به‌اشتراک‌گذاری فایل‌ها و ارتباطات در زمان خاموشی اینترنت

سرکوب و خاموشی اینترنتی که در کشمیر جاری است، طولانی‌ترین قطعی اینترنت است که در دل یک دموکراسی رخ داده و اثرات فاجعه‌باری بر زندگی مردم این منطقه داشته است. واتس‌اپ هم روی زخم آنها نمک پاشید و در دسامبر ۲۰۱۹ اکانت کشمیری‌ها را به دلیل آن‌که بیش از ۱۲۰ روز غیرفعال بودند، از دسترس خارج کرد. این سیاست واتس‌اپ است.

در هنگام نگارش این مجموعه در ژانویه ۲۰۲۰، دادگاه عالی هند حکم داد که قطعی نامحدود اینترنت در کشمیر «غیرقانونی و سوء استفاده از قدرت» است. در پی صدور این حکم اینترنت پهن‌باند به صورت محدود و اینترنت موبایل به صورت کامل به برخی نقاط کشمیر بازگشت، اما کاربران فقط می‌توانستند به وب‌سایت‌های منتخبی که به «فهرست سفید» اضافه شده‌اند، دسترسی داشته باشند.

هدف از قطع اینترنت این است که امکان به‌اشتراک‌گذاری اطلاعات و برقراری ارتباط برای مردم مسدود شود و آن‌ها چاره‌ای جز روی آوردن به گزینه‌های جایگزین نداشته باشند؛ گزینه‌هایی همچون ارتباط موبایلی و پیامکی که شنودشان آسان‌تر است و امنیت پایین‌تری دارند. پیدا کردن راه‌هایی برای دور زدن محدودیت‌ها در زمان خاموشی سراسری اینترنت آسان نیست. در دوره‌ای که سخت‌ترین محدودیت‌ها در کشمیر اعمال شد و خاموشی سراسری برقرار بود مردم برای ارتباط با عزیزان‌شان به نامه‌های دست‌نوشته و پیک و پست روی آورده بودند.

ما نمی‌توانیم راه‌حل‌هایی قطعی برای دور زدن محدودیت‌ها در زمان قطعی اینترنت ارائه کنیم، اما از خلال گفت‌وگو با کنشگران و کسانی که تجربه زیست در زمان خاموشی را داشته‌اند، دریافته‌ایم که روش‌ها و رویکردهایی برای به‌اشتراک‌گذاری آفلاین و ارتباطات وجود دارند که ممکن است در چنین شرایط بغرنجی به کار بیایند؛ که البته بستگی به شرایط موجود دارند. لطفا در نظر داشته باشید که برای راه‌اندازی برخی از این گزینه‌ها نیاز به دسترسی به اینترنت دارید. یعنی باید اپلیکیشنی را دانلود و آماده بهره‌برداری کنید.

فایل‌ها را از راه بلوتوث، وای‌فای دیرکت یا NFC به اشتراک بگذارید

برای این‌که با گوشی‌تان به دیگر گوشی‌های پیرامون متصل شوید، از راه بلوتوث، وای‌فای دیرکت یا ارتباطات کوتاه‌برد (NFC) نیازی به اینترنت ندارید. روی برخی گوشی‌های قدیمی‌تر اندرویدی برای اشاره به NFC از «اندروید بیم» (Android Beam) استفاده می‌شود. بلوتوث و وای‌فای دیرکت هر دو تکنولوژی‌هایی هستند که می‌توانند دو دستگاه را بدون نیاز به مسیریاب (روتر) یا اکسس‌پوینت دیگری در میانه راه، به هم متصل کنند. وای‌فای دیرکت برد بیش‌تری دارد و انتقال داده‌ها در آن سریع‌تر از بلوتوث است، اما باتری بیش‌تری مصرف می‌کند. ارتباط کوتاه‌برد (ان‌اف‌سی) بردی کم‌تر از ۴ سانتی‌متر دارد و انتقال داده‌ها در آن بسیار کندتر از بلوتوث و وای‌فای دیرکت است، اما سرعت اتصال آن بالاتر است و مصرف باتری بسیار کم‌تری دارد. بنابراین می‌تواند برای انتقال فایل‌های کوچک وقتی هر دو دستگاه در دست‌تان است، گزینه مناسب‌تری باشد.

به احتمال زیاد امکان استفاده از بلوتوث، وای‌فای دیرکت و ان‌اف‌سی روی موبایل شما فراهم است و می‌توانید از میان گزینه‌های به‌اشتراک‌گذاری (Sharing) آن‌ها را پیدا کنید. گذشته از این، اپلیکیشن‌هایی نظیر Files By Google این فن‌آوری‌ها را به امکانات‌شان افزوده‌اند.

