انٹرنیٹ بندش کے دوران فائل شیئرنگ اور مواصلت

عربی اور ہسپانوی میں بھی دستیاب ہے
آخری جائزہ: 31 جنوری 2020

جمہوریت میں اب تک کا سب سے طویل انٹرنیٹ شٹ ڈاؤن ہونے کی وجہ سے ، کشمیر میں جاری انٹرنیٹ شٹ ڈاؤن اور کریک ڈاؤن کا خطہ کے لوگوں کی زندگیوں پر تباہ کن اثر پڑا ہے۔ چوٹ کی توہین میں اضافہ کرتے ہوئے ، دسمبر 2019 میں ، کشمیریوں کے واٹس ایپ اکاؤنٹس کو واٹس ایپ نے اپنی پالیسیوں کے مطابق صارفین کی 120 دن کی غیرموجودگی کی وجہ سے منسوخ کرنا شروع کردیا گیا۔

جنوری 2020 میں اس تحریر کے وقت ، ہندوستانی سپریم کورٹ نے فیصلہ دیا کہ کشمیر میں غیر معینہ مدت کے لئے انٹرنیٹ بندش غیر قانونی اور اختیارات کا غلط استعمال ہے۔ کچھ علاقوں میں محدود براڈبینڈ اور موبائل انٹرنیٹ کو بحال کیا گیا ہے ، لیکن صرف "وائٹ لسٹڈ" ویب سائٹ کو منتخب کرنے کے لئے۔

انٹرنیٹ بندشیں لوگوں کو معلومات کو شیئر کرنے اور بات چیت کرنے سے روکنے کے لئے تیار کیا گیا ہے (اور لوگوں کو مواصلات کی کم محفوظ شکلوں جیسے موبائل فون اور ایس ایم ایس کی طرف بھی دھکیلتا ہے ، جس سے حکام کو روکنے اور مانیٹرکرنے میں آسانی ہوتی ہے)۔ مکمل شٹ ڈاؤن کے دوران ہمیشہ اچھے کام نہیں ہوتے ہیں۔ مثال کے طور پر ، کشمیر میں شٹ ڈاؤن کے سخت ادوار کے دوران ، لوگوں نے اپنے پیاروں کو پیغامات پہنچانے کے لئے ہاتھ سے لکھے ہوئے نوٹ اور کورئیر استعمال کیے۔

ہمارے پاس تمام رکاوٹوں کو دور کرنے کے یقینی طریقے سے آگاہی نہیں ہے ، لیکن کارکنوں اور ساتھیوں سے گفتگو کے ذریعے ، ہم نے حالات کے لحاظ سے آف لائن شیئرنگ اور مواصلات کے لئے کچھ طریقے اور رسائی سیکھ لئے ہیں جو آپ کے لئے کارآمد ثابت ہوسکتے ہیں۔ نوٹ کریں کہ ان میں سے کچھ اختیارات کے لئے ابتدائی طور پر انٹرنیٹ ترتیب دینے کے لئے انٹرنیٹ کی ضرورت ہوتی ہے (جیسے ایپس کو ڈاؤن لوڈ کرنا وغیرہ)۔

