Hoja de Consejos para el Plan de Seguridad Tecnológica

Priorizar la seguridad

Considera utilizar un dispositivo más seguro. Si crees que alguien está vigilando tu computadora, tableta o teléfono inteligente, intenta utilizar un dispositivo diferente al que el agresor no haya tenido acceso físico o remoto en el pasado y al que no tenga acceso ahora (como una computadora en una biblioteca o el teléfono de un amigo). Esta es una forma de reducir el riesgo de ser vigilado por un agresor.

Obtén más información. Enfrentarse a la violencia, los malos tratos y el acecho puede ser muy difícil y peligroso. Los trabajadores contra la violencia de tu zona pueden informarte sobre las opciones y los recursos locales, y ayudarte a crear un plan para tu seguridad. Puedes llamar a tu organización local contra la violencia para que te pongan en contacto con un trabajador de apoyo cerca de ti o encontrar uno en www.sheltersafe.ca.

Confía en tus instintos. Los agresores suelen estar muy decididos a mantener el control sobre las mujeres y la tecnología es una de las muchas herramientas que utilizan para hacerlo. Si parece que la persona sabe demasiado sobre ti, podría estar obteniendo información de diversas fuentes, como monitorear tus dispositivos, acceder a tus cuentas en línea, rastrear tu ubicación o recopilar información sobre ti en Internet.

Planea estratégicamente en torno a tu tecnología. Cuando los agresores hacen un uso indebido de la tecnología, suele ser una reacción natural querer deshacerse de los dispositivos o cerrar las cuentas en línea para que deje de hacerlo. Sin embargo, algunos agresores pueden intensificar su comportamiento controlador y peligroso si sienten que han perdido el control sobre su pareja actual o anterior. Antes de retirar una cámara oculta o un localizador GPS que hayas encontrado, o de desinstalar un programa de acoso, piensa en cómo puede responder el agresor y planea tu seguridad. Por ejemplo, algunas mujeres optan por utilizar un dispositivo más seguro para determinadas interacciones, pero también siguen utilizando el dispositivo monitoreado como una forma de recopilar evidencia y evitar el escalamiento del comportamiento.

Identifica el abuso

Busca patrones. Tómate un tiempo para pensar qué tipo de tecnología puede utilizarse para acecharte, vigilarte o acosarte. Por ejemplo, si el agresor ha insinuado que te vigila, piensa en lo que sabe.

¿Sólo sabe lo que haces en un área específica de tu casa? Si es así, puede que haya una cámara oculta en esa habitación.

Si sospechas que te están siguiendo, ¿lo hacen sólo cuando estás en el coche o también cuando vas a pie? Si es sólo en el coche, puede que haya un dispositivo oculto en él. Si es en todas partes, puede tratarse de algo que llevas contigo, como tu teléfono o un rastreador en tu bolso.

Reducir las posibles fuentes de tecnología que están siendo utilizadas indebidamente puede ayudarte a crear un plan de seguridad y a documentar el abuso. Encuentra más información sobre Evaluación de la violencia facilitada por la tecnología aquí.

Documenta los incidentes. Documentar una serie de incidentes puede mostrar a la policía o al tribunal un patrón de comportamiento que se ajuste a la definición legal de acecho o acoso. La documentación también puede ayudarte a ver si la situación está empeorando y con la planeación de tu seguridad. Para más información, consulta Consejos de documentación para mujeres que experimentan violencia facilitada por la tecnología.

Denuncia los incidentes. También puedes considerar denunciar los incidentes a las autoridades policiales o solicitar una Fianza de Paz o una Orden de Protección Familiar. Si el comportamiento de acoso se produce en línea, también puedes denunciar el abuso al sitio web o la aplicación donde está ocurriendo el acoso. Si el comportamiento viola las condiciones de servicio de la plataforma, es posible que se elimine el contenido o que se

prohíba el acceso a la persona. Es importante reconocer que denunciar el contenido puede eliminarlo por completo, por lo que debe documentarse como evidencia antes de denunciarlo.

Pasos para aumentar la seguridad

Cambia contraseñas y nombres de usuario. Si crees que están accediendo a tus cuentas en línea, puedes cambiar tus nombres de usuario y contraseñas utilizando un dispositivo más seguro. Una vez que hayas actualizado la información de la cuenta, es importante que no accedas a ellas desde un dispositivo que creas que está siendo vigilado. También puedes plantearte crear cuentas nuevas, como una nueva dirección de correo electrónico con un nombre de usuario que no se pueda identificar fácilmente en lugar de tu nombre real u otra información reveladora. Es importante no vincular estas cuentas nuevas a cuentas o números antiguos, y no utilizar la misma contraseña para todas las cuentas. Encuentra más consejos sobre Seguridad de Contraseñas.

Comprueba tus dispositivos y configuraciones. Revisa tu teléfono inteligente, tus aplicaciones y tus cuentas en línea para comprobar la configuración de privacidad y asegurarte de que otros dispositivos o cuentas no estén conectados al tuyo y de que cualquier acceso entre dispositivos, como el Bluetooth, está desactivado cuando no lo utilizas. Asegúrate de que sabes qué es cada una de tus aplicaciones y qué hace. Elimina cualquier aplicación de tu dispositivo que no conozcas o que no utilices. Busca picos en el uso de datos, ya que pueden indicar que se está utilizando software de monitoreo, como programas espía.

