La nube, guía para las personas sobrevivientes

En la actualidad, la mayoría de los teléfonos, tabletas, computadoras y otros dispositivos requieren que usted conecte su nuevo dispositivo a una cuenta en la nube (normalmente Google o Apple para teléfonos y Microsoft para computadoras Windows). Las aplicaciones y otras cuentas que utiliza en sus dispositivos también guardan información en la nube. Esto incluye fotos, documentos, contraseñas, contactos, mensajes y correo electrónico. Dependiendo de los dispositivos, aplicaciones y cuentas que utilice, también podría almacenarse en la nube otra información sobre usted, como un registro de su ubicación, actividad en línea, llamadas, publicaciones en redes sociales, transacciones financieras, transporte público o viajes compartidos y demás.

¿Qué es la nube?

"La nube" se refiere al almacenamiento y acceso a la información a través de internet en lugar del disco duro de su computadora. El internet utiliza una red mundial de servidores remotos conectados en línea para almacenar contenidos.

¿Qué implicación tiene la nube en la planificación de la seguridad?

El mayor riesgo es que cualquiera que tenga acceso a sus dispositivos o conozca sus datos de acceso, podría ver toda la información que usted tiene almacenada en sus cuentas en la nube. Si su cuenta en la nube se comparte o está vinculada a cuentas de otras personas, estas personas también podrían ver parte de su información.

Por otro lado, la nube también puede utilizarse como parte de una estrategia de seguridad, ya que puede almacenar información durante largos períodos de tiempo y tener acceso a ella posteriormente, cuando sea más seguro, o desee compartirla con personas de confianza. De esta

manera se puede proteger la información si alguna persona daña o destruye sus dispositivos. También usted puede crear nuevas cuentas seguras estratégicamente en la nube para aumentar su privacidad y seguridad. (Por ejemplo, creando una cuenta de Proton Drive o una cuenta alternativa de Google, desde una computadora a la que la persona agresora nunca haya tenido acceso).

A continuación le presentamos algunos consejos para minimizar los riesgos y las estrategias para utilizar la nube de forma más segura y privada.

La seguridad es primero. Antes de tomar estas medidas, piense en su seguridad. Algunas personas pueden tener un comportamiento más agresivo cuando sus contraseñas, cuentas o dispositivos están protegidos. Podría hablar con una persona intercesora acerca de la planificación de su seguridad.

Confíe en sus instintos. Si siente que alguna persona sabe demasiado sobre usted, es posible que sea porque está controlando sus dispositivos, accediendo a sus cuentas en línea, rastreando su ubicación o recopilando información sobre usted en Internet. Si sospecha que alguien le vigila, considere la posibilidad de utilizar otro teléfono o dispositivo, como el teléfono de una amistad o una computadora de la biblioteca, de la escuela o del trabajo. Para obtener más información, lea seguridad telefónica y privacidad.

Busque más información. Enfrentarse a la violencia, los malos tratos y el acoso puede ser difícil y peligroso. Las personas intercesoras pueden brindarle ayuda para buscar opciones y recursos locales y a crear un plan para su seguridad. Puede llamar a un número de teléfono de ayuda

nacional que le informará sobre los recursos locales con los que puede contar.

Estrategias de seguridad y privacidad de la nube

Paso uno: Revise el acceso a sus cuentas.
La mayoría de las cuentas en la nube mantienen un registro de los dispositivos que tienen acceso a su cuenta. A menudo se trata de información sobre el tipo de dispositivo, la última vez que se utilizó para acceder a su cuenta y, a veces, la ubicación geográfica del dispositivo. Este registro suele estar en la sección de configuración de seguridad de su cuenta. Puede revisar la lista, y si nota que un dispositivo desconocido accede a su cuenta, puede hacer una captura de pantalla o una foto de la lista antes de hacer algún cambio, en caso de que desee documentar lo que está ocurriendo. Si esto le va a brindar más seguridad, puede eliminar el acceso a uno o a todos los dispositivos que usted elija.

Segundo paso: refuerce la seguridad de su cuenta.
Después de eliminar cualquier dispositivo no deseado, puede proteger su cuenta. Empiece por revisar los correos electrónicos o números de teléfono que estén conectados a su cuenta, por si alguien pudiera recibir una notificación de que está haciendo cambios en ella.

A continuación, puede cambiar su contraseña y configurar funciones de seguridad adicionales, como la autenticación multifactorial. Obtenga más información leyendo acerca de las contraseñas, privacidad y seguridad en línea.

Más consejos sobre el uso de la nube

- Cierre la sesión de sus cuentas y aplicaciones cuando haya terminado de utilizarlas. Esto es especialmente importante en caso de que otras personas tengan acceso a su teléfono, computadora u otros dispositivos.
- Si otras personas pueden acceder a su cuenta en la nube, una opción es minimizar la información que se almacena allí. Algunas cuentas y aplicaciones le permiten elegir si su información se queda solo en ese dispositivo o si se sincroniza en todos sus dispositivos.
- Si sospecha que otra persona tiene acceso a sus cuentas en la nube, antes de buscar cualquier cosa que no le gustaría que se supiera considere la posibilidad de cerrar la sesión de todas sus cuentas en la nube o abrir un navegador diferente en el que usted no esté conectado(a) a ninguna cuenta en la nube.

Configuración de un teléfono nuevo

Si decide adquirir un nuevo teléfono u otro dispositivo porque le preocupa que su teléfono anterior haya sido manipulado o esté siendo vigilado, es importante crear también nuevas cuentas en la nube y no transferir datos de sus antiguas cuentas o copias de seguridad. Si otra persona tiene acceso a su cuenta anterior en la nube y usted la conecta a su nuevo teléfono, esa persona también tendrá acceso a su nuevo teléfono. Si tiene stalkerware u otras aplicaciones en su antiguo teléfono y transfiere sus archivos anteriores o restaura datos desde una copia de seguridad, podrían añadirse a su nuevo teléfono. Obtenga más información, lea sobre el stalkerware.

Es posible que pueda conectar sus cuentas anteriores a su nuevo dispositivo, pero solo en caso de que pueda asegurarlas primero. Es posible que esto pueda ser inútil o inseguro si la otra persona tiene acceso físico a su dispositivo, o si le amenaza o coacciona para que comparta su contraseña. Revise los pasos anteriores para proteger sus cuentas.

Conclusión

Para las personas sobrevivientes, la nube, como cualquier otra tecnología, puede representar un riesgo si se le da un mal uso, pero también puede generar grandes beneficios. Es importante entender la manera en la que alguien podría acceder a su información a través de la nube, para que de esa manera, usted pueda minimizar los riesgos de seguridad y privacidad. Dependiendo de su situación, la nube puede ser muy útil para almacenar una gran cantidad de información de forma segura, (como fotos, documentos, sus actividades). Una persona intercesora puede asistir para evaluar los riesgos y beneficios y ayudarle a decidir si esta herramienta es adecuada para usted.

 Financiado por US DOJ-OVW Subvención Número 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 frecuentemente. Visite TechSafety.org para consultar la última versión de este y otros materiales.