Temas para iniciar una conversación sobre la Planeación de Seguridad Tecnológica

Cómo utilizar este recurso

Este recurso está diseñado para ayudar a los trabajadores contra la violencia a hablar de la violencia de género facilitada por la tecnología (VGFT) con sobrevivientes. La violencia de género facilitada por la tecnología es una táctica común de violencia doméstica. Si la persona con la que trabajas ha

sufrido VGFT, debe tenerse muy en cuenta en su plan de seguridad. Este recurso contiene preguntas, estrategias de seguridad tecnológica y enlaces a documentos que puedes utilizar para guiar tus conversaciones sobre planeación de seguridad con sobrevivientes que experimentan VGFT.

También puedes consultar los recursos complementarios: "¿Estás sufriendo abuso tecnológico?" y "Lista de verificación para la planeación de seguridad tecnológica".

Consideraciones iniciales:

- Es posible que las siguientes estrategias de seguridad tecnológica no se adapten a todas las situaciones. Reúnete con tu cliente donde se encuentre y empieza la conversación con la forma de abuso tecnológico que ella identifique que puede estar ocurriendo. Esto no pretende ser una lista de verificación como tal, sino más bien sugerencias sobre cómo incorporar la tecnología a la planeación de seguridad.
- Siempre que planees la seguridad de una persona que ha sufrido violencia facilitada por la tecnología, es importante tener en cuenta que el agresor puede tener acceso a sus dispositivos o cuentas en línea y puede estar monitoreando sus comunicaciones y movimientos a través de estos dispositivos y cuentas. Hacer cambios en cualquier dispositivo, cuenta de redes sociales, correo electrónico u otra tecnología puede alertar al agresor de que tu cliente está buscando ayuda y puede desencadenar abusos adicionales. En estas situaciones puede ser necesario tomar precauciones adicionales en la planeación de la seguridad.

¿Alguien controla, toma, rompe o te obliga a compartir tu teléfono?

- ¿Tienes tu propio teléfono? ¿Para qué utilizas el teléfono?
- ¿Alguien te impide hablar con tu familia o amigos?
- ¿Compartes tu teléfono con alguien más o alguien más mira tu teléfono?
- ¿Alguna vez has necesitado utilizar tu teléfono pero no has podido usarlo? ¿Puedes contarme más sobre lo que estaba pasando?
- ¿Alguien sabe cómo desbloquear tu teléfono o te obligan a desbloquearlo?

Estrategias de seguridad tecnológica sugeridas:

- Si decides que no es seguro dejar de utilizar un teléfono que el abusador está monitoreando o al que tiene acceso, utiliza tu teléfono con normalidad, pero encuentra otra forma de hablar de forma segura sobre cosas privadas y planea tu seguridad.
- Cuando veas a alguien, hazle saber que tu teléfono no es privado. Utiliza una palabra clave que permita a la otra persona saber si alguien está escuchando tu llamada o leyendo tus mensajes.
- Anota los números de las personas que aparecen en tu teléfono y guárdalos en un lugar seguro en caso de que te lo quiten o rompan.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

¿Alguien accede, controla o bloquea tus cuentas (correo electrónico, bancos, redes sociales, etc.)?

- ¿Compartes cuentas con alguien? ¿La configuran o toman decisiones por ti sobre tu cuenta?
- ¿Alguien tiene acceso a tus cuentas de correo electrónico, cuentas bancarias, GooglePlay, Apple ID o cuenta de iCloud?
- ¿Lo que haces en tu teléfono o en tus cuentas es privado o lo ve alguien más?
- ¿Alguien conoce tus contraseñas o entra a tus cuentas?
- ¿Alguien te ha bloqueado alguna vez tus cuentas o ha hecho cambios en ellas?
- ¿Alguien abre cuentas a tu nombre o miente diciendo que quieres una cuenta?
- ¿Tienes tu propia cuenta bancaria o la compartes con alguien?

Estrategias de seguridad tecnológica sugeridas:

- Utiliza una contraseña larga combinando números y símbolos que sea difícil de adivinar.
- Utiliza la verificación en dos pasos o la autenticación multifactorial si es seguro hacerlo.
- Utiliza una contraseña diferente para cada cuenta.
- Considera el cambio de contraseñas de las cuentas o la creación de nuevas cuentas.
- Configura nuevas cuentas "seguras" en un teléfono seguro o en una computadora de la biblioteca. Utiliza esas cuentas sólo en un dispositivo al que el agresor no tenga acceso.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

¿Alguien le avergüenza, humilla, amenaza o suplanta tu identidad utilizando redes sociales, aplicaciones, mensajes de texto, correo electrónico o teléfono?

- ¿Alguien dice cosas malas de ti en redes sociales?
- ¿Otras personas empiezan a decir cosas para lastimarte o dan "me gusta" a cosas desagradables sobre ti que otros han publicado?
- ¿Alguien hace que sientas miedo por utilizar las redes sociales? ¿Qué hacen?
- ¿Alguien, en las redes sociales, te ha engañado o ha actuado como si fuera tú o alguien que conoces?

