فہرست کا مجموعہ:

انٹرنیٹ بندشوں کے دوران دستاویزسازی

آف لائن دستاویزات کے لئے ایک فون مرتب کرنا

کیا مجھے یہ دستاویزی ایپ استعمال کرنا چاہئے؟

انٹرنیٹ بندشوں کے وقت قابل تصدیق میڈیا کو برقرار رکھنا

انٹرنیٹ یا کمپیوٹر کے بغیر فون میڈیا کا بیک اپ (بیک-آف) بنانا

انٹرنیٹ بندشوں کے دوران فائل شیئرنگ اور مواصلت

انٹرنیٹ بندش کے دوران دستاویز کاری کا تعارف:

جون 2019 میں میانمار میں انسانی حقوق کی پامالی اور انسانی بحران کے دوران ملک کی وزارت ٹرانسپورٹ اور مواصلات نے ٹیلی کام کمپنیوں کو راکھین ریاست اور پڑوسی ریاست چین کے کچھ حصوں میں اپنی موبائل انٹرنیٹ سروس بند رکھنے کا حکم دیا- میانمار کی حکومت نے "امن میں رخنہ ڈالنا" اور "غیر قانونی سرگرمیوں" کا حوالہ دیتے ہوئے یہ دعویٰ کیا کہ "لوگوں کے مفاد کے لئے" انٹرنیٹ سروس بند کی گئ۔

جبکہ حقیقت میں اس بلیک آؤٹ سے ایک ملین سے زائد افراد ضروری معلومات و مواصلات کی سہولیت سے محروم ہوئے، اور انسانیت سوز کوششوں میں خلل پڑا۔ جیسا کہ *Fortify Rights* سے تعلق رکھنے والے میتھیو اسمتھ نے کہا ہے کہ ، "یہ انٹرنیٹ شیٹ ڈون روہنگیا کے خلاف جاری نسل کشی اور راکھائن کے خلاف جنگی جرائم کے تناظر میں ہورہا ہے اور اگر اس کا مقصد عسکریت پسندوں کو نشانہ بنانا تھا تو پھر بھی یہ انتہائی غیر متنازعہ ہے"۔

ستمبر 2019 میں پانچ علاقوں میں جزوی طور پر یہ شٹ ڈاؤن اٹھایا گیا تھا، اسی ماہ کے دوران ، پڑوسی ملک بنگلہ دیش میں جہاں بہت سے روہنگیا کے باشندے فرار ہوگئے ہیں ، حکام نے موبائل فون آپریٹرز کو روہنگیا پناہ گزین کمپنییوں میں تری جی اور فور جی خدمات بند کرنے اور روہنگیا پناہ گزینوں کو سم کارڈ فروخت نہ کرنے کا حکم دیا۔ جبکہ 2020 میں بھی راکھین کی چار بستیاں باہری دنیا سے منقطع ہے اور آے دن بنگلہ دیش مہاجر کیمپوں میں اپنی خدمات کو محدود کر رہا ہے۔

انٹرنیٹ بندشوں کے دوران دستاویزسازی

عالمی سطح پر انٹرنیٹ کی بندش میں اضافہ ہو رہا ہے۔ **AccessNow کی #KeepItOn** مہم کے مطابق، جنوری سے جولائی 2019 کے درمیان جان بوجھ کر 128 شٹ ڈاؤن ہوئے، جبکہ 2018 میں یہ تعداد 196 تھی، اور 2017 میں 106، اور 2016 میں یہ تعداد 75 تھی۔
دنیا بھر میں حکومتیں ، ٹیلی کام کمپنیوں کے تعاون سے ، تیزی سے انٹرنیٹ بندشوں کی طرف راغب ہو رہی ہیں اور ان کو ایک حکمت عملی کے طور استعمال کیا جارہا ہے تاکہ لوگوں کو دبایا جائے ، انسانی حقوق کی خلاف ورزیوں کے بارے میں معلومات کی دستاویزی اور اسے شیر کرنا روکا جاسکے۔