فائلوں کو براہ راست Bluetooth, Wifi Direct, or NFC کے ساتھ شیئر کریں

بلوٹوتھ ، وائی فائی ڈائرکٹ (Wifi Direct)، یا نزدیک فیلڈ مواصلات (NFC) (Android Beam) کے ذریعے اپنے فون کو قریبی آلے کے ساتھ مربوط کرنے کے لئے آپ کو انٹرنیٹ کنیکشن کی ضرورت نہیں ہے۔ بلوٹوتھ اور وائی فائی ڈائریکٹ دونوں وائرلیس ٹیکنالوجیز ہیں جو دو ڈیوائسز کو "جوڑا" بنا سکتی ہیں کسی دوسرے روٹر یا رسائی کے نقطہ کے بغیر۔ وائی فائی ڈائرکٹ بلوٹوتھ کے مقابلے میں ایک وسیع تر رینج اور تیز ڈیٹا ٹرانسفر مہیا کرتا ہے ، لیکن اس میں بہت زیادہ طاقت استعمال ہوتی ہے۔ دریں اثنا ، این ایف سی کے پاس بلوٹوتھ یا وائی فائی ڈائرکٹ سے کہیں زیادہ قلیل رینج (4 سینٹی میٹر) ہوتی ہے اور کمتر منتقلی کی رفتار، لیکن یہ تیز رفتار سے جڑتا ہے اور کم طاقت کا استعمال کرتا ہے ، لہذا جب آپ کے ہاتھ میں دونوں ڈیوائسز ہوں تو چھوٹی ٹرانسفر کے لئے یہ مفید ثابت ہوسکتا ہے۔

ممکنہ طور پر آپ کے پاس بلوٹوتھ ، وائی فائی ڈائرکٹ(Wifi Direct) ، اور این ایف سی(NFC) کی خصوصیات ہیں جو آپ کے فون میں بنی ہیں جو آپ کے اشتراک کے اختیارات میں دکھائی دیتی ہیں۔ اس کے علاوہ ،Files By Google طرح فائلوں کے اشتراک کی خصوصیات والی ایپس بھی ان ٹیکنالوجیز کو مربوط کرتی ہیں۔

اہم: ان خدمات کے ذریعہ فراہم کردہ کنکشن کی آسانی کا منفی پہلو یہ ہے کہ وہ محفوظ نہیں ہیں۔ معلومات کے لئے بلوٹوتھ اور وائی فائی بیکنز / اسکینرز کا استعمال آپ کے مقام کا پتہ لگانے یا آپ کے آلے کی تحقیقات کے لئے کیا جاسکتا ہے۔ درانداز آپ کے آلہ کے ساتھ جوڑا بنانے ، ناپسندیدہ فائلیں بھیجنے یا اگر آپ کا آلا نہ محفوظ ہو تواسکا کنٹرول حاصل کرنے کی کوشش کر سکتے ہیں۔ محفوظ تر بننے کے لئے ، جب آپ محفوظ مقامات میں ہوں تو ان خدمات کو بند کردیں اور صرف ان کو آن کریں ، جب آپ کو ضرورت ہو تو ایپ کی اجازت کو محدود کریں ، اور اپ ڈیٹ کو چلانے اور مضبوط رکھنے جیسے اچھے فون سیکیورٹی طریقوں پر عمل کریں اور مضبوط پاس کوڈ رکھیں۔

وائرلیس ڈرائیو کے ذریعے یا وائرلیس لوکل ایریا نیٹ ورک (WLAN) کے ذریعے فائلوں کا اشتراک کریں۔

کسی وائرلیس ہارڈ ڈرائیو یا فلیش ڈرائیو کا استعمال کسی ٹیم میں ، یا ایک ہی وقت میں متعدد افراد میں فائلوں کو بانٹنے کے لئے کیا جاسکتا ہے۔ وائی فائی ڈرائیو عام طور پر آپ کے فون کو ڈرائیو سے منسلک کرنے کے لئے ہدایات اور / یا ایک ایپ کے ساتھ ہوگی ، اور اسکا استعمال نسبتاً آسان ہے۔ سیکیورٹی کے لئے ڈرائیو پر پاس ورڈ ترتیب دینا یاد رکھیں۔

اگر آپ کے پاس وائرلیس ڈرائیو نہیں ہے تو ، آپ اسے ایک وائرلیس روٹر میں پلگ کرکے باقاعدہ USB ڈرائیو پر فائلوں کا بھی اشتراک کرسکتے ہیں۔ مثال کے طور پر ، USB پورٹ والا ٹریول روٹر نسبتا سستا اور بہت پورٹیبل ہے۔ صارفین مقامی نیٹ ورک کے ذریعہ USB ڈرائیو سے رابطہ کرسکتے ہیں (انٹرنیٹ کی ضرورت نہیں ہے)۔ اپنے فون پر منسلک USB ڈرائیو پر فائلوں تک رسائی حاصل کرنے کے لئے ، آپ کو ایک فائل مینیجر ایپ استعمال کرنے کی ضرورت ہوگی جو نیٹ ورک اسٹوریج ، جیسے Solid Explorer سے مربوط ہوسکے۔ آپ کے روٹر کا IP پتہ عام طور پر آپ کے فون کی جدید وائی فائی سیٹنگ میں پایا جاسکتا ہے۔