نکته مهم: نقطه ضعف اتصال آسانی که با استفاده از این روش‌ها میسر می‌شود این است که این‌گونه ارتباطات امن نیستند. اسکنرهای وای‌فای و بلوتوث می‌توانند به سادگی برای رهگیری موقعیت مکانی شما مورد استفاده قرار گیرند. نفوذگران ممکن است تلاش کنند تا به دستگاه شما متصل شوند، فایل‌های ناخواسته و بدافزار برای‌تان بفرستند یا حتی اگر سیستم‌تان آسیب‌پذیر باشد، کنترل آن را به دست بگیرند. **برای این‌که امن‌تر باشید وقتی از این دستگاه‌ها استفاده نمی‌کنید حتما آن‌ها را خاموش نگه دارید و فقط وقتی به جای امنی می‌رسید آن‌ها را به حالت روشن برگردانید. سطح دسترسی به اپلیکیشن‌ها را فقط به چیزها یا کسانی که نیاز دارید محدود کنید و با به‌روزرسانی مستمر گوشی و حراست از آن با یک پسورد مستحکم، نکات پایه امنیت موبایل را رعایت کنید.**

به‌اشتراک‌گذاری فایل‌ها از طریق درایوهای وایرلس یا شبکه وای‌فای محلی (WLAN)

یک هارد درایو وایرلس یا فلش درایو می‌تواند برای هم‌رسانی فایل‌ها میان اعضای یک تیم یا چندین نفر به صورت هم‌زمان مورد استفاده قرار گیرد. معمولا هاردهای وایرلس به همراه دستورات مشخص یا اپلیکیشن‌هایی عرضه می‌شوند که امکان ارتباط گوشی شما با هارد را فراهم می‌کنند و استفاده از آن‌ها هم نسبتا آسان است. به خاطر داشته باشید که حتما برای افزایش امنیت درایوی که در آن فایل‌ها را ذخیره می‌کنید، رمز عبور بگذارید.

اگر هارد وایرلس در اختیار ندارید، می‌توانید یکی از درایوهای یواس‌بی معمولی را به مسیریاب (روتر) وصل کنید و آن‌گاه فایل‌ها را به اشتراک بگذارید. به عنوان مثال، یک مسیریاب مسافرتی که پورت یواس‌بی دارد را می‌توانید نسبتا ارزان تهیه کنید و نکته این‌که می‌توانید به سادگی آن را به هر جایی که بخواهید حمل کنید. کاربران بدون این‌که به اینترنت دسترسی داشته باشند، می‌توانند به سادگی از طریق یک شبکه محلی به درایو یواس‌بی وصل شوند. برای این‌که بتوانید فایل‌های ذخیره‌شده روی درایو یواس‌بی را روی موبایل‌تان ببینید، باید از اپلیکیشن مدیریت فایلی که به معدن داده‌های شبکه متصل می‌شود استفاده کنید؛ اپلیکیشنی مانند Solid Explorer. آدرس آی‌پی مسیریاب را معمولا می‌توانید در تنظیمات پیشرفته وای‌فای روی موبایل‌تان پیدا کنید.

کاربران می‌توانند به یک درایو یواس‌بی که به یک مسیریاب وایرلس وصل شده، متصل شوند و فایل‌ها را روی شبکه محلی به اشتراک بگذارند.

یکی از گزینه‌های موجود دیگر برای این کار اپلیکیشن PirateBox است. پروژه‌ای که نرم‌افزاری رایگان ارائه کرده که با بهره‌گیری از آن کاربران می‌توانند همان‌طور که در بالا توضیح دادیم، فایل‌ها را به اشتراک بگذارند، با این تفاوت که با «پایرت‌باکس» شما می‌توانید این کار را به صورت ناشناس انجام دهید. امکان چت و پیام‌رسانی هم در این اپلیکیشن ارائه می‌شود. برای راه‌اندازی این اپلیکیشن باید از پیش آن را دانلود و نصب کنید و چند افزونه را هم به آن بیفزایید. توضیحات کامل را می‌توانید در وب‌سایت پایرت‌باکس ببینید.

با استفاده از چت‌های همتابه‌همتا ارتباط برقرار کنید

دو اپلیکیشن پیام‌رسانی نسبتا جدیدی که اخیرا ارائه شده‌اند و از طریق شبکه کنشگران به ما معرفی شده‌اند Briar و Bridgfy هستند که هنوز امتحان‌شان نکرده‌ایم، اما می‌دانیم که گروه‌های دیگری مشغول تست آن‌ها هستند.

