NNEDV

Pasos para aumentar privacidad y seguridad en línea

Hay varias formas de aumentar la privacidad y la seguridad, y aun así, mantenerse conectado(a).

La seguridad ante todo. Antes de tomar estas medidas, piense en su seguridad. Algunas personas pueden intensificar su comportamiento abusivo cuando se dan cuenta que usted ha protegido sus cuentas, dispositivos o contraseñas. Valdría la pena hablar con una persona intercesora sobre la planificación de la seguridad.

Confíe en sus instintos. Si parece que alguien sabe demasiado sobre usted, es posible que esté controlando sus dispositivos, accediendo a sus cuentas en línea, rastreando su ubicación o recopilando información sobre usted en Internet. Si sospecha que alguien le está vigilando, considere la posibilidad de utilizar otro teléfono o dispositivo, como el teléfono de una amistad o una computadora de la biblioteca, la escuela o el trabajo. Aquí puede obtener más información sobre privacidad y seguridad telefónica.

Obtenga más información. Enfrentarse a la violencia, el abuso y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden ayudarle a descubrir opciones y recursos locales y a crear un plan para su seguridad. Puede ponerse en contacto con un teléfono de ayuda nacional para que le pongan en contacto con recursos locales.

Privacidad y seguridad en línea

Compartir en las redes sociales

- Las redes sociales están diseñadas para ser sociales, y por defecto, la información suele ser de dominio público. Algunos sitios le permiten elegir quién puede ver su perfil o sus publicaciones. Utilice las

herramientas y guías de configuración de la privacidad que ofrecen muchas redes sociales para satisfacer sus necesidades de privacidad.

- Tenga cuidado a la hora de conectarse a las cuentas de redes sociales o de utilizar una cuenta para acceder a otra, ya que esto dificulta el control de su privacidad.
- Cuando tome fotos o vídeos y quiera publicarlos en las redes sociales tenga en cuenta la información que aparece en el trasfondo, ya que esta podría ser utilizada por alguien para encontrarle; como nombres de calles, direcciones, matrículas o nombres de empresas.
- Revise regularmente quién está en su lista de "amistades" o "seguidores", y tenga en cuenta que los amigos de sus amistades pueden ver su perfil y sus publicaciones.
- Obtenga más información sobre citas en línea y los juegos en línea.
- Lea aquí para obtener más información sobre sitios para compartir vídeos.
- Consulte nuestra guía sobre Facebook
- **Información adicional:** Lea las políticas de privacidad de las aplicaciones y sitios para averiguar quién tiene acceso a su información y cómo pueden obtenerla. Muchos sitios y aplicaciones venderán su información o la compartirán si reciben una citación u orden judicial; esto puede ser importante para las personas sobrevivientes que tienen o pueden tener casos legales con una persona agresora.

Hable con sus amigos y familiares

- Hable con sus amistades y familiares para limitar lo que publican sobre usted.

- Pida a sus jefes, grupos comunitarios, equipos deportivos

Intermediarios de datos y retirada de contenidos de Internet

Puede haber distintos tipos de información sobre usted en Internet que le gustaría eliminar porque es "delicada", porque puede afectar su vida de algún modo o poner en peligro su seguridad, por ejemplo la dirección de su casa o sus imágenes íntimas. También puede encontrar información inexacta. Dependiendo de la delicadeza de la información, puede ser mejor ignorarla. Muchas personas sobrevivientes prefieren dejar información inexacta en Internet para ocultar la información exacta que también está disponible. Si la información que encuentra en la web es abusiva o potencialmente peligrosa, puede ponerse en contacto con el sitio web y pedirles que la retiren. Lea más sobre sus opciones para eliminar contenido delicado del Internet.

Las empresas denominadas intermediarios de datos son una forma muy común de difundir información personal en Internet. Los intermediarios de datos recopilan su información personal de Internet y de fuentes públicas. Pueden incluir sus direcciones actuales y anteriores y otros datos de contacto, así como información sobre su edad, contactos sociales, educación, trabajo y otros datos. En algunos casos, los registros en papel más antiguos se digitalizan y pueden consultarse en Internet. Lea más información sobre los intermediarios de datos y cómo darse de baja para que dejen de mostrar su información en Internet.