دریں اثنا ، دوسرا آپشن PirateBox ہے ، ایک do-it-yourself پروجیکٹ جو آزادانہ طور پر لائسنس یافتہ سافٹ ویئر فراہم کرتا ہے۔ صارف اوپر کی طرح فائلیں شیئر کرسکتے ہیں ، لیکن Piratebox انہیں گمنامی میں ایسا کرنے دیتا ہے ، اور اس میں چیٹ اور میسجنگ کی خصوصیات بھی شامل ہیں۔ Piratebox کو ترتیب دینے کے لئے سافٹ ویئر کے کچھ ٹکڑے ڈاؤن لوڈ ، انسٹال اور ترتیب دینے کی ضرورت ہے۔ ہدایات Piratebox ویب سائٹ پر ہیں۔

اپ ڈیٹ: پیریٹ بوکس پروجکٹ (Pirate Box Project) آہستہ آہستہ بند ہو رہا ہے۔ ویب سائٹ اور گٹھب(GitHub) ذخیرہ اب بھی آن لائن ہے ، لیکن پروجکٹ کا مرکزی ڈویلپر اب اسے فعال طور پر برقرار نہیں رکھتا۔

کارکنوں کے نیٹ ورک کے توسط سے ہم آگاہ ہوچکے ہیں دو نئی قسم کی peer-to-peer میسیجنگ ایپ Briar اور Bridgefy ہیں۔ ہم نے ابھی ان کی جانچ نہیں کی ہے ، لیکن ہم دوسروں کو جانتے ہیں جو ان کی جانچ کر رہے ہیں۔

انکرپٹڈ میسجنگ ایپ ہے جو مرکزی سرور پر انحصار نہیں کرتی ، بلکہ end-to-end ،ایک اوپن سورس Briar اس کے بجائے صارفین کے آلات کے مابین پیغامات کو ہم آہنگی دیتا ہے (لہذا ہر صارف کے آلے پر مواد زندہ رہتا ہے)۔ یہ یہاں تک کہ جب بلوٹوتھ یا وائی فائی کا استعمال کرتے ہوئے انٹرنیٹ موجود نہ ہو (جب انٹرنیٹ موجود ہو تو ، میں نجی گروپس ، عوامی فورم اور Briar نیٹ ورک پر ڈیوائسز کو ہم آہنگی دیتی ہے) سینک کرسکتا ہے۔ Tor ایپ

بلاگ بھی شامل ہیں۔ آف لائن استعمال کرتے وقت ، آپ کی بلوٹوتھ یا وائی فائی کی حد (زیادہ سے زیادہ ~ 100 میٹر) کے ذریعہ آپ کی حد محدود ہوتی ہے۔

دریں اثنا ، Bridgefy ایک end-to-end انکرپٹڈ (سوائے "براڈکاسٹ" خصوصیت کا استعمال کرتے ہوئے) میسجنگ ایپ ہے جو پیغام بھیجنے کے لئے بلوٹوتھ استعمال کرتا ہے۔ Briar کے برعکس ، پیغامات دوسرے Bridgefy صارفین کے میش نیٹ ورک کی مدد سے طویل فاصلے کا سفر کرسکتے ہیں (صرف مطلوبہ وصول کنندہ ہی میسج پڑھ سکتا ہے)۔ Bridgefy کے پاس Briar کے نجی گروپس ، فورم اور بلاگ کی خصوصیات کا فقدان ہے ، لیکن اس میں براڈکاسٹ موڈ موجود ہے جس کے ذریعے آپ حدود میں موجود 7 Bridgefy صارفین کو پیغام بھیج سکتے ہیں ، جنہیں آپ کے رابطے ہونے کی ضرورت نہیں ہے (براڈکاسٹ پیغامات ضرورت کے مطابق انکرپٹڈ نہیں ہیں)۔