«ایران در خاموشی» آنها را آزمایش کرده و اطلاعات بیشتر در جعبه‌ابزارهای ما موجود است:

جعبه‌ابزار اختلال در اینترنت

جعبه‌ابزار قطع اینترنت

جعبه‌ابزار خاموشی کامل

«برایر» یک اپلیکیشن متن‌باز (open-source) است که پیام‌ها را سرتاسری رمزگذاری می‌کند و به سروری مرکزی متکی نیست. برایر به جای ذخیره‌سازی داده‌ها روی یک سرور متمرکز، آن‌ها را روی دستگاه‌های کاربران ذخیره می‌کند. حتی وقتی دسترسی به اینترنت وجود ندارد شما می‌توانید از طریق این اپلیکیشن و مبتنی بر بلوتوث یا وای‌فای (وقتی اینترنت وجود دارد، اپلیکیشن همه دستگاه‌های موجود را از طریق شبکه «تور» همسان می‌کند) به موبایل‌ها و دیگر ابزارهای پیرامون‌تان متصل شوید. برایر امکان ایجاد گروه‌های خصوصی، انجمن‌های عمومی و وبلاگ هم ارائه می‌کند. وقتی به صورت آفلاین از این اپلیکیشن استفاده می‌کنید، برد آن همان حداکثر برد بلوتوث یا وای‌فای است که نزدیک به ۱۰۰ متر است.

از طریق پیامک‌های رمزگذاری‌شده ارتباط برقرار کنید

پیامک‌های متنی روی شبکه‌های موبایل ارسال می‌شوند و برای استفاده از آن‌ها نیازی به دسترسی به اینترنت نیست. احتمال این‌که امکان استفاده از پیامک حتی در زمان خاموشی اینترنت فراهم باشد بالاست. با این همه، اس‌ام‌اس سیستم بسیار ناامنی است. بر خلاف اپلیکیشن‌های مبتنی بر اینترنت نظیر واتس‌اپ یا سیگنال، پیامک‌ها به صورت سرتاسری رمزگذاری نمی‌شوند. این یعنی پیامک‌های متنی و فراداده (metadata) مرتبط با آن‌ها می‌توانند از سوی دولت‌ها یا اپراتورهای موبایل و یا هکرها در میانه راه شنود شوند. امکان جعل شماره‌ها (Spoofing) هم در سیستم پیامک‌رسانی فراهم است، به این معنی که فرستنده می‌تواند وانمود کند دارد از شماره خاصی این پیامک را برای‌تان ارسال می‌کند.

اگر لازم است از اس‌ام‌اس برای برقراری ارتباط استفاده کنید Silence اپلیکیشنی است که اس‌ام‌اس‌ها را سرتاسری رمزگذاری می‌کند. «سایلنس» اپلیکیشنی متن‌باز است و از پروتکل رمزگذاری سیگنال استفاده می‌کند. هنوز خودمان موفق به آزمایش این اپلیکیشن نشده‌ایم، اما گزارش‌هایی از استفاده از آن دریافت کرده‌ایم. برای استفاده از آن، هم فرستنده و هم گیرنده باید اپلیکیشن را دانلود و نصب کرده و کلیدهایشان را با یکدیگر به اشتراک گذاشته باشند. از آن‌جایی که پیامک‌ها لزوما از مجرای اپراتور موبایل شما رد می‌شوند، حتی با استفاده از سایلنس هم این‌که دارید پیامکی رمزگذاری‌شده می‌فرستید و فراداده آن را هم رمزگذاری کرده‌اید، از طرف شرکت مخابراتی خدمات‌دهنده شما قابل رویت است.

خاموشی موضعی: دور زدن سایت‌های فیلترشده

«خاموشی اینترنت» همیشه به معنی قطع کامل اینترنت نیست. گاهی خاموشی می‌تواند صرفا با مسدود کردن دسترسی به برخی وب‌سایت‌ها یا پلتفرم‌های شبکه‌های اجتماعی همراه باشد. دولت‌ها از طریق خدمات‌دهندگان اینترنت (ISP) می‌توانند وب‌سایت‌ها را بر اساس آدرس آی‌پی، محتوا یا دی‌ان‌اس آن‌ها فیلتر کنند. مطمئن نیستند آیا وب‌سایتی برای شما فیلتر شده یا نه؟ سازمان‌هایی نظیر OONI و «نت‌بلاکس» بر روند فیلترینگ و ایجاد اختلال در اینترنت در سراسر جهان نظارت دارند و گزارش‌های مستمر منتشر می‌کنند.