"انٹرنیٹ کی بندش اور انسانی حقوق کی خلاف ورزیاں ساتھ ساتھ چلتی ہیں۔"
– Berhan Taye, AccessNow

انٹرنیٹ بندشیں مختلف قسم کی شکلیں لے سکتے ہیں جیسےکسی خاص پلیٹ فارم پہ اس کی بندش جس میں مشہور ایپس، سائٹس موبائل ڈیٹا بند، بینڈوڈتھ گھٹانا یا مکمل انٹرنیٹ بندش، کو نشانہ بنایا جاتا ہیں - ان تمام قسم کی بندشوں کا مقصد معلومات تک پہنچانے کی صلاحیت کو روکنا اور اصل وقت میں خلاف ورزیوں کو بے نقاب ہونے سے روکنا ہوتا ہے۔ یہ اکثر مظاہروں ، انتخابات اور سیاسی عدم استحکام کے ادوار کے دوران پیش آتے ہیں ، اور ان کے ساتھ اکثر ریاستی جبر ، فوجی جرائم اور تشدد ہوتے ہیں۔ جبکہ حکومتیں "عوامی تحفظ" یا دیگر وجوہات کے نام پر شٹ ڈاؤن کو جائز قرار دینے کی کوشش کر سکتی ہیں ، لیکن شٹ ڈاؤن ان وقت واضح طور پر رونما ہوتا ہے جب جابرانہ ریاستوں کو اپنے لوگوں ، معلومات ، یا سیاسی بیانیہ پر سخت کنٹرول کھونے کا خدشہ ہوتا ہے۔ بندش انسانی حقوق کی خلاف ورزی کرتی ہے ، لوگوں کی زندگی اور معاش کو بری طرح متاثر کرتی ہے اور عالمی معاشی اثر بھی پڑتا ہے۔

انٹرنیٹ بند کے دوران انسانی حقوق کی پامالیوں کی دستاویزی کرنا بہت ہی اہم ہے۔ اگرچہ کسی خاص وقت میں معلومات کا اشتراک نہیں کیا جاسکتا، دستاویزات ان آوازوں کو محفوظ رکھنے کا ایک طریقہ ہوسکتا ہیں جنہیں حکام خاموش کرنے کی کوشش کر رہے ہو ، اور ان بدعنوانیوں کے ثبوتوں کو محفوظ کرنے کے لئے جن کا استعمال بعد میں احتساب کا مطالبہ کرنے کے لئے کیا جاسکتا ہے۔ بےشک ، جابرانہ سیاق و سباق اور انٹرنیٹ شٹ ڈاؤن کی تکنیکی راہ میں حائل دستاویزات کی خلاف ورزی - اور اس دستاویزات کو محفوظ طریقے سے برقرار رکھنا - زیادہ مشکل اور خطرناک ہے۔ **کارکن کیسے بند کے دوران اپنے ویڈیوز محفوظ طریقے سے ریکارڈ اور ان کو آف لائن بھی شیئر کرسکتے ہیں ؟**

یہ سلسلہ

اپنے کام کے ذریعے ہم نے ان کارکنوں سے جنھوں نے انٹرنیٹ شٹ ڈاؤن کا تجربہ کیا ہے کچھ مفید نکات انٹرنیٹ بند کے دوران **ویڈیو دستاویزات بنانے کے حوالے سے سیکھے ہیں** جو ہم اس سلسلے میں شیئر کر رہے ہیں ہم نے انھیں اینڈرائیڈ ڈیوائسز کو ذہن میں رکھتے ہوئے لکھا ہے ، لیکن ان نکات کو آئی فونز پر بھی لاگو کیا جاسکتا ہے۔ کچھ حکمت عملیوں میں پیشگی منصوبہ بندی کی ضرورت ہے (اور انٹرنیٹ تک رسائی) ، لہٰذا یہ بہتر ہوگا کہ آپ ان حالات کا شکار ہوجانے سے پہلے ان اقدامات کا جائزہ لیں اور ان اقدام کو نافذ کریں اس سے پہلے کہ آپ کے پاس انٹرنیٹ نہ ہو اور آپ کو دستاویزات کی ضرورت پڑے۔کسی بھی سبق کی ایک کاپی محفوظ رکھے تاکہ آپ ان کا حوالہ دے سکیں یا بند کے دوران ان کا اشتراک کرسکیں۔اور آخر کار ، اپنے روزمرہ کے کام میں ان تکنیکوں اور طریقوں پر عمل کرنا شروع کریں تاکہ آپ بحران کی صورتحال میں پڑنے سے پہلے آپ جبلتی طور پر تیار ہو۔