ایس ایم ایس (SMS) ٹیکسٹ میسجز سیل نیٹ ورکس پر بھیجے جاتے ہیں اور انٹرنیٹ پر انحصار نہیں کرتے ، لہذا انٹرنیٹ بند کے دوران بھی کام کرسکتے ہیں۔ تاہم ، ایس ایم ایس بہت غیر محفوظ سمجھا جاتا ہے۔ انٹرنیٹ پر منحصر ایپس جیسی WhatsApp or Signal کے برخلاف ، ایس ایم ایس end-to-end انکرپٹڈ نہیں ہوتا ہے۔ اس کا مطلب یہ ہے کہ ٹیکسٹ پیغامات (اور ان کا میٹا ڈیٹا) حکومتوں اور موبائل کیریئر کے ذریعہ پڑھا جاسکتا ہیں ، یا ہیکرز کے ذریعہ روکا جاسکتا ہے۔ ایس ایم ایس کی "جعل سازی" بھی کی جاسکتی ہے ، اس کا مطلب یہ ہے کہ بھیجنے والے کسی دوسرے صارف کی نقالی شکل میں ان کی ایڈریس کی معلومات میں ہیرا پھیری کرسکتا ہے۔

اگر آپ کو ایس ایم ایس (SMS) استعمال کرنے کی ضرورت پڑے تو ، Silence ایک ایپ ہے جو end-to-end ایس ایم ایس پیغامات کو انکرپٹ کرتی ہے۔ یہ اوپن سورس ہے اور سگنل انکرپشن پروٹوکول کا استعمال کرتا ہے۔ جب کہ ہم نے خود کوشش نہیں کی ، ہم نے سنا ہے کہ دوسروں نے اسے استعمال کیا ہے۔ بھیجنے والے اور وصول کنندہ دونوں کو یہ نصب کرنے اور ایک دوسرے کے ساتھ چابیاں کا تبادلہ کرنے کی ضرورت ہے ۔ چونکہ ایس ایم ایس پیغامات لازمی طور پر آپ کے ٹیلی کام کے سرورز سے گزرتے ہیں ، یہاں تک کہ Silence کے ساتھ یہ بھی حقیقت ہے کہ آپ ایک انکرپٹڈ میسج بھیج رہے ہیں اور آپ کے میسج کے بارے میں میٹا ڈیٹا ٹیلی کام کمپنی کے لئے قابل رسائی ہوگا۔

ایک "انٹرنیٹ شٹ ڈاؤن" کا مطلب اکثر انٹرنیٹ کو بلیک آؤٹ نہیں کرنا ہوتا ، بلکہ مخصوص ویب سائٹ یا سوشل میڈیا پلیٹ فارم تک رسائی کو روکنا ہوتا ہے۔ انٹرنیٹ سروس پرووائڈر (ISP) کے توسط سے حکومتیں ، IP ایڈریس ، مواد یا DNS تلاش کے ذریعہ سائٹوں کو بلاک کرسکتی ہیں۔ یقین نہیں ہے کہ اگر کسی سائٹ کو مسدود کیا جارہا ہے؟ ادارے جیسے Open Observatory of Network Interference and Netblocks پوری دنیا میں انٹرنیٹ میں خلل پڑنے اور سنسرشپ کی نگرانی اور پیمائش کرتے ہیں۔

خوش قسمتی سے ، جب تک کہ آپ کو انٹرنیٹ تک رسائی حاصل ہو ، جزوی بلاکس کے آس پاس جانے کی کوشش کرنے کے کچھ طریقے موجود ہیں۔ انکرپشن کی طرح ، یہ بات بھی ذہن میں رکھیں کہ آپ کے ملک میں مسدود بلاک سائٹوں کو جرم قرار دیا جاسکتا ہے۔

