Cómo comprender el cifrado:
Las conexiones con la seguridad del sobreviviente

Para muchos sobrevivientes de violencia doméstica, violencia sexual, hostigamiento y trata de personas, contar con formas privadas y seguras de comunicarse y almacenar archivos digitales es parte vital de su seguridad. Para los proveedores de servicios dirigidos a las víctimas y otros profesionales que trabajan con sobrevivientes de abuso, usar herramientas de comunicación y almacenamiento que prioricen la privacidad y la seguridad les ayuda a garantizar que están respaldando la privacidad y seguridad del sobreviviente. Un cifrado fuerte es parte crucial de la solución.

Estos son algunos ejemplos de cómo el cifrado E2E y el cifrado de conocimiento cero pueden ayudar a mitigar los impactos del abuso facilitado por la tecnología.

1. Planificación de la seguridad y reubicación:

El cifrado de extremo a extremo puede ofrecer un canal seguro para que un sobreviviente haga planes y se comunique con personas en las que confía como, por ejemplo, cuando está intentando reubicarse y conseguir una vivienda y obtener apoyo. (Esto es particularmente cierto cuando la persona que comete el abuso no tiene acceso a los dispositivos o cuentas del sobreviviente).

2. Cómo proteger la integridad de las pruebas:

El uso de cifrado E2E y de conocimiento cero al almacenar y transferir pruebas digitales a las fuerzas del orden, fiscales u otros profesionales del sistema legal, ayuda a mantener la integridad de esas pruebas. Cuando las pruebas digitales pasan a través de fuentes no seguras o cuando existe la posibilidad de interceptación, la integridad de las pruebas puede reducirse, aumentando la posibilidad de que su autenticidad sea puesta en duda en un tribunal de justicia.

3. Cómo proteger la integridad de las pruebas:

El uso de cifrado E2E y de conocimiento cero al almacenar y transferir pruebas digitales a las fuerzas del orden, fiscales u otros profesionales

¿Qué es el cifrado y cómo funciona?

En términos generales, el cifrado es el proceso de codificar información de forma que solo pueda ser leída por aquellos que tienen acceso a las claves necesarias para decodificarla. Este proceso de decodificación recibe el nombre de descifrado. No todos los cifrados son iguales, y algunas plataformas de comunicación y almacenamiento en línea usan métodos de cifrado débiles. Para garantizar que los sobrevivientes sigan controlando su información, es importante que ningún tercero tenga la clave de acceso a sus comunicaciones o información almacenada en la nube.

El cifrado de extremo a extremo (E2E) ofrece el nivel más fuerte de seguridad y confianza para las tecnologías de la comunicación, porque, a propósito, solo el dispositivo del remitente y el dispositivo del destinatario deseado tienen las claves para descifrar el mensaje. Para los casos en que la información delicada debe ser almacenada de forma segura en línea, el estándar debería ser el cifrado de "conocimiento

del sistema legal, ayuda a mantener la integridad de esas pruebas. Cuando las pruebas digitales pasan a través de fuentes no seguras o cuando existe la posibilidad de interceptación, la integridad de las pruebas puede reducirse, aumentando la posibilidad de que su autenticidad sea puesta en duda en un tribunal de justicia.

4. Cómo buscar ayuda:

El cifrado E2E permite a los sobrevivientes comunicarse de forma segura y protegida cuando decidan buscar ayuda. Los ayuda a protegerse contra la interceptación, eliminación o alteración. Ayuda a garantizar que las comunicaciones privadas se mantengan así, de forma que solo los dispositivos del remitente y del destinatario deseado puedan acceder a los mensajes.

Proteger el cifrado de extremo a extremo para proteger a los sobrevivientes

El cifrado fuerte es una herramienta que ayuda a proteger la privacidad y seguridad de los sobrevivientes. Lamentablemente, los esfuerzos por socavar el cifrado E2E y el cifrado de conocimiento cero también socavarán la privacidad y seguridad del sobreviviente. Usar formas más débiles de cifrado o crear puertas falsas a los métodos más seguros de cifrado suponen una amenaza para la seguridad de todos aquellos que dependen de él para una comunicación privada.

La mejor forma de mantener seguras a las personas en línea es continuar manteniendo prácticas implacables de cifrado de extremo a extremo y de cifrado de conocimiento cero, y adoptar y reforzar políticas de cifrado fuerte. Los sobrevivientes de violencia doméstica, agresión sexual, hostigamiento y trata de personas merecen saber que sus comunicaciones privadas permanecen confidenciales mientras buscan apoyo, y que las pruebas que recaban pueden ser conservadas sin riesgo de manipulación o eliminación maliciosa. Cuando la tecnología basada en cifrado E2E y de conocimiento cero está disponible para los sobrevivientes, se les empodera con más opciones para encontrar ayuda, seguridad y recuperación.

Obtenga más información sobre los elementos técnicos y humanos del cifrado en www.internetsociety.org, y sobre cómo ayudar a los sobrevivientes en www.techsafety.org. Siga nuestro trabajo en Twitter en @internetsociety y @nnedv.