Consigue un nuevo dispositivo. Si sospechas que tu dispositivo actual está siendo vigilado, lo más seguro puede ser conseguir un dispositivo nuevo con

una cuenta a la que el agresor no tenga acceso. Un teléfono de pago por uso es una opción menos costosa. Pon un código de acceso en el nuevo dispositivo y no lo vincules a tus antiguas cuentas en la nube, como iCloud o Google, a las que la persona podría tener acceso. Considera la posibilidad de desactivar la localización y el uso compartido de Bluetooth cuando no esté en uso. También puedes conservar el dispositivo antiguo para que el agresor piense que sigues usándolo y no intente acceder al nuevo.

Protege tu ubicación. Si el agresor parece saber siempre dónde estás, es posible que te esté rastreando a través de tu teléfono inteligente o vehículo o mediante un dispositivo de localización. Puedes comprobar tu teléfono, aplicaciones y cuentas para ver si está activado el uso compartido de la ubicación y actualizar la configuración para que se adapte mejor a tus necesidades. También puedes llamar a tu proveedor de telefonía móvil para preguntarle si utiliza algún servicio de localización compartida, sobre todo si tienes un plan familiar con el agresor. El rastreo de ubicación a través de tu coche podría ser a través de un servicio de asistencia en carretera o de conductor seguro. Si te preocupa la posibilidad de que haya un dispositivo de rastreo oculto en tu coche u otras pertenencias, es posible que una agencia policial, un investigador privado o un mecánico de autos puedan revisarlo. Es importante planear la seguridad y documentar la evidencia antes de retirar un dispositivo o cambiar el acceso del agresor a tu información de ubicación.

Considera cámaras y dispositivos de audio. Si sospechas que te están vigilando a través de cámaras o grabadoras de audio, puede estar ocurriendo a través de dispositivos ocultos, regalos recibidos del agresor o incluso dispositivos cotidianos como cámaras web, asistentes personales (como Google Home o Alexa) o sistemas de seguridad. Si te preocupan las cámaras ocultas, puedes considerar probar un detector de cámaras, aunque algunos sólo localizan cámaras inalámbricas, no cámaras con cable, o viceversa. Los

dispositivos cotidianos o los regalos pueden protegerse cambiando la configuración de la cuenta o las contraseñas. Las cámaras web integradas pueden cubrirse con un trozo de cinta adhesiva removible (aunque esto sólo se refiere a la cámara, no al software espía de la computadora). Recuerda elaborar un plan de seguridad y documentar la evidencia antes de retirar los dispositivos o cortar el acceso del agresor.

Pasos para aumentar la Privacidad

Protege tu dirección. Si te preocupa que alguien descubra la dirección de tu casa, puedes abrir un buzón privado (apartado de correos). Ten en cuenta que esto es más útil si te has mudado recientemente o el agresor no conoce ya tu dirección. Dile a tus amigos y familiares que no compartan tu dirección y sean prudentes a la hora de facilitarla a comercios locales. Además, para conocer sus opciones, averigua qué información es pública en tu comunidad en caso de que compres una casa.

Limita la información que proporcionas sobre ti misma. Hoy en día, casi todo lo que hacemos nos pide información de identificación personal, ya sea para hacer una compra, abrir una tarjeta de descuento o crear una cuenta en Internet. La información que proporcionamos se vende a menudo a terceros y más tarde acaba en Internet en motores de búsqueda y con intermediarios de datos. Cuando sea posible, opta por no aceptar la recopilación de información o proporciona sólo la mínima necesaria. Puedes ser creativa: por ejemplo, en lugar de utilizar tu nombre y apellidos, utiliza tus iniciales. También puedes utilizar un número de teléfono virtual gratuito, como Google Voice, para disponer de un número alternativo que compartir cuando lo necesites.

Controla tu privacidad en línea y fuera de línea. Nuestro Kit de Herramientas de Seguridad y Privacidad Tecnológicas contiene Consejos sobre Privacidad y Seguridad en Línea, que incluyen más información sobre cómo cambiar la configuración de tus dispositivos electrónicos, cuentas de redes sociales como Facebook y Twitter, y la red Wi-Fi de tu casa. Sigue esos pasos para aumentar tu privacidad y disminuir los riesgos de que el agresor haga un mal uso de esas tecnologías, te localice o vigile tu actividad.

La Violencia de Género Facilitada por la Tecnología (VGFT) es parte de un continuo de violencia que puede ocurrir tanto en línea como en persona. Si tú o alguien que conoces está experimentando VGFT, no están solos. Pueden utilizar sheltersafe.ca para encontrar un refugio o casa de transición cerca de ti y hablar sobre las opciones para crear un plan de seguridad. No es necesario permanecer en un refugio para acceder a servicios y apoyo gratuitos y confidenciales.

Adaptado para Canadá con autorización del proyecto Safety Net de NNEDV, basado en su recurso Plan de Seguridad Tecnológica: Una Guía para Sobrevivientes y Defensores.