Estrategias de seguridad tecnológica sugeridas:

- Lleva un registro de las publicaciones en redes sociales, quién las publicó y quién las recibió (utiliza la función "descargar datos", haz una captura de pantalla o una foto con otro dispositivo "seguro", o cópialas, imprímelas o guárdalas en una USB).
- Ajusta la configuración de seguridad y privacidad (incluido el etiquetado) en las aplicaciones de redes sociales. Bloquea al agresor si es seguro hacerlo.
- Estos comportamientos pueden ser ilegales y se puede pedir ayuda a un abogado o a la policía.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

¿Alguien te acosa, abusa, castiga o amenaza a través de mensajes de texto, aplicaciones de comunicación (WhatsApp, Viber, Skype, Facetime), correo electrónico o teléfono?

- ¿Alguien ha dicho cosas usando el teléfono para lastimarte o asustarte?
- ¿Tienes que hacer cosas con el teléfono para no meterte en problemas?
- ¿Alguien te envía mensajes todo el tiempo o se enoja si no respondes?

Estrategias de seguridad tecnológica sugeridas:

- Anota lo que se dijo en las llamadas telefónicas y guarda los registros del historial de llamadas, a veces llamados "recientes" (haz una captura de pantalla, una foto con otro dispositivo "seguro" o imprímela). También se puede acceder al historial de llamadas y a los registros de mensajes de texto a través de los proveedores de telefonía móvil.
- Conserva los mensajes de texto (haz una copia, captura de pantalla, foto con otro dispositivo "seguro", imprime o guarda en un USB).
- Apaga el Wi-Fi y el Bluetooth y pon el dispositivo en modo avión o vuelo para conservar el historial de llamadas y los mensajes de texto en el dispositivo.
- Lleva el dispositivo y todas las copias, capturas de pantalla, impresiones o USB a tu abogado o a la policía para que documenten formalmente la evidencia, ya que estas conductas pueden ser ilegales.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

¿Alguien comparte o amenaza con compartir imágenes sin tu consentimiento (abuso basado en imágenes)?

- ¿Alguien tiene fotos o videos privados tuyos con o sin tu consentimiento?
- ¿Han compartido esas fotos o han dicho que las compartirán?
- ¿Te dijeron estas cosas en persona o te las enviaron?

Estrategias de seguridad tecnológica sugeridas:

- Pide a la persona que retire la imagen y la borre.
- Denuncia la imagen a la empresa de la red social.
- Compartir imágenes íntimas sin consentimiento va contra la ley y se puede pedir ayuda a un defensor legal, un abogado o la policía.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

¿Sabe alguien dónde estás, qué haces o te acecha utilizando aplicaciones de rastreo de ubicación/GPS, vigilancia, programas espía/registrador de teclas o cámaras ocultas?

- ¿Alguien utiliza tu teléfono para vigilarte o saber adónde vas?
- ¿Alguien sabe cosas que tú no le has dicho? ¿Cómo crees que se han enterado?
- ¿Hay alguien que parece saber algunas cosas pero no otras? ¿Qué cosas saben? ¿Dónde "vive/está" esa información?
- ¿Ocurren cosas raras con tu teléfono, coche o casa que no tienen sentido?

- Si tu cliente sospecha que alguien está vigilando su ubicación o si la están acechando, sus dispositivos, su casa, su coche, sus pertenencias o los dispositivos o pertenencias de sus hijos pueden verse comprometidos.
- Todo acecho debe tomarse en serio.

Estrategias de seguridad tecnológica sugeridas:

- Considera utilizar un dispositivo "seguro" (por ejemplo, un teléfono nuevo o el teléfono de un familiar/amigo de confianza) para las actividades de planeación de seguridad y/o dejarlo con familiares/amigos de confianza.
- Averigua si existe un patrón relacionado con lo que alguien sabe. ¿Saben dónde vas todo el tiempo o sólo cuando conduces tu coche o utilizas el transporte público? Considera trazar un mapa de lo que la persona sabe y dónde puede encontrarse esa información. Esto puede ayudar a determinar de dónde obtiene la información. Por ejemplo, si tiene acceso a los lugares a los que vas utilizando una aplicación de viajes compartidos, pero no a otras formas de transporte u otra información, puede que sea esa aplicación específica de viajes compartidos la que esté comprometido.
- Verifica la configuración de ubicación global en el teléfono y de cada aplicación, ya que algunas aplicaciones pueden recopilar y compartir información de ubicación. También verifica la existencia de herramientas de rastreo de ubicación como Tile o AirTags.
- Los comportamientos de acecho pueden ser ilegales y se puede pedir ayuda a un abogado o a la policía.
- Para más consejos, consulta nuestra Lista de verificación para la planeación de seguridad tecnológica.

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 o llamar / enviar mensaje de texto al Teléfono de Ayuda para Niños para hablar sobre las opciones y 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 Technology Safety de WESNET, basado en su recurso *Abuso Tecnológico:* Temas para iniciar una conversación con clientes y Planeación de seguridad.