Cifrado

Cómo puede proteger a los periodistas y la prensa libre

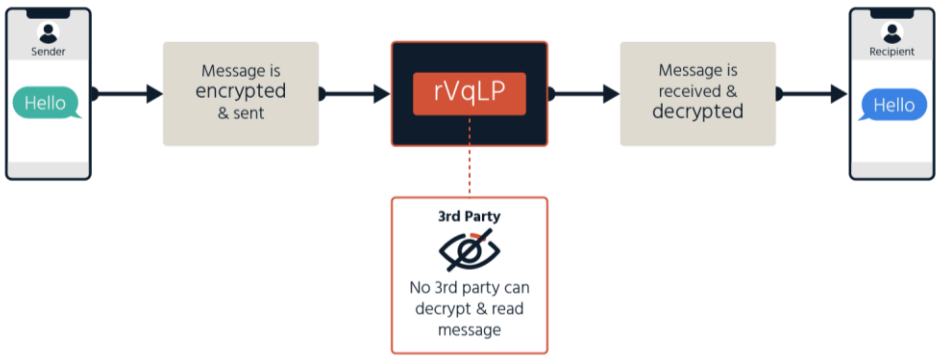
Agosto de 2022

El cifrado es una herramienta diseñada para ayudar a los usuarios de Internet a mantener su información en línea y sus comunicaciones privadas y seguras. 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 las violaciones de datos, así como para asegurarse de que se mantenga la privacidad de los mensajes privados.

El cifrado es esencial para proteger la libertad de expresión y la privacidad.

¿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 la clave.



Para algunos grupos o comunidades, como los periodistas, el cifrado es especialmente crucial para mantener a las personas seguras y garantizar una libertad de prensa saludable.

Cifrado y seguridad periodística

El cifrado es una herramienta esencial para los periodistas. Si los periodistas no pueden comunicarse en confianza con sus colegas y fuentes, no pueden hacer su trabajo de manera segura. Del mismo

modo, si no pueden proteger el anonimato de sus fuentes, esas fuentes pueden no presentarse y el público pagará el precio.

Conexión segura con las fuentes: las fuentes de los periodistas a veces comparten información incriminatoria sobre una institución o información personal sobre sí mismos solo si los periodistas aceptan proteger su identidad. El cifrado de extremo a extremo permite a los periodistas construir una relación de confianza con estas fuentes.

Protección de la integridad de la información: los periodistas deben señalar de manera confiable a los lectores que han creado contenido confiable y asegurarse de que coincida con lo que su público objetivo puede ver en línea.

Los protocolos de Internet como HTTPS ayudan a proteger los datos a medida que pasan entre los sitios web de noticias y el lector. También protege al periodismo de la censura: es más difícil para los censores bloquear mensajes o acceder a noticias si no pueden interceptar el contenido.

Protección contra los atacantes: hay muchos casos de periodistas y medios de comunicación cuyos dispositivos y plataformas en línea han sido pirateados y vigilados por actores gubernamentales y privados sobre sus informes, incluido un caso en el que la Agencia de Seguridad Nacional de EE. UU. (NSA) pirateó los informes del Sistema de comunicación interna de Al-Jazeera. Los periodistas también se enfrentan a amenazas como el abuso en línea, *doxxing* (recopilación y publicación de información personal en línea) y acoso. El cifrado de extremo a extremo ayuda a proteger sus comunicaciones de la vigilancia e interceptación por parte de terceros.

Responsabilizar a los gobiernos y a las instituciones: un componente importante del periodismo es su capacidad para responsabilizar a las personas e instituciones en el poder por sus decisiones y acciones. Para hacer esto, es fundamental que los periodistas tengan herramientas de seguridad digital que eviten que entidades poderosas, nacionales o extranjeras, accedan y/o alteren sus investigaciones, conversaciones y fuentes.