آئی پی (IP) پر مبنی اور مواد پر مبنی بلاکنگ کو نظرانداز کرنے کا ایک طریقہ یہ ہے کہ ورچوئل پرائیوٹ نیٹ ورک یا وی پی این ، جیسے ProtonVPN or TunnelBear کا استعمال کریں۔ جب آپ وی پی این کے ذریعے جڑ جاتے ہیں تو ، آپ کے انٹرنیٹ ٹریفک کو کسی دوسرے مقام پر ، جیسے کسی دوسرے ملک میں ، وی پی این سرور

کے ذریعے خفیہ شدہ اور راستہ بنایا جاتا ہے ، اس طرح آپ کی آئی ایس پی پر اصل منزل اور اپنے ٹریفک کے مواد کو چھپایا جاتا ہے۔

VPN

یہ بات ذہن میں رکھیں کہ کچھ حکومتیں VPN کے استعمال پر پابندی عائد کرتی ہیں یا VPN روابط کا پتہ لگانے اور روکنے کی کوشش کرسکتی ہیں۔ قابل اعتبار وی پی این فراہم کنندہ ، اور ترجیحی طور پر وہ ڈیٹا یا لاگ ان کو محفوظ نہ کرنے والا استعمال کرنا بھی ضروری ہے ، کیونکہ فراہم کنندہ آپ کی انٹرنیٹ کی سرگرمی کو دیکھ سکے گا۔ وی پی این فراہم کنندہ کس ملک میں مقیم ہے ، اور ان کے دائرہ اختیار کی بنیاد پر وہ کون سے قانونی عمل کے تابع ہوسکتے ہیں اس سے آگاہ رہیں۔ یہ بھی غور کریں کہ حکومت سے منظور شدہ وی پی این واقعتا آپ کے ڈیٹا کی نگرانی اور معائنہ کرسکتے ہیں۔

DNS servers

ڈی این ایس (DNS) سرورز ان ڈومین ناموں کا جو صارفاین browser میں ٹائپ کرتے ہیں ترجمہ ہندسی IP پتہ میں کرتے ہیں یہ پتہ پھرWebpages کی استعمال ہوتے ہیں- ایک (ISP) ان DNS سرورز میں تبدیلی لا سکتا ہے جن کو وہ کچھ جانکاریاں بند کرنے کے لئے کنٹرول کرتا ہے- 2014 میں ، ترک وزیر اعظم رجب طیب اردوان نے اس تکنیک کا استعمال کرتے ہوئے ترک انتخابات کے دوران ٹویٹر کو روکنے کی کوشش کی تھی۔ ان پابندیوں کو فوری طور پر ان کارکنوں نے ناکام بنا دیا جنہوں نے وی پی این استعمال کرنے اور ڈی این ایس سرورز کو تبدیل کرنے کے طریق کار مرحلہ وار نکات شیر کیے تھے

آپ اپنے فون کے نیٹ ورک یا وائی فائی کی ترتیبات میں طے شدہ DNS سرور کو تبدیل کرسکتے ہیں۔ طے شدہ DNS سرور کے بجائے ، آپ DNS بیسڈ بلاکس کے آس پاس حاصل کرنے کے لئے متبادل DNS سرورز جیسے Google Public DNS or CloudFlare استعمال کرسکتے ہیں۔ CloudFlare میں 1.1.1.1 نامی ایک ایپ بھی ہے جو صارفین کو ایک سادہ ایپ انٹرفیس کے ذریعے Cloudflare ڈی این ایس سرور پر سوئچ کرنے کی سہولت دیتی ہے۔

عام طور پر مسدود کرنے کی عمومی تکنیک کو روکنے کے لئے یہ صرف دو طریقے ہیں۔ مزید گہرائی سے متعلق معلومات کے لئے Internet Society, Access Now, Security-in-a-Box, and EFF سے مددگار ہدایت نامہ دیکھیں۔