Consejos de seguridad y privacidad para la antigua tecnología

Las conversaciones sobre el abuso de la tecnología y la privacidad tecnológica se centran a menudo en los dispositivos, servicios y plataformas más recientes y modernos. Sin embargo, las tecnologías más antiguas, como los teléfonos inalámbricos y las máquinas de fax, no sólo se siguen utilizando, sino que siguen siendo muy importantes para las personas sobrevivientes del abuso. Algunas personas agresoras utilizan la antigua tecnología para acechar y acosar, y la antigua tecnología puede representar riesgos para la privacidad y puede afectar a la seguridad. Por ello, es importante comprender la manera en que se puede hacer mal uso de la antigua tecnología y cómo minimizar los riesgos.

Dele prioridad a su seguridad.

Esta fuente de información analiza algunas medidas de seguridad para ciertas antiguas tecnologías. Antes de profundizar en ello, mencionamos algunos aspectos sobre la seguridad:

- **Obtenga ayuda**. Atravesar situaciones de violencia, el abuso y el acoso puede ser difícil y peligroso, pero no tiene que hacerlo por su cuenta. Las personas intercesoras pueden ayudarle a encontrar los recursos locales y las opciones. También le pueden brindar la ayuda para a diseñar un plan que le permita a usted mantener su seguridad. Puede ponerse en contacto con la línea de ayuda nacional para que le conecten con los recursos locales.
- **Confíe en sus instintos.** Las personas agresoras suelen estar decididas a mantener el control y, una manera de hacerlo es a través de la tecnología. Hay medidas que usted puede tomar para asegurar sus dispositivos, aplicaciones (apps) y cuentas. No hay una forma

"definitiva" de abordar la situación. Lo que funciona para otra persona puede no funcionar o ser seguro para usted.

- **ATENCIÓN:** Hacer cambios suele alertar a la otra persona. La persona podría obligarle a desbloquear su teléfono o a compartir sus contraseñas. Podría volverse más agresiva. El hacer cambios también podría eliminar la evidencia.

Teléfonos inalámbricos.

Aunque el uso de los teléfonos inalámbricos tiende a desaparecer, siguen existiendo y en ocasiones pueden aumentar la seguridad. Es importante tener en cuenta las diferencias que existen, porque estos podrían ser una estrategia para la seguridad o también podrían representar un riesgo para la privacidad. En las zonas en las que la señal de los teléfonos móviles es poco fiable, puede ser útil tener un teléfono fijo en caso de emergencia. Sin embargo, algunos teléfonos inalámbricos antiguos pueden ser fácilmente interceptados, lo que significa que otra persona puede escuchar la conversación. Los teléfonos inalámbricos transmiten las conversaciones entre la unidad base y el teléfono de mano.

Los teléfonos inalámbricos más antiguos pueden ser análogos, lo que significa que se envían las ondas sonoras de su voz, mientras que los teléfonos digitales más recientes envían información que puede estar codificada o encriptada. Las llamadas de los teléfonos análogos más antiguos podrían ser interceptadas por escáner, monitores de bebés u otros teléfonos inalámbricos. Los teléfonos domésticos más nuevos, inalámbricos o no, pueden transmitir las llamadas a través de Internet (lo que se llama VoIP), y utilizan la codificación para dar seguridad a las conversaciones.

Estrategias de seguridad.

- Antes de intercambiar información sensible, cambie a un teléfono fijo o con cable o a un teléfono móvil seguro (que crea usted que no pueda ser controlado a distancia).
- Si cambia a un teléfono fijo o con cable, desconecte la unidad base inalámbrica después de realizar la llamada, para asegurarse de que la conversación no siga siendo transmitida y escuchada.

Fax.

Las máquinas de fax se siguen utilizando en las empresas, los servicios jurídicos y los tribunales para enviar documentos, ya sea a través de una línea telefónica o de Internet. La información que aparece en la parte superior del fax se denomina encabezado, e incluye el número de fax del remitente. Esto podría utilizarse para determinar la ubicación si alguien hace una búsqueda inversa del número de teléfono. La mayoría de las máquinas de fax tienen discos duros que guardan un registro de los faxes que se han enviado y recibido, y a menudo también una copia del propio fax. Es posible que otra persona pueda ver su fax más adelante. Los faxes electrónicos (e-faxes) se envían a través de Internet como archivos adjuntos de correo electrónico y, al igual que el correo electrónico normal, podrían ser interceptados si alguien tiene acceso a la cuenta de correo electrónico.

