Criptografia

BRASIL 2022

Internet Society Capítulo Brasil

CPJ

Como pode proteger jornalistas e a Liberdade de Imprensa

A criptografia é uma ferramenta projetada para ajudar os usuários da Internet a manter seus dados e comunicações online confidenciais e seguros. Ela pode desempenhar um papel fundamental na proteção de atividades digitais diárias, como transações bancárias e compras online, prevenindo vazamentos de dados e garantindo que as mensagens permaneçam privadas.

A criptografia é essencial para estabelecer uma base de confiança online que ajude a proteger a liberdade de expressão e a privacidade.

O que é criptografia?

Criptografia é o processo de embaralhar ou codificar arquivos e conteúdos, para que só possam ser lidos por alguém que tenha os meios de fazê-los retornarem a seu estado original.

Criptografia de ponta a ponta (E2E, end-to-end) é qualquer forma de criptografia em que apenas o remetente e o destinatário pretendido têm as chaves para descriptografar a mensagem. O aspecto mais importante da criptografia de ponta a ponta é que terceiros, até mesmo a empresa que fornece o serviço de comunicação, não têm conhecimento das chaves de criptografia.

Para algumas comunidades, como jornalistas, a criptografia é especialmente crucial para manter as pessoas seguras e garantir uma liberdade de imprensa saudável.

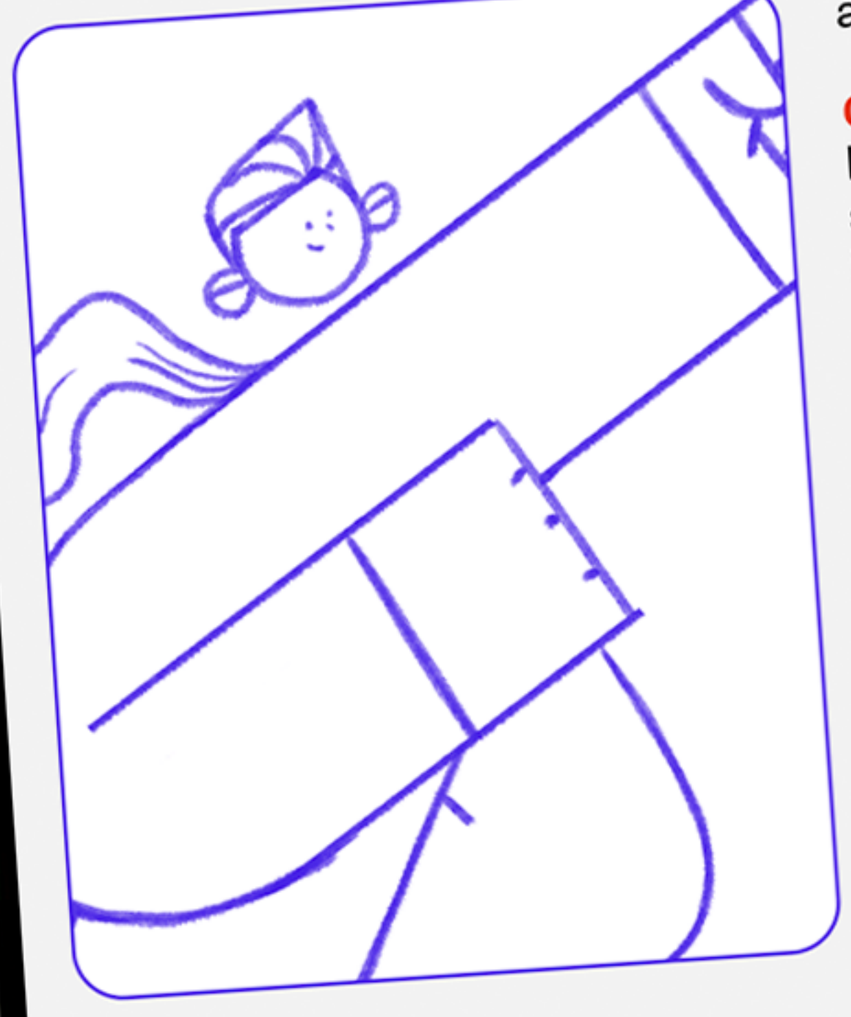
Criptografia

BRASIL 2022

CPJ

Internet Society Capítulo Brasil

Criptografia e a segurança de jornalistas



A criptografia é uma ferramenta essencial para jornalistas. Se não puderem se comunicar de forma privada com colegas e fontes, não poderão fazer seu trabalho em segurança. Da mesma forma, se não puderem proteger o anonimato de suas fontes, essas fontes podem não se apresentar, e o público pagará o preço.