- **تیار رہنا:** ○ آف لائن دستاویزات کے لیے فون سیٹ کرنا
- **کیپچر:** ○ کیا مجھے یہ دستاویزی ایپ استعمال کرنی چاہیے؟
- **برقرار رکھنا:** ○ انٹرنیٹ بند ہونے کے دوران قابل تصدیق میڈیا کو برقرار رکھنا
- ○ انٹرنیٹ یا کمپیوٹر کے بغیر فون میڈیا کا بیک اپ لینا
- **شئر کرنا اور بات چیت:** ○ انٹرنیٹ بند ہونے کے دوران فائل شیئرنگ اور کمیونیکیشن

ایک حتمی نوٹ: اگرچہ یہ نکات آپ کو شٹ ڈاؤن کی صورت میں دستاویز کاری جاری رکھنے میں مدد دے سکتے ہیں، لیکن ہم اس بات پر زور دینا چاہتے ہیں کہ حتمی حل انٹرنیٹ تک رسائی کو بحال کرنا، اور لوگوں کے ریکارڈ کرنے کے حق، اور اظہار رائے کی آزادی، معلومات، اور کامیابی کے ساتھ دفاع کرنا ہے۔ اسمبلی خوش قسمتی سے، NetBlocks، AccessNow، اور بہت سی دیگر تنظیموں کی قیادت میں ایک عالمی تحریک چل رہی ہے جو فعال طور پر بند ہونے کے بارے میں معلومات کی نگرانی اور اشتراک کر رہی ہیں۔ عالمی سطح پر وکلاء شٹ ڈاؤن کے

خلاف اسٹریٹجک قانونی چارہ جوئی میں مصروف ہیں۔ ہم انسانی حقوق کو برقرار رکھنے کے لیے ان کے کام کے ساتھ یکجہتی کے ساتھ کھڑے ہیں۔

****

آف لائن دستاویزات کے لئے ایک فون مرتب کرنا

یہ پوسٹ انٹرنیٹ شٹ ڈاؤن کے دوران ڈاکومینٹنگ کے سلسلے کا حصہ ہے۔

آخری جائزہ: 31 جنوری 2020

انٹرنیٹ بندش کے باوجود ، دستاویزکار اب بھی ایسے اہم ویڈیو ثبوتوں کو گرفت میں لے سکتے ہیں جن کا آف لائن اشتراک کیا جاسکتا ہے یا جب وہ آن لائن واپس آئے۔ یہاں کچھ تجاویز ہیں جو ہم نے کارکنوں اور دوسرے پریکٹیشنرز سے آف لائن دستاویزات کے لئے ایک فون سیٹ اپ کرنے کے بارے میں سیکھی ہے۔ نوٹ کریں کہ کچھ اقدامات کے لئے **انٹرنیٹ تک رسائی** کی ضرورت ہے ، لہذا انہیں انٹرنیٹ بند ہونے سے پہلے یا اس کے دوران جب اسے بحال کیا جائے تو ضرور کرے۔ نیز، اس وقت تک انتظار نہ کریں جب تک کہ آپ ان دبائو پر مبنی صورتحال میں نہ ہوں آپ ان اقدامات پر عمل پیرا نہ ہوسکو۔ انہیں ابھی کریں ، **اور فون کو استعمال کرتے ہوئے مشق کرنے میں** وقت لگائیں اس سے پہلے کہ آپ کو کسی بحران میں اس کا استعمال کرنا پڑے۔

