INTERCAMBIAR DE ARCHIVOS Y COMUNICARSE DURANTE UN APAGÓN DE INTERNET

El continuo bloqueo de internet y la represión en Cachemira, el apagón de internet más largo jamás impuesto en una democracia, ha tenido un impacto catastrófico en la vida de las personas en la región. Para agravar la situación, en diciembre de 2019, las cuentas de WhatsApp de Cachemira comenzaron a revocarse debido a los 120 días de inactividad de las personas usuarias según las políticas de WhatsApp.

Al momento de escribir este blog en enero de 2020, la Corte Suprema de la India dictaminó que el cierre indefinido en Cachemira es ilegal y un abuso de poder. La banda ancha limitada y la Internet móvil se han restaurado en algunas áreas, pero solo para algunos sitios web “incluidos en la lista blanca”.

Los apagones de Internet están diseñados para impedir que las personas compartan información y se comuniquen (y también empujan a las personas a formas de comunicación menos seguras, como teléfonos móviles y SMS, que son más fáciles de interceptar y controlar por las autoridades). No siempre hay buenas soluciones durante los apagones completos. Durante los períodos más estrictos del bloqueo en Cachemira, por ejemplo, las personas recurrieron al uso de notas escritas a mano y correos para enviar mensajes a sus seres queridos.

No tenemos formas seguras de eludir todos los bloqueos, pero a través de conversaciones con activistas y compañerxs, hemos aprendido algunos métodos y enfoques para compartir y comunicar sin conexión que pueden funcionar para ti, dependiendo de las circunstancias. Ten en cuenta que algunas de estas opciones requieren que Internet se configure inicialmente (por ejemplo, para descargar aplicaciones, etc.).

Comparte archivos directamente con Bluetooth, Wifi Direct o NFC

No necesitas tener una conexión a Internet para conectar tu teléfono con otro dispositivo cercano a través de Bluetooth, Wifi Direct o Near Field Communication (NFC) (a veces llamado Android Beam en dispositivos más antiguos). Bluetooth y Wifi Direct son tecnologías inalámbricas que pueden “emparejar” dos dispositivos sin otro enrutador o punto de acceso intermedio. WiFi Direct proporciona un rango más amplio y una transferencia de datos más rápida que Bluetooth, pero consume mucha más energía. Mientras tanto, NFC tiene un rango mucho más corto (~ 4 cm) y velocidades de transferencia mucho más lentas que Bluetooth o WiFi Direct, pero se conecta más rápido y usa menos energía, por lo que puede ser útil para transferencias pequeñas cuando tienes ambos dispositivos en tus manos.

Es probable que tengas funciones Bluetooth, WiFi Direct y NFC integradas en tu teléfono que se muestran en las opciones de uso compartido. Además, las aplicaciones con funciones para compartir archivos, como Files By Google, también integran estas tecnologías.

Importante: la desventaja de la facilidad de conexión proporcionada por estos servicios es que no son seguros. El bluetooth y los escaners de wifis se pueden usar para rastrear tu ubicación o buscar información en tu dispositivo. Los infiltrados pueden intentar emparejarse con tu dispositivo, enviarte archivos no deseados o incluso obtener el control de tu dispositivo si es vulnerable. **Para estar más segurx, desactiva estos servicios cuando no los estés utilizando y solo actívalos cuando estés en lugares seguros, limita los permisos de la aplicación solo a lo que necesitas y a quién necesitas, y practica una buena seguridad en tu teléfóno, como ejecutar actualizaciones y tener una buena contraseña de acceso.**

Comparte archivos con una unidad inalámbrica o mediante una red de área local inalámbrica (WLAN)

Se puede utilizar un disco duro inalámbrico o una unidad flash para compartir archivos entre un equipo o varias personas a la vez. La unidad wifi generalmente viene con instrucciones y/o una aplicación para conectar tu teléfono a la unidad, y es relativamente fácil de usar. Recuerda establecer una contraseña en el disco por seguridad.

Si no tienes una unidad inalámbrica, también puedes compartir archivos en una unidad USB normal conectándola a un enrutador inalámbrico. Un enrutador de viaje con un puerto USB, por ejemplo, es relativamente económico y muy portátil. Los usuarios pueden conectarse a la unidad USB a través de una red local (no se requiere internet). Para acceder a los archivos en la unidad USB conectada en tu teléfono, necesitarás usar una aplicación de administrador de archivos que pueda conectarse al almacenamiento en red, como Solid Explorer. La dirección IP de tu enrutador generalmente se puede encontrar en la configuración avanzada de wifi de tu teléfono.

Mientras tanto, otra opción es PirateBox, un proyecto de hágalo usted mismx que proporciona software con licencia gratuita. Los usuarios pueden compartir archivos como se indicó anteriormente, pero Piratebox les permite hacerlo de forma anónima, y también incluye funciones de chat y mensajería. Configurar un Piratebox requiere descargar, instalar y configurar algunas piezas de software. Las instrucciones están en el sitio web de Piratebox.

Actualización: el proyecto Pirate Box se está cerrando lentamente. El sitio web y el repositorio de Github todavía están en línea, pero la principal persona desarrolladora del proyecto ya no está dando mantenimiento activo.

Comunicarte a través del chat de peer to peer

Dos nuevas aplicaciones de mensajería entre pares que conocemos a través de redes activistas son Briar y Bridgefy. Todavía no los hemos probado, pero conocemos a otrxs que los están probando.