Estrategias de seguridad.

- A veces, un fax puede ser reenviado a otro destinatario, a parte de la persona a quien usted se lo envía. Por ejemplo, un fax enviado a su abogado podría ser enviado posteriormente al abogado de la persona agresora.
    - Puede solicitar que se elimine la información del encabezado antes de ser reenviado para proteger su privacidad.

    - Antes de utilizar un fax público (como el de una tienda), analice la información que enviará por fax y determine si su uso podría afectar su privacidad. Si no siente la seguridad de poder enviarlo desde ese lugar, hable con un proveedor de servicios para víctimas sobre otras opciones.
- Evite enviar información personal o confidencial a través de un e-fax.
- Si se trata de enviar un fax a un lugar donde hay varias personas, avise con anticipación a la persona a la que se lo enviará para que ella misma esté presente para recibirlo y pueda retirarlo de inmediato.

Servicios TTY y de retransmisión.

TTY significa teletipo. Un TTY es un dispositivo para personas sordas o con impedimentos auditivos que se conecta a una línea telefónica. El TTY también puede utilizarse a través de una aplicación o una computadora. La retransmisión es un servicio gratuito en el que un operador facilita la conversación entre una persona que utiliza un TTY y otra que no lo tiene. El registro de llamadas o las transcripciones de TTY pueden guardarse en papel o de manera electrónica. Las personas agresoras que vigilan las llamadas TTY o una conversación de retransmisión, podrían ver o grabar esta información. Como la comunicación por TTY es escrita, podría ser más fácil para una persona agresora hacerse pasar por otra.

Estrategias de seguridad.

- Para mantener la privacidad, podría eliminar regularmente el historial del TTY o destruir la impresión en papel. Sin embargo, una persona agresora podría darse cuenta, lo que podría ser un riesgo para la seguridad.

- Otra alternativa podría ser considerar la posibilidad de guardar la transcripción de una conversación de TTY como prueba de acoso o abuso.
- Para evitar la suplantación de identidad, establezca una palabra o frase clave para que los demás sepan que es usted.
- Si es posible, utilice un TTY, un dispositivo o una computadora "más seguro" al que no tenga acceso la persona agresora, o reúnase en persona para hablar de información delicada.

Hardware de registro de pulsaciones de teclas.

Son dispositivos que pueden registrar todo lo que se escribe en un teclado. Los hardware de registro de pulsaciones de teclas pueden parecer pequeños conectores o un enchufe que conecta al teclado a la computadora, algo conectado a un puerto USB o incluso un teclado externo. Los datos de las pulsaciones de teclas pueden incluir contraseñas, lo que podría dar a alguien acceso al correo electrónico, a las cuentas bancarias, etc.

Es posible que alguna persona haya instalado uno si ha accedido a su computadora o la ha arreglado, o le ha dado una pieza nueva. La información registrada por el hardware de registro de pulsaciones puede leerse a distancia o en persona.

Estrategias de seguridad

- Revise si hay algún dispositivo o enchufe conectado a su computadora o teclado que no reconozca o que usted no haya colocado.
- Tenga precaución al retirar cualquier objeto que encuentre. Podría alertar a la persona agresora o borrar las evidencias de abuso. Puede

consultar con una persona intercesora sobre sus opciones y planear una estrategia de seguridad.

- Si decide dejar el registro de pulsaciones en su lugar y necesita pedir ayuda, acceder a cuentas confidenciales o cambiar las contraseñas de las cuentas, considere la posibilidad de utilizar un dispositivo diferente al que la persona agresora no tenga acceso, por ejemplo, hacer uso de una computadora en una biblioteca o el teléfono de alguna de sus amistades.

Apoyado por el DOJ-OVW de los Estados Unidos. Subvención No. 15JOVW-21-GK-02255-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas, pertenecen a los autores y no representan necesariamente las opiniones del DOJ.

Actualizamos nuestros contenidos frecuentemente. Visite TechSafety.org para obtener la última versión de este y otros materiales.