Trabajar de forma remota:
Consejos para configurar teléfonos

Aunque a los/las intercesores/as se les solicite trabajar desde su casa durante la crisis de salud pública o si pudiesen trabajar desde su casa como parte de su cronograma normal, es vital poder recibir y hacer llamadas, enviar y recibir mensajes de texto y chatear de forma segura. A continuación encontrará soluciones y consejos para las consultas frecuentes que se realizan a la hora de instalar un acceso telefónico remoto.

¿Cómo se puede desviar nuestra línea telefónica a un intercesor que trabaja desde su casa?

1. Contacte a su compañía telefónica y consulte sus opciones.
2. De ser posible, cambie a VoIP (protocolo de voz por internet). TechSoup ofrece acceso a VoIP alojado por Tech Impact (en Inglés).
3. Si recibe mensajes de texto a través de su línea telefónica, la herramienta que utiliza para administrar esos mensajes de texto podría ofrecer servicios de desvío de llamadas a otra línea telefónica.
4. Considere desviar su línea telefónica a la línea National DV si/cuando no pueda recibir llamadas. Conozca más sobre la línea DV (en Inglés).
5. De ser posible, utilice un servicio de respuestas.

AVISO: planifique desviar las llamadas por turnos y asegúrese de que ninguna persona esté conectada en un periodo de 24 horas.

¿Cómo puede un intercesor realizar llamadas a sobrevivientes cuando trabaja desde su casa?

1. Oculte el número de salida.
2. Utilice un servicio de suplantación que cambie el número en el identificador de llamadas. Ingrese "suplantación de número telefónico" en Google para encontrar empresas.

3. Envíe un enlace al/a la sobreviviente para realizar una llamada de voz por internet, por ejemplo a través de Cyph o de Gruveo.
4. Utilice VoIP, servicios basados en internet que admitan llamadas por audio. Genere cuentas para el programa, como Google Suite para organizaciones sin fines de lucro. NO haga que los/las intercesores/as configuren cuentas personales con su información personal.

¿Qué sucede con los mensajes de texto, el chat o el video?

A continuación encontrará recursos adicionales para utilizar mensajes de texto, chat o video para comunicarse con sobrevivientes.

- Mensajería Directa y Mensajes de Texto con Sobrevivientes: Mejores Prácticas
- Chat con Sobrevivientes: Mejores Prácticas
- Comunicación con Sobrevivientes Mediante Video: Mejores Prácticas

¿Qué se puede hacer si los teléfonos de la agencia no son una opción inmediata y los/las intercesores/as debe utilizar sus teléfonos celulares, tabletas y computadoras personales?

Las obligaciones de confidencialidad exigen que nadie fuera de su programa pueda ver la información personal identificable de los/las sobrevivientes, esto incluye evitar la divulgación inadvertida. Para cumplir con estas obligaciones, enfóquese en estos consejos:

1. Priorice la seguridad.
    - No comparta su dispositivo con otras personas de su hogar. Si pueden configurarse diferentes cuentas o perfiles en el dispositivo, cree una nueva cuenta de usuario para el uso laboral del/de la intercesor/a en vez de utilizar el perfil o la cuenta personal existente.
    - Utilice contraseñas, claves o demás métodos de bloqueo que tengan un alto nivel de seguridad.

- Instale software contra programas maliciosos y manténgalo actualizado.
- Habilite la opción de borrar información de forma remota, en el caso de robo o pérdida de un dispositivo.

2. Utilice cuentas de correo electrónico, mensajería directa, mensajería instantánea, llamadas de voz, almacenamiento de archivo, etc. que pertenezcan al programa.
3. Tanto como sea posible, utilice computadoras y no teléfonos para el correo electrónico, el acceso a archivos e incluso para mensajes de texto, videos y llamadas.
4. No guarde nombres de los/las sobrevivientes, números de teléfono, correos electrónicos, contacto digital ni ninguna otra información en los contactos, los correos electrónicos, las conversaciones por texto, los calendarios ni en ningún otro lugar.
5. Borre todos los mensajes de texto y correos electrónicos con regularidad y rápidamente y, de ser posible, borre la información que identifique a los/las sobrevivientes de todos los registros de llamadas, mensajes, videos, etc. del dispositivo Y de las cuentas basadas en la nube y en la información de facturación.
   Aviso: asegúrese de capacitar o dar acceso a los/las intercesores/as para poder borrar información del almacenamiento en la nube.

El bienestar de los/las intercesores/as es una prioridad en todo momento, pero esta necesidad se amplifica durante un desastre o una crisis de salud pública. Con la tecnología, el foco está en generar un balance personal/laboral con los siguientes consejos:

1. No difunda los números personales a fin de preservar la privacidad del/de la intercesor/a y para ayudar a mantener los límites. Consulte cómo realizar llamadas, como se indicó anteriormente.
2. Organice turnos para dividir las llamadas, mensajes de texto, chat y demás comunicaciones con los/las sobrevivientes que ingresen a la línea.

3. Utilice acuerdos de teléfonos móviles y brinde apoyo informático. Sea claro/a con los/las intercesores/as acerca de la información mencionada a través de la capacitación y de un acuerdo escrito. De ser posible, cuente con personal informático o consultoría que ayude a los/las intercesores/as a asegurar sus dispositivos y a configurar el acceso a la cuenta.

Conozca más: Uso de Teléfonos Móviles para Comunicarse con Sobrevivientes: Mejores Prácticas

¿Cómo puede un intercesor que trabaja desde casa acceder a archivos electrónicos de forma remota?

Si los/las intercesores/as deben acceder a archivos cuando no se encuentran en la oficina, la transmisión y el acceso seguros son importantes. Algunos servicios basados en la nube ofrecen opciones de cifrado de "conocimiento cero" o "conocimiento nulo" en los cuales ninguna persona, ni siquiera la compañía tecnológica que presta el servicio, puede ver el contenido de los archivos porque solamente su programa cuenta con la clave de cifrado. Además, busque servicios que le permitan controlar el acceso individual de los/las usuarios/as, a fin de que pueda añadir o suspender el acceso de usuarios/as según sea necesario. Tanto Tresorit como SpiderOak's CrossClave ofrecen encriptación de cero conocimiento.

Para obtener más información sobre cómo asegurar el internet en el hogar, consulte Privacidad y Seguridad del WiFi: Consejos para las Agencias de Servicios a la Víctima y Sobrevivientes.

 Financiado por US DOJ-OVW subvención n.° 2019-TA-AX-K003. Las opiniones, los hallazgos, las conclusiones o las 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.