Conectando-se de forma segura com fontes: Muitas vezes as fontes dos jornalistas somente compartilham informações incriminatórias sobre uma instituição ou informações pessoais sobre si mesmas se os jornalistas concordarem em proteger suas identidades. A criptografia de ponta a ponta permite que os jornalistas construam um relacionamento baseado em confiança com essas fontes.

Protegendo a integridade da informação: os jornalistas precisam demonstrar aos leitores que criaram um conteúdo confiável e garantir que suas informações correspondam ao que seu público-alvo possa checar online.

Protocolos de Internet como HTTPS ajudam a proteger os dados à medida que passam entre os sites de notícias e o leitor. Isso também protege o jornalismo da censura: é mais difícil para os censores bloquearem mensagens ou acesso a notícias se eles não podem interceptar o conteúdo.

Proteção contra ataques: há muitos casos de jornalistas e agências de notícias que tiveram seus dispositivos e plataformas online hackeadas e vigiadas por atores governamentais e privados por causa de suas reportagens, incluindo um caso em que a Agência de Segurança Nacional dos EUA (NSA) supostamente invadiu o sistema de comunicação interno da Al-Jazeera. Os jornalistas também enfrentam ameaças como abuso online, doxxing (coleta e publicação de informações pessoais online) e perseguição. A criptografia de ponta a ponta ajuda a proteger as comunicações de interceptação e vigilância por terceiros.

Responsabilizando governos e instituições: um componente importante do jornalismo é sua capacidade de responsabilizar pessoas e instituições no poder por suas decisões e ações. Para fazer isso, é fundamental que os jornalistas tenham ferramentas de segurança digital que impeçam entidades poderosas, domésticas ou estrangeiras, de acessar e/ou alterar suas pesquisas, conversas e fontes.

Uma forte política de criptografia protege jornalistas em todos os lugares: quando os países apoiam criptografia de ponta a ponta, eles ajudam jornalistas em seus próprios países e em todo o mundo, definindo um padrão global de proteção para a criptografia.

Criptografia

BRASIL 2022

A criptografia já permitiu que jornalistas expusessem a corrupção global

O vazamento conhecido como Panamá Papers começou no final de 2014, quando uma fonte desconhecida entrou em contato com Bastian Obermayer, repórter do jornal alemão Suddeutsche Zeitung. Obermayer diz que a fonte o contatou por meio de bate-papo criptografado e ofereceu dados destinados a "trazer a público esses crimes". A fonte alertou, porém, que sua "vida estaria em perigo" e que só estaria disposta a se comunicar por meio de canais criptografados, se recusando a encontrar-se pessoalmente. O vazamento do Panamá Papers revelou o sistema global de evasão fiscal de um escritório de advocacia panamenho para seus clientes. Foram 2,6 terabytes de dados, 11,5 milhões de documentos, que envolveram cerca de 400 jornalistas de mais de 100 meios de comunicação, em mais de 80 países.

A criptografia já ajudou um denunciante a se conectar com jornalistas

Em 2015, o Intercept recebeu arquivos de um indivíduo por meio do SecureDrop, software desenvolvido para ajudar denunciantes a vazar informações anonimamente para a mídia. A reportagem mostrou que a Securus, empresa que presta serviços telefônicos a mais de 2.200 presídios nos EUA, manteve registros de todas as ligações feitas pelos mais de 1,2 milhão de presos que usam o serviço em 37 estados, incluindo horário, números de telefone chamados, nomes de presos e até mesmo as gravações de áudio de cada chamada. Os registros eram rotineiramente vendidos a policiais e promotores, incluindo conversas de presos com advogados que deveriam ser protegidas pelo privilégio advogado-cliente. A revelação chocante só veio à tona porque um indivíduo que acessou os arquivos os compartilhou com o The Intercept via SecureDrop.