شٹ ڈاؤن اکثر و بیشتر معلومات پر قابو پانے اور اظہار رائے کی آزادی اور مجلس پر پابندی کے ساتھ موافق ہوتا ہے۔ اگر آپ دستاویز کار ہیں تو ، ان ادوار کے دوران اپنی اور اپنی معلومات کی حفاظت کے لئے اضافی احتیاطی تدابیر اختیار کریں۔ اگر یہ خطرہ ہے کہ حکام آپ کا فون ضبط کریں گے ، یا آپ کو اسے غیر مقفل کرنے اور اس کے مندرجات (شٹ ڈاؤن کے دوران یا دوسری صورت میں) ظاہر کرنے پر مجبور کریں گے ،تو دستاویزات کے لئے اپنے بنیادی ذاتی فون کے علاوہ ایک الگ فون استعمال کرنے پر غور کریں۔ اس سے یہ مدد مل سکتی ہے کہ آپ جو معلومات لے رہے ہیں اس سلسلہ میں سمجھوتہ کم سے کم ہو (جیسے آپ کے کنٹیکٹس ، اکاؤنٹس ، پیغامات وغیرہ)۔ اگر آپ دوسرا آلہ استعمال کرنے سے قاصر ہیں تو ، آپ حساس ڈیٹا کی مقدار کو کم کرنے اور اپنے بنیادی فون پر سیکیورٹی کو بہتر بنانے کے لئے اس گائیڈ پر عمل کرسکتے ہیں۔

اگر کسی پرانے فون کو دوبارہ استمال کرنا ہو تو پہلے اسے صاف کریں

اپنے فون کو صاف کرنے کے لئے ، فیکٹری ری سیٹ چلائیں۔
نوٹ: مطالعات سے ثابت ہوا ہے کہ آپ کے فون پر فیکٹری ری سیٹ چلانے سے ضروری نہیں کہ تمام ڈیٹا صاف ہو جائے ۔ در حقیقت ، ڈیٹا کو مٹا دینے کا واحد 100٪ محفوظ طریقہ فون کو تباہ کرنا ہے ، لیکن اگر آپ فون کو دوبارہ استعمال کرنا چاہتے ہیں تو یہ طریقہ آپشن نہیں ہے! اس مضمون میں ، ایک اینڈرائیڈ انجینئر تجویز کرتا ہے کہ فیکٹری ری سیٹ ہونے سے پہلے اس بات کو یقینی بنائے کہ آپ کے آلے کے مندرجات کو خفیہ کردہ ہے۔ بہرحال زیادہ تر موجودہ فون پر خفیہ کاری طے شدہ ہے ، لیکن ایسی صورت میں ، ری سیٹ کرنے سے پہلے ترتیبات> سیکیورٹی> انکرپٹ فون پر جائیں۔ اس طرح ، جب آپ فون کو فیکٹری پر ری سیٹ کرتے ہیں تو ، انکرپشن کی کلید گم جاتی ہے ، اور کوئی بھی موجود ڈیٹا ناقابل استعمال ہو گا ۔

فون کی بنیادی حفاظت پر عمل کریں

فون کے تحفظ کے حوالے سے کچھ ایسے عام طریقے ہیں جو ہر ایک صورتحال میں متعلقہ ہیں - چاہے آپ انٹرنیٹ بندش کے دوران دستاویزسازی کر رہے ہو یا نہیں - یہاں دیگر تنظیموں کے کچھ مفید ذرائع ہیں۔ اگرچہ یہ 100٪ تحفظ کی گارنٹی نہیں ہے، کچھ اہم نکات یہ ہیں:

- یقینی بنائیں کہ آپ کا فون انکرپٹڈ ہے۔ نئے فونوں میں انکرپشن پہلےسےموجود ہوتی ہے۔ اگر آپ کو اپنے فون کے بارے میں یقین نہیں ہے تو ، اپنے فون پر سیکیورٹی کی ترتیبات کی پڑتال کریں۔