Una política de cifrado sólida protege a los periodistas en todas partes: cuando los países admiten el cifrado de extremo a extremo, ayudan a los periodistas en sus propias naciones y en todo el mundo al establecer un estándar para las protecciones de cifrado globales.

· El cifrado permitió a los periodistas exponer la corrupción global

La filtración de los Panama Papers comenzó a fines de 2014 cuando una fuente desconocida contactó a Bastian Obermayer, un reportero del periódico alemán Suddeutsche Zeitung. Obermayer dice que la fuente lo contactó a través de un chat cifrado y le ofreció datos destinados a "hacer públicos estos crímenes". Pero la fuente advirtió que su "vida estaba en peligro", solo estaba dispuesto a comunicarse a través de canales cifrados y se negó a reunirse en persona. La filtración de los Panama Papers reveló el sistema de evasión fiscal global de una firma de abogados panameña para sus clientes. Comprendió 2,6 terabytes de datos (11,5 millones de documentos) e involucró a alrededor de 400 periodistas de más de 100 organizaciones de medios en más de 80 países que trabajaron juntos para contar las historias ocultas en su interior.

El cifrado ayudó al denunciante a conectarse con los periodistas

En 2015, The Intercept recibió archivos de un individuo a través de SecureDrop, un software diseñado para ayudar a los denunciantes a filtrar información de forma anónima a los medios. La historia mostró que Securus, una compañía que brinda servicios telefónicos a más de 2200 prisiones en los EE. UU., mantuvo registros de cada llamada telefónica realizada por los más de 1,2 millones de presos que usan el servicio en 37 estados, incluida la hora, los números telefónicos a los que llamaron, nombres de los presos e incluso las grabaciones de audio de cada llamada. Los registros se vendían rutinariamente a clientes de las fuerzas del orden público, incluidas las conversaciones de los reclusos con los abogados que deberían ser protegidas por el privilegio abogado-cliente. La sorprendente revelación solo apareció porque una persona que accedió a los archivos los compartió con The Intercept a través de SecureDrop.

Por qué el "Acceso excepcional" no es la respuesta

Por lo general, el "acceso excepcional" se refiere a otorgar a las agencias de aplicación de la ley y de inteligencia el poder de interceptar y acceder a comunicaciones cifradas u obligar a las empresas a hacerlo por ellos. Esto no solo debilita la seguridad en Internet; también pone a los periodistas en riesgo tanto en línea como en la vida real. Así es como funciona:

- **La debilidad forzada nos debilita a todos**: cualquier punto de entrada a un servicio seguro es una debilidad. El acceso excepcional pone en riesgo la información privada y las conversaciones porque permite el acceso del gobierno a su información privada y al mismo tiempo crea una puerta para los actores maliciosos. No existe una cerradura digital que puedan abrir solo los "buenos" y otros no.
- **La falta de cifrado puede disuadir a los periodistas de publicar contenido riesgoso**: si los periodistas no tienen una forma segura de realizar su trabajo, pueden optar por no buscar historias sensibles debido a las posibles reacciones violentas, al escrutinio y al acoso que puedan recibir. Una nación democrática sana necesita una prensa libre, fuerte e independiente para informar al público sobre las acciones de los gobiernos, las instituciones y las empresas en las que elige confiar.

Recomendación

Proteja la libertad de prensa defendiendo un cifrado sólido de extremo a extremo y garantizando que los periodistas y el público tengan libertad para usarlo. Los periodistas deben estar seguros en línea

para hacer que los gobiernos e instituciones rindan cuentas, contar historias importantes e impactantes, proteger sus fuentes y promover democracias saludables.

Obtenga más información sobre cómo el cifrado afecta a los periodistas

Para obtener más información, visite www.cpj.org y @pressfreedom en Twitter.

Capacitación y recursos de cifrado de Internet Society

https://www.internetsociety.org/es/issues/encryption/resources/

https://www.internetsociety.org/es/learning/encryption/