Cifrado:

Cómo puede proteger a los grupos de defensa y a los movimientos de cambio social

Octubre 2021

El cifrado es una herramienta diseñada para ayudar a los usuarios de Internet a mantener la privacidad y la protección de su información y sus comunicaciones en línea. Desempeña un papel fundamental en la protección de las actividades digitales cotidianas, como la banca en línea, las compras, la prevención del robo de información confidencial en caso de fugas de datos, así como para asegurarse de que se mantenga la privacidad de los mensajes que deben ser privados.

El cifrado es esencial para proteger la libertad de expresión y la privacidad. Para algunas comunidades, como las personas defensoras de derechos humanos, los grupos de defensa, las organizaciones comunitarias y sus actores, el cifrado es particularmente crucial y debe usarse con otras herramientas más convencionales de protección de la privacidad para mantener la seguridad de las personas, tanto en línea como en su vida cotidiana.

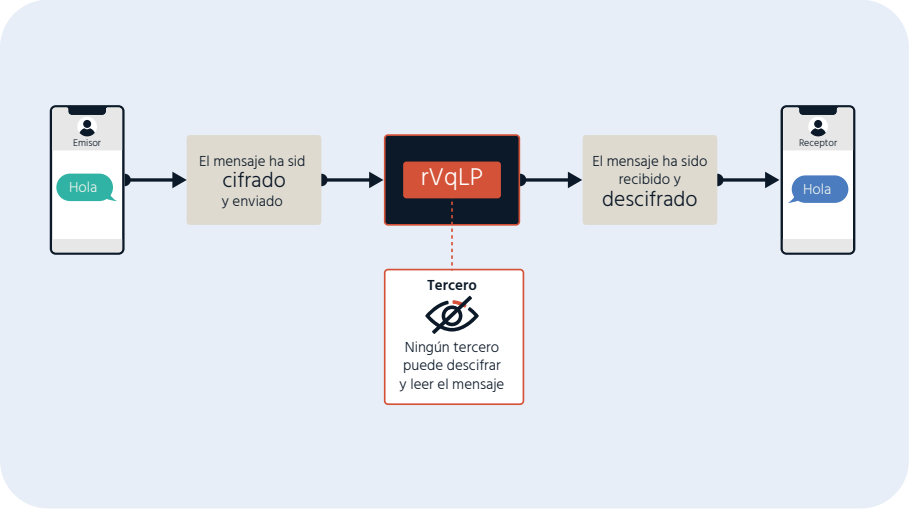
Cómo el cifrado respalda la seguridad de los grupos de defensa

El cifrado es una herramienta esencial que permite a los grupos de defensa aumentar la percepción del público sobre los casos de violaciones de derechos humanos y hacer que los gobiernos asuman su responsabilidad. Si los grupos de defensa no pueden compartir recursos e involucrar a los actores con confidencialidad, no pueden defender los derechos humanos de manera segura. Del mismo modo, si los grupos de defensa no pueden proteger el anonimato de quienes respaldan a su comunidad, es posible que quienes los respaldan no se hagan presentes, en detrimento del público, ya que los derechos humanos continúan deteriorándose. Estas son algunas de las formas en que los grupos de defensa dependen del cifrado:

- Participación de forma segura con los actores comunitarios: los miembros de la comunidad, incluidos periodistas, grupos de interés, académicos e individuos, compartirán recursos e información personal sobre sí mismos solo si los grupos de defensa garantizan la protección de su identidad. El cifrado de extremo a extremo permite a los grupos de defensa crear una relación de confianza con su comunidad, haciendo crecer su movimiento y reduciendo al mínimo el riesgo para los individuos.
- Protección de la integridad de la información: los grupos de defensa deben indicar de manera confiable a la comunidad que han compartido información digna de confianza. Los protocolos de Internet, como HTTPS, ayudan a proteger los datos a medida que pasan entre los sitios web y los lectores. También protegen de la censura a los grupos de defensa: es más difícil para los censores bloquear mensajes o acceder a los sitios web si no pueden interceptar el contenido.
- Protección contra ataques personales: hay muchos casos de grupos de defensa cuyos dispositivos y plataformas en línea han sido hackeados y vigilados por actores gubernamentales y privados, incluido un caso en el que el software espía de NSO Group se utilizó para vigilar a más de 50 000 objetivos, incluidos jefes de Estado, activistas y periodistas, según lo reveló el Proyecto Pegasus. Los grupos de defensa también enfrentan amenazas como abusos en línea, doxxing (recopilación y publicación de información personal en línea), acoso y, en casos extremos, secuestro y actos de violencia. Si bien los grupos de defensa deben permanecer alerta ante una gran cantidad de técnicas de vigilancia, tanto digitales como más tradicionales, el cifrado de extremo a extremo ayuda a aumentar la protección de sus comunicaciones contra la vigilancia e interceptación por parte de terceros. Si bien el hackeo y la vigilancia aún pueden ocurrir en los dispositivos de los usuarios, debilitar los servicios de cifrado o no usarlos en absoluto haría que estos ataques sean aún más fáciles y frecuentes.