Briar es una aplicación de mensajería cifrada de código abierto de extremo a extremo que no se basa en un servidor central, sino que sincroniza los mensajes entre los dispositivos de los usuarios (por lo que el contenido reside en el dispositivo de cada usuario). Se puede sincronizar incluso cuando no hay internet usando Bluetooth o WiFi (cuando hay internet, la aplicación sincroniza dispositivos a través de la red Tor). Briar también presenta grupos privados, foros públicos y blogs. Cuando se usa sin conexión, su alcance está limitado por su alcance Bluetooth o WiFi (máximo ~ 100 metros).

Mientras tanto, Bridgefy es una aplicación de mensajería cifrada de extremo a extremo (excepto cuando se usa la función de "transmisión") que utiliza Bluetooth para enviar mensajes. A diferencia de Briar, los mensajes pueden viajar distancias más largas saltando a lo largo de una red mesh de otras personas usuarias de Bridgefy (solo el destinatarix puede leer el mensaje). Bridgefy carece de los grupos privados, foros y funciones de blog de Briar, pero tiene un modo de transmisión a través del cual puedes enviar un mensaje a hasta 7 usuarios de Bridgefy dentro del alcance, que no necesitan ser tus contactos (los mensajes de transmisión no están encriptados).

Comunicarte a través de SMS cifrados

Los mensajes de texto SMS se envían a través de redes celulares y no dependen de Internet, por lo que aún pueden funcionar durante los apagones de Internet. Sin embargo, los SMS se consideran muy inseguros. A diferencia de las aplicaciones dependientes de Internet como WhatsApp o Signal, los SMS no están encriptados de extremo a extremo. Esto significa que los mensajes de texto (y sus metadatos) pueden ser leídos por gobiernos y operadores de telefonía móvil, o interceptados por piratas informáticos. Los SMS también pueden ser "falsificados", lo que significa que un remitente puede manipular la información de su dirección para hacerse pasar por otro usuario.

Si necesitas usar SMS, Silence es una aplicación que encripta los mensajes SMS de extremo a extremo. Es de código abierto y utiliza el protocolo de cifrado de Signal. Si bien no lo hemos probado nosotrxs mismxs, hemos escuchado que otros lo han usado. Tanto el remitente como el destinatario deben tenerlo instalado e intercambiar claves entre ellos. Dado que los mensajes SMS pasan necesariamente por los servidores de sus telecomunicaciones, incluso con Silence el hecho de que estás enviando un mensaje cifrado y los metadatos sobre su mensaje serán accesibles para la compañía de telecomunicaciones.

Bloqueo parcial de Internet: acceder a sitios bloqueados

Un "apagón de Internet" a menudo no significa un apagón total de Internet, sino que bloquea el acceso a sitios web específicos o plataformas de redes sociales. Los gobiernos, a través de los proveedores de servicios de Internet (ISP), pueden bloquear sitios en función de la dirección IP, el contenido o las búsquedas de DNS. ¿No estás segurx si un sitio está siendo bloqueado?

Organizaciones como Open Observatory of Network Interference y Netblocks monitorean y miden las interrupciones de internet y la censura en todo el mundo.

Afortunadamente, siempre que tengas acceso a Internet, hay algunas maneras de tratar de sortear los bloqueos parciales. Al igual que con el cifrado, ten en cuenta que eludir los sitios bloqueados puede estar criminalizado en tu país.

VPN

Una forma de evitar el bloqueo basado en IP y en contenido es utilizar una red privada virtual o VPN, como ProtonVPN o TunnelBear. Cuando te conectas a través de una VPN, tu tráfico de Internet se cifra y se enruta a través de un servidor VPN en otra ubicación, como en otro país, ocultando así el verdadero destino y el contenido de tu tráfico a tu ISP.

Ten en cuenta que algunos gobiernos prohíben el uso de VPN o pueden intentar detectar y bloquear las conexiones VPN. También es importante utilizar un proveedor de VPN confiable, y preferiblemente uno que no almacene datos o registros, ya que el proveedor podrá ver tu actividad en Internet. Ten en cuenta en qué país se basa el proveedor de VPN y a qué procesos legales pueden estar sujetos según su jurisdicción. También considera que las VPN aprobadas por el gobierno pueden permitir la vigilancia e inspección de sus datos.

Servidores DNS

Los servidores DNS (“sistema de nombres de dominio”) funcionan traduciendo los nombres de dominio o URL que un usuario escribe en un navegador en las direcciones IP numéricas que Internet utiliza para identificar páginas web. Un ISP puede modificar los servidores DNS que controla para bloquear ciertas consultas o devolver una página incorrecta que dice que el sitio web no existe. En 2014, el primer ministro turco, Recep Tayyip Erdogan, intentó bloquear Twitter durante las elecciones turcas utilizando esta técnica. La prohibición fue frustrada rápidamente por activistas que compartieron consejos paso a paso sobre cómo usar las VPN y cambiar los servidores DNS.

Puedes cambiar el servidor DNS predeterminado en la configuración de red o wifi de tu teléfono. En lugar del servidor DNS predeterminado, puedes usar servidores DNS alternativos como Google Public DNS o CloudFlare para sortear los bloques basados en DNS. Cloudflare también tiene una aplicación llamada 1.1.1.1 que permite a los usuarios cambiar a un servidor DNS de Cloudflare a través de una interfaz de aplicación simple.

Estas son solo dos formas de eludir las técnicas de bloqueo más comunes. Consulta las guías de Internet Society, Access Now, Security-in-a-Box, y EFF para obtener información más detallada.