- آپریٹنگ سسٹم (OS) کی اپڈ یٹس کو باقاعدگی سے چلائیں ، کیونکہ وہ اکثر سیکیورٹی کے نقاًص کو ٹھیک کرتے ہیں۔
- اپنی اہم ایپس (جیسے میسجنگ ایپس) کو باقاعدگی سے اپ ڈیٹ کریں۔
- ایک مضبوط فون پاس کوڈ مرتب کریں جو کم از کم 6 ہندسوں پر مشتمل ہو اور فنگر پرنٹ / ٹچ یا چہرے کی پاس کوڈ پر انحصار نہ کریں ۔
- ایک اسکرین لاک اور لاک ٹائمر مرتب کریں۔
- اگر آپ کو ان کی ضرورت نہ ہو تو مقام کی آپشن کو موبایل میں بند کریں (بشمول ہنگامی محل وقوع کی خدمت ، محل وقوع کی درستگی ، مقام کی تاریخ ، اور مقام کی شراکت کی خصوصیات ، اور وائی فائی اور بلوٹوتھ سکیننگ آپشنز)۔ انفرادی ایپس کیلئے مقام کی اجازت کی بھی جانچ کریں۔
- ٹریکنگ سے بچنے کے لئے جب آپ کو بلوٹوتھ اور وائی فائی کی ضرورت نہ ہو ، تو بند کریں۔
- اگر آپ موبایل استعمال نہیں کرتے تو اسے بند کرے۔

مفید دستاویزات ایپس انسٹال کریں

تصویر یا ویڈیو دستاویزات کے لئے ،آپ اپنے فون پر بلٹ-ان کیمرا ایپ استعمال کرسکتے ہیں ، یا آپ ایک زیادہ مہارت والے دستاویزات ایپ کا استعمال کرسکتے ہیں ، جیسے ProofMode یا دیگر ، جو زیادہ مضبوط میٹا ڈیٹا کی گرفت اور برآمد ، شناخت اور توثیق ، خفیہ کاری ، محفوظ گیلریاں یا دیگر خصوصیات کی اجازت دیتا ہے۔ .

شٹ ڈاؤن کو دستاویز کرنے کے لئے ایک مفید ایپ OONI Probe ہے ، جو ایک اوپن سورس ایپ ہے جو آپ کے فون سے یہ جانچ کرنے کے لئے تخمینہ لگاتی ہے کہ آیا سائٹو یا پلیٹ فارمز کو روکا جارہا ہے۔ یہ آپ کو دکھا سکتا ہے کہ کس طرح ، کب ، کہاں ، اور کس کے ذریعہ سائٹس کو مسدود کیا جارہا ہے۔ اس ایپ کو استعمال کرنے سے پہلے ممکنہ خطرات کو سمجھنا یقینی بنائیں۔

اگر آپ کو یقین نہیں ہے کہ کون سے دستاویزات ایپس (استعمال) کرنے ہے؟ ہم اپنے سبق میں کچھ رہنمائی سوالات فراہم کرتے ہیں ، "کیا مجھے یہ دستاویزی ایپس استعمال کرنے چاہئے؟"۔

روزمرہ کی کچھ ایپس انسٹال کریں

آپ کے فون پر بہت کم ڈیٹا اور صرف کچھ مخصوص ایپس رکھنے سے شکوک و شبہات پیدا ہوسکتے ہیں۔ اپنے موبایل کو اس طرح بنائے تاکہ یہ ایک عام موبایل لگے ، کچھ روزمرہ ایپس انسٹال کریں جو اس علاقے میں عام ہیں جہاں آپ دستاویزسازی کررہے ہو (لیکن یہ معروف ذرائع سے ڈاؤن لوڈ کیے جاتے ہیں) ، اور اپنی گیلری کے لئے کچھ بے ضرر تصاویر لیں۔