Cuando se inscriba para abrir nuevas cuentas

- Establezca más de una cuenta de correo electrónico. Puede utilizar cuentas de correo separadas para buscar trabajo, grupos sociales, citas por Internet, etc.
- Incluso puede ir un paso más allá y utilizar un servicio que "enmascare" la dirección de su cuenta, de modo que cuando se le pida que introduzca su dirección de correo electrónico, se utilice una dirección de correo proxy.
- Utilice nombres de usuario diferentes cuando establezca distintas cuentas en línea.

- Utilice una foto de perfil distinta para cada perfil de cuenta. También puede considerar utilizar una foto que no sea suya.
- Tenga cuidado al compartir información personal más allá de lo necesario para crear una cuenta o configurar un perfil. A veces, los sitios no dejan claro que la información es opcional, así que averigüe si es obligatoria.
- Haga clic en "no" cuando los sitios o las aplicaciones le ofrezcan consultar su lista de contactos, su lista de amigos de Facebook o cualquier otra fuente de información sobre sus contactos, para ayudarle a conectar con sus amigos que ya están en su sitio.
- No permita que su perfil sea objeto de búsquedas públicas (opt out).

- Las mejores contraseñas tienen al menos 12 caracteres.

Refuerce sus contraseñas

- Use contraseñas distintas para cada cuenta y utilice un gestor de contraseñas seguro para llevar un control.
- No comparta sus contraseñas con nadie, a menos que exista algo específico que no le haga sentir incomodidad al hacerlo. Puede ser un signo de abuso que alguien le exija que le dé su contraseña. Usted tiene derecho a su intimidad. Si siente inseguridad, solicite ayuda.
- Utilice opciones de seguridad adicionales, como la autenticación multifactorial. Un ejemplo de cómo funciona es que cuando inicia sesión en una cuenta, también recibe un código de verificación en su teléfono o en su correo electrónico.
- Lea más información sobre contraseñas.

Navegación web en privado

La mayoría de los navegadores ofrecen la opción de navegar de forma privada, lo que significa que una vez que cierra la ventana del navegador, los sitios web que ha visitado no se guardan en el historial. Sin embargo, si ha marcado o descargado algo, se podrá seguir viendo.

- También puede eliminar regularmente el historial, las cookies, los archivos temporales de Internet y los formularios y contraseñas guardados de su navegador web. ATENCIÓN: Si le preocupa que alguien esté vigilando su navegación por Internet, eliminar toda esta información de un golpe podría alertar a la persona que vigila su navegación por Internet, lo que podría suponer un riesgo para su seguridad.
- Lea más sobre Consejos de privacidad del navegador de Internet.

Cuidado con las redes inalámbricas

- Si desea ocultar su ubicación en los sitios web que visita, en lugar de usar una red Wifi pública, considere la posibilidad de utilizar una VPN (Red Privada Virtual), de igual manera, puede utilizar una en casa, o incluso instalarla en el router doméstico.
- Cambie la contraseña predeterminada de su red inalámbrica doméstica.
- Lea más sobre la seguridad WiFi.

Minimice el uso compartido de la ubicación

- Ajuste la configuración de sus dispositivos, aplicaciones y cuentas para limitar o desactivar el uso compartido de la ubicación.
- No incluya la ubicación en sus fotos. Puede desactivar la opción de guardar o compartir la ubicación en los ajustes de la cámara y de las aplicaciones para compartir fotos.
    - Lea más información sobre el rastreo de la ubicación.

Conectarse a Internet puede ayudar a reducir el aislamiento. Seguir estos consejos puede ayudarle a estar en línea, al tiempo que minimiza los riesgos de seguridad y mantiene su información personal privada y segura.

Financiado por US DOJ-OVW Subvención #15JOVW-21-GK-02216-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para consultar la última versión de este y otros materiales.