Internet Society

Cifrado



- Hacer que los gobiernos y las instituciones rindan cuentas: una parte importante de la defensa de los derechos humanos es la capacidad de hacer que las personas e instituciones que ostenten el poder asuman la responsabilidad por sus decisiones y acciones. Para hacer esto, es fundamental que los grupos de defensa tengan herramientas de seguridad digital que eviten que entidades poderosas, nacionales o extranjeras, accedan o modifiquen sus investigaciones, conversaciones y bases de datos comunitarias.
- Una política de cifrado sólida protege a los grupos de defensa en todas partes: cuando los países respaldan el cifrado de extremo a extremo, ayudan a los grupos de defensa locales e internacionales al establecer un estándar para las protecciones de cifrado global. Cuando los países debilitan el cifrado, sientan un peligroso precedente del que podrían abusar los gobiernos extranjeros que carecen de los mismos estándares sólidos de estado de derecho.

¿Qué es el cifrado?

El cifrado es el proceso de codificar la información para que solo pueda leerlo alguien con las claves para abrir y descifrar la información. El cifrado de extremo a extremo (E2E) proporciona el nivel más fuerte de seguridad y confianza, porque según el diseño, solo el destinatario tiene la clave para descifrar el mensaje. Ningún tercero debe tener acceso a esa clave. Pero algunos gobiernos y organizaciones están presionando para debilitar el cifrado como un medio para combatir el delito.

Por qué las puertas traseras de cifrado no son la respuesta

Las fuerzas del orden y las agencias de inteligencia solicitan cada vez más "puertas traseras de cifrado" para interceptar o acceder a comunicaciones cifradas para ayudarse a 'capturar a los malos' u ordenar a las empresas que lo hagan por ellos. Esto no solo debilita la infraestructura global de Internet; también pone la vida de las personas defensoras de derechos humanos en mayor riesgo de sufrir perjuicios. Así es como funciona:

- La debilidad forzada nos debilita a todos: cualquier punto de entrada a un servicio seguro es una debilidad. Las puertas traseras de cifrado ponen en riesgo la información y las conversaciones privadas porque permiten que el gobierno acceda a la información privada de usted, pero al mismo tiempo crea un acceso para los actores maliciosos a través del mismo punto de entrada. No existe una cerradura digital que solo puedan abrir los 'buenos' y otros no.
- La criminalidad es subjetiva: Si bien las autoridades pueden argumentar que las puertas traseras del cifrado pueden ayudar a atrapar a los delincuentes, en demasiados países la insuficiencia de los estándares del estado de derecho hace que las autoridades persigan penalmente y acosen a los verdaderos defensores de los derechos humanos. En algunos países, los grupos de defensa y los actores humanitarios pueden ser sometidos a prisión, tortura e incluso a pena de muerte por llamar la atención sobre los abusos en contra de los derechos humanos y ejercer su libertad de expresión. Sin el cifrado, es posible que los defensores que vivan en estos países o viajen a ellos no puedan defender de manera segura y cómoda a las víctimas de abuso y quedarían vulnerables al procesamiento judicial y la persecución.
- La falta de cifrado puede erosionar los mecanismos para hacer que los grupos de poder asuman su responsabilidad: si los grupos de defensa no tienen una forma segura de realizar su trabajo, pueden optar

Internet Society

por no perseguir problemas de alto perfil debido a la posible reacción, el escrutinio y el acoso que pueden recibir. Una nación democrática saludable necesita una comunidad fuerte y con voz para llamar la atención sobre el impacto social de las acciones de los gobiernos, instituciones, empresas y otros actores poderosos.

Proteja el cifrado, protéjase a sí mismo

Proteja nuestras herramientas digitales más fuertes para mantener a salvo a las personas mientras estén en línea. Tanto los grupos de defensa como el público necesitan estar seguros en línea para hacer que los gobiernos e instituciones asuman su responsabilidad, así como para contar historias importantes e impactantes y promover democracias saludables.

- Utilice servicios de comunicaciones cifradas de extremo a extremo.
- Obtenga más información sobre cómo funciona el cifrado, por qué está bajo amenaza y cómo puede protegerlo.
- Tome el curso de capacitación gratuito en línea sobre cifrado de Internet Society.
- Únase a los Amigos de la Coalición Global por el Cifrado para mantenerse actualizado con las noticias más recientes sobre cifrado de todo el mundo.
- Únase a su Capítulo local de Internet Society para defender el cifrado en su país o región.

Internet Society