Porque o “acesso excepcional” não é a resposta

O "acesso excepcional" geralmente se refere a dar às agências de segurança e de inteligência o poder de interceptar e acessar comunicações criptografadas para ajudar a "capturar os caras maus" ou ordenar que as empresas as acessem diretamente. Isso não apenas enfraquece a infraestrutura global da Internet, mas também coloca jornalistas em maior risco de dano. **Veja como:**

Enfraquecer propositalmente a criptografia deixa todos mais vulneráveis: qualquer ponto de entrada para um serviço seguro é uma fraqueza. O acesso excepcional coloca informações e conversas privadas em risco porque permite ao Estado o acesso às suas informações privadas, mas simultaneamente cria uma porta de entrada para atores mal-intencionados pelo mesmo ponto de acesso. Não há fechadura digital que apenas os 'mocinhos' possam abrir e outros não.

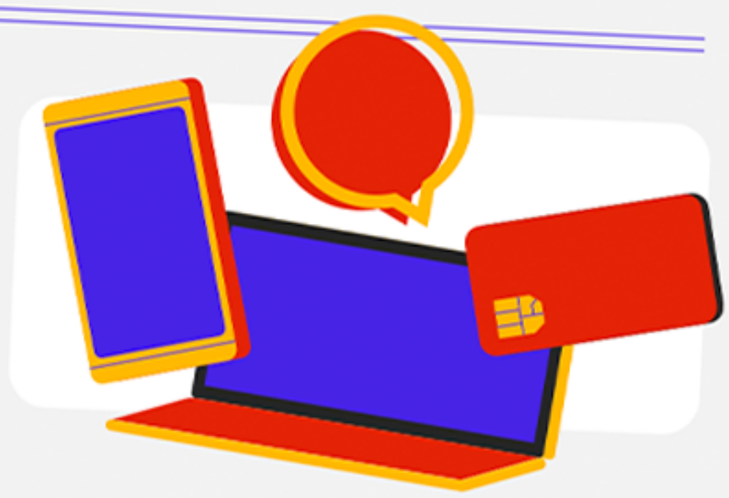
A falta de criptografia pode impedir jornalistas de publicar conteúdos que possam ser arriscados: se os jornalistas não têm uma maneira segura de realizar seu trabalho, eles podem optar por não buscar histórias sensíveis devido à possível reação, escrutínio e assédio. Uma nação democrática saudável precisa de uma imprensa livre, forte e independente para informar o público sobre as ações de governos, instituições e empresas.

Criptografia
BRASIL 2022

CPJ

Internet Society
Capítulo Brasil

Nós usamos a CRIPTOGRAFIA todos os dias



Navegação na Internet: Navegadores e websites usam o HTTPS. um protocolo criptografado, de forma a oferecer comunicação segura, fazendo com que nossos dados não possam ser lidos por criminosos enquanto estiverem em trânsito.

Comércio eletrônico: Nós confiamos às empresas a proteção de nossas informações bancárias quando fazemos compras ou usamos o banco na Internet. A criptografia é um importante método de se obter isso.

Mensagens seguras: Quando usamos um aplicativo de mensagens, esperamos que essas mensagens sejam particulares. Alguns aplicativos de mensagens usam criptografia para manter a privacidade e segurança das comunicações de seus usuários. Outros usam até mesmo criptografia ponto a ponto, de forma que apenas o remetente e o destinatário possam ler as mensagem, por exemplo, iMessage, WhatsApp e Signal.

Recomendação

Proteger a liberdade de imprensa defendendo uma criptografia forte de ponta a ponta e garantindo que os jornalistas e o público em geral são livres para usá-la. Os jornalistas precisam estar seguros no ambiente online para garantir que governos e instituições possam ser responsabilizados, para contar histórias importantes e impactantes, para proteger suas fontes e promover democracias saudáveis.

Saiba mais sobre como a criptografia afeta os jornalistas

Instituto Iris: A criptografia para a proteção da atividade jornalística

https://irisbh.com.br/a-criptografia-para-a-protecao-da-atividade-jornalistica/

Recursos e treinamento sobre criptografia da Internet Society

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

Para mais informações, acesse www.cpj.org e @pressfreedom no Twitter.