuentos para personas que se califiquen como de bajos ingresos.

- Un/a amigo/a de confianza o un/a familiar podría darle a usted un teléfono que no utilice. Asegúrese de borrar la memoria del teléfono y de hacer un "reinicio de fábrica" para eliminar cualquier información del teléfono.

Importante: No conecte el nuevo teléfono a ninguna cuenta anterior, en especial cuentas en la nube como Google o iCloud, y no use su número anterior. No transfiera información de su antiguo teléfono al nuevo mediante una tarjeta de memoria, una tarjeta SIM, sus cuentas en la nube ni copias de respaldo. Hacer eso podría volver a instalar un programa de acoso.

2. **Tenga una estrategia para el teléfono controlado.** Algunos/as agresores/as podrían aumentar la intensidad de su maltrato si pierden acceso o control. Usted puede pedir ayuda con un plan de seguridad. También podría querer mantener el teléfono controlado como evidencia. Si se queda con el teléfono, decida cómo lo guardará. Podría apagarlo, quitarle la batería o cubrirlo con papel laminado. Recuerde que una vez que vuelva a encenderlo, su ubicación será visible si alguien la está controlando a través de una señal de celular o WiFi. Usted también podría considerar quedarse con el teléfono y utilizarlo de manera estratégica para prevenir que el/la agresor/a sospeche. Todas estas son opciones para considerar y consultar con un/a intercesor/a.
3. **Hable con amigos y familia.** La familia y los/las amigos/as podría compartir su ubicación inadvertidamente, o revelar con quién habla o qué está haciendo a través de publicaciones en redes sociales o con otras personas. Si usted tiene hijos/as, enséñeles como evitar compartir su ubicación o información acerca de sus actividades personales.
4. **Documente lo qué está sucediendo.** Usted puede documentar lo que está sucediendo, si le parece seguro, mediante fotos de pantalla y creando un registro de lo que está sucediendo antes de hacer cualquier cambio. Usted puede optar por compartir esto con oficiales de seguridad, un/a abogado/a o

guardarlo para otra ocasión. Documentar el maltrato podría ayudarlo/a a generar o actualizar un plan de seguridad. Conozca más acerca de Documentar el maltrato.

Parte 3: Medidas para Aumentar la Seguridad y la Privacidad

1. **Ponga una clave de acceso en el teléfono.** La mayoría de los teléfonos piden una contraseña de 4 dígitos, pero algunos le permitirán generar códigos más complejos, patrones de seguridad o un acceso biométrico con su huella digital o con reconocimiento facial. Si usted no puede poner una contraseña en su teléfono o si el/la agresor/a le exige que comparta su contraseña, considere pedir prestado un teléfono para almacenar información de seguridad o para llamar a una línea directa.
2. **Asegure las cuentas en línea de su teléfono.** Los teléfonos suelen tener una cuenta en línea con la compañía telefónica y una cuenta en la nube para almacenar información personal (probablemente una cuenta Google o iCloud). Revise los ajustes de seguridad y considere cambiar las contraseñas de su teléfono y de las cuentas en la nube para asegurarse de que otra persona no pueda acceder a su información.
3. **Utilice programas antivirus y antispyware (programa espía) en su teléfono.** Puede buscar programas reconocidos en línea y luego buscarlos en las tiendas de aplicaciones. Muchos cuentan con versiones gratuitas y los servicios pueden proteger contra programas de acoso y prevenir que se descarguen otras aplicaciones maliciosas en su dispositivo.
4. **Apague la función de compartir ubicación.** Los teléfonos tienen GPS integrados que pueden determinar su ubicación y algunos teléfonos y aplicaciones le dan la opción de compartir esa información. Usted puede administrar cómo se comparte la ubicación dentro de los ajustes del teléfono, donde puede elegir qué aplicaciones pueden acceder a su ubicación o apagar

completamente la función de compartir ubicación. Algunas aplicaciones le permiten incluso gestionar su ubicación dentro de los ajustes de la aplicación.

5. **Revise sus ajustes de privacidad y seguridad.** La mayoría de los teléfonos tienen ajustes que le permiten administrar su privacidad y seguridad. Puede encontrar estos controles en los ajustes del teléfono o de la aplicación. Para obtener más información, lea Consejos de Seguridad y Privacidad en Línea, y consulte nuestras guías sobre Facebook y Twitter (en inglés) para saber más sobre sus ajustes de privacidad y seguridad.
6. **Cierre sesión en aplicaciones y cuentas.** Considere cerrar sesión en las cuentas para que otros no puedan acceder a ellas en caso de poder acceder a su teléfono. Tal vez no pueda cerrar sesión en algunas aplicaciones sin quitarlas por completo de su teléfono. Podría ser más incómodo acceder a las cuentas a través del navegador, pero usted puede tomar su decisión en base a sus propios riesgos de privacidad y seguridad.
7. **Revise las aplicaciones descargadas.** Si usted encuentra una aplicación desconocida en su teléfono, bórrela. Las aplicaciones son fáciles de descargar y de olvidar, y algunas podrían estar recopilando su información privada. Sin embargo, tenga cuidado antes de eliminar una aplicación si usted sospecha que puede ser un programa espía (spyware) o de acoso. Busque información sobre los programas espía desde un dispositivo más seguro.
8. **Evite los teléfonos liberados o con "*jailbreak*".** Eliminar las restricciones del fabricante o de la compañía de teléfono genera que sean más vulnerables a los programa espía (spyware) o de acoso. Saber si su teléfono fue liberado o si tuvo "*jailbreak*" puede ser una pista sobre si alguien puede haber instalado una aplicación de control en su dispositivo.
9. **Use números de teléfono virtuales.** Considere usar un número de teléfono virtual que le permita revisar llamadas, recibir mensajes de voz y hacer llamadas o enviar mensajes de texto sin compartir el número de teléfono del dispositivo. Los números virtuales se pueden vincular a una cuenta en la nube,

por ejemplo Google Voice, así que también debe asegurarse de que la cuenta en línea también sea segura.

10. **Intente no almacenar información sensible en su teléfono.** Mientras menos sensible sea la información que posee en su teléfono, menos probable será que alguien más pueda acceder a ella. Puede que usted quiera borrar ciertos mensajes de texto o mensajes de voz de su teléfono y de las cuentas en la nube asociadas (como Google o iCloud).
11. **Si está considerando una aplicación de seguridad...** Existen muchas "aplicaciones de seguridad personal" que ofrecen aumentar la seguridad personal de sus usuarios; algunas están desarrolladas o promocionadas específicamente para sobrevivientes de violencia. Conozca más en nuestro Centro de Aplicaciones de Seguridad (en inglés) para saber si tales aplicaciones son adecuadas para usted.

 Este producto fue financiado por el acuerdo de cooperación n.° 2019-V3-GX-K017, otorgado por la Oficina para Víctimas de Delito, Oficina de Programas de Justicia, Departamento de Justicia de los Estados Unidos. Las opiniones, los hallazgos, las conclusiones o las recomendaciones aquí expresados pertenecen a los/las contribuyentes y no necesariamente reflejan la postura oficial ni las políticas del Departamento de Justicia de los Estados Unidos.

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