خوش‌بختانه تا زمانی که دسترسی شما به اینترنت برقرار است، راه‌هایی برای دور زدن محدودیت‌ها و فیلترینگ وجود دارند. همچون رمزگذاری، باید این نکته را در خاطر داشته باشید که تلاش برای دور زدن وب‌سایت‌های فیلترشده هم ممکن است بنا بر قوانین جایی که در آن زندگی می‌کنید، جرم باشد.

وی‌پی‌ان

یک راه برای دور زدن فیلترینگ وب‌سایت‌هایی که بر اساس آدرس آی‌پی یا محتوا فیلتر شده‌اند، استفاده از شبکه خصوصی مجازی، یا همان وی‌پی‌ان است. ProtonVPN و TunnelBear دو نمونه از وی‌پی‌ان‌ها هستند. وقتی از طریق وی‌پی‌ان به اینترنت وصل می‌شوید، ترافیک اینترنت‌تان رمزگذاری شده و از مجرای سرور وی‌پی‌انی که در مکان دیگری (یا حتی کشور دیگری) مستقر است، می‌گذرد. به این ترتیب مقصد نهایی و محتوای ترافیک اینترنت شما از چشم خدمات‌دهنده اینترنت‌تان پنهان می‌ماند.

این نکته را مد نظر داشته باشید که برخی دولت‌ها استفاده از وی‌پی‌ان را ممنوع کرده‌اند و ممکن است تلاش کنند اتصالات وی‌پی‌ان شما را کشف و مسدود کنند. استفاده از وی‌پی‌ان امن و معتبر هم نکته مهمی است و بهتر است از گزینه‌هایی استفاده کنید که داده‌ها و گزارش‌های فعالیت شما را ذخیره نمی‌کنند، چون در آن صورت خدمات‌دهنده اینترنت ممکن است بتواند جزئیات فعالیت‌های شما در اینترنت را ببیند. دقت کنید که خدمات‌دهنده وی‌پی‌ان شما در کدام کشور مستقر است و بسته به موقعیت جغرافیایی آن‌ها، کدام قوانین ممکن است شامل حال شما شود. این نکته را هم در نظر داشته باشید که وی‌پی‌ان‌های مورد تایید دولت‌ها ممکن است در واقع امکان شنود و بازرسی داده‌های شما را برای آن‌ها فراهم کنند.

سرورهای دی‌ان‌اس

سیستم نام‌گذاری دامنه‌ها (DNS) سرورهایی هستند که برای ترجمه نام دامنه‌های اینترنتی یا URLها به آدرس آی‌پی کار می‌کنند. اینترنت، وب‌سایت‌ها را فقط از آدرس آی‌پی آن‌ها می‌شناسد. خدمات‌دهنده اینترنت (ISP) می‌تواند تنظیمات سرورهای دی‌ان‌اسی را که تحت کنترل دارد به‌گونه‌ای تغییر دهد که برخی درخواست‌ها مسدود شوند یا به ازای آن دستورها صفحات نامرتبطی بارگذاری شوند که به شما اعلام می‌کنند دسترسی به وب‌سایتی که می‌خواهید مسدود است. در سال ۲۰۱۴ نخست‌وزیر ترکیه، رجب طیب اردوغان، تلاش کرد تا با بهره‌گیری از همین تکنیک در جریان انتخابات ترکیه دسترسی به توییتر را مسدود کند. این تلاش با واکنش سریع کنشگران که راهنمای گام به گام استفاده از وی‌پی‌ان‌ها و تغییر سرورهای دی‌ان‌اس را منتشر کردند، ناکام ماند.

شما می‌توانید تنظیمات پیش‌فرض سرورهای دی‌ان‌اس (DNS) را روی تنظیمات شبکه یا وای‌فای موبایل خود تغییر دهید. به جای سرورهای دی‌ان‌اس پیش‌فرض، می‌توانید از سرورهای جایگزین از جمله Google Public DNS.
شما می‌توانید آدرس‌های دی‌ان‌اس (DNS) را در تنظیمات پیشرفته وای‌فای تغییر دهید. فقط به خاطر داشته باشید که بهتر است پیش از اعمال هر تغییری از تنظیمات پیشین‌تان اسکرین‌شات بگیرید تا در صورت لزوم به آن برگردید.

این‌ها فقط دو راه‌حل موجود برای دور زدن رایج‌ترین تکنیک‌های فیلترینگ‌اند. برای اطلاعات دقیق‌تر و کامل‌تر می‌توانید راهنماهایی را که در این وب‌سایت‌ها ارائه می‌شوند، مطالعه کنید: Internet Society و Access Now و Security-in-a-Box و EFF.