سوشل میڈیا ایپس کیلئے، آپ متبادل اکاؤنٹ بنانے اور ان میں لاگ ان کرسکتے ہیں ، حالانکہ یہ بات ذہن میں رکھیں کہ جعلی اکاؤنٹس زیادہ تر پلیٹ فارمز کی خدمت کی شرائط کی خلاف ورزی کرتے ہیں ، اور کچھ پلیٹ فارمز کی شناختی توثیق کی تقاضوں میں جعلی اکاؤنٹس بنانا مشکل ہوسکتا ہے۔ اس کے علاوہ ، آپ کو مواد تیار کرنے اور ان میں دوست شامل کرنے میں کچھ وقت گزارنے کی ضرورت ہوگی ، جو کہ تھوڑا مشکل کام ہوسکتا ہے ۔

انٹرنیٹ نہ ہونے کی صورت میں ایپس انسٹال کرنا

انٹرنیٹ تک رسائی کے بغیر ایپس کو ڈاؤن لوڈ اور انسٹال کرنا ظاہر ہے کہ ایک مشکل کام ہے۔ اگر آپ انٹرنیٹ کی بندش کا ہو تو آپ کو ایپس پیشگی طور پر ڈاؤن لوڈ کرنے کی ضرورت ہے۔

بعد میں آپ کی اور دوسروں کی مدد کرنے والی ایک حکمت عملی یہ ہے کہ آپ اپنے موبایل پر Android پیکیج (.apk) فائل ڈاؤنلوڈ کرکے محفوظ کریں لیکن (**ایپ کسی قابل اعتماد ذریعہ سے ڈاؤن لوڈ کی ہوں** ، جیسے براہ راست ڈویلپر سے) ۔ ان APKs کو آف لائن رکھنے سے آپ کو یا دوسروں کو ایپس کا اشتراک کرنے کی سہولت ملتی ہے جب انٹرنیٹ موجود نہ ہو۔

جب کہ ہمیں اس کو آزمانے کا موقع نہیں ملا ، F-Droid ایپ ان APKs کو آف لائن تبدیل کرنے کے لئے ایک انٹرفیس مہیا کرتی ہے۔ ان کا ٹیوٹریل یہ ہے۔

حقیقی ذاتی یا نجی / حساس معلومات کو ڈیوائس سے دور رکھیں

دستاویزسازی کے لئے ڈیوائس کو محفوظ کرنے کی کوشش کریں۔ اسے ای میل ، فون کالز ، یا ذاتی یا کارکنوں کے پیغامات کے لئے استعمال نہ کریں جنھیں خطرہ لاحق ہوسکتا ہے ، اور اس ڈیوایس کو اپنے کسی بھی اصلی ، بنیادی اکاؤنٹ سے مربوط مت کریں۔

مضامین کو غیر واضح کرنے کے لئے خصوصیات کا استعمال کریں

اگر آپ کے فون کی تلاش لی جائے تو ، اپنے ارادوں کو کم واضح رکھنا یا اپنے مواد تک رسائ کو مشکل بنانا فائدہ مند ثابت ہو ساکتا ہے۔ ایسے حالات کی پیش گی میں جہاں آپ کے فون کی صرف سطحی اور جلد جانچ کی جائے گی، آپ کچھ آسان تدابیر استعمال کرسکتے ہیں جیسے:

- لانچر ایپ کا استعمال کرتے ہوئے اپنے ایپ شارٹ کٹس کے نام اور آئیکنز کو تبدیل کرنا (مثلاً Nova Launcher، لیکن یہاں بہت ایسے ایپس ہے) لیکن کوئی مخصوص ایپ موجود نہیں ہے۔
- اگر آپ کا فون اس کو سپورٹ کرتا ہے تو پرائیویٹ موڈ (سمسونگ) یا (LG) Content Lock جیسی بلٹ ان پرائیویسی فیچر کا استعمال کرے۔

- کسی فولڈر میں میڈیا کو اپنی گیلری میں آنے سے روکنے کے لئے کسی بھی فولڈر کے اندر "Nomedia." نامی خالی فائل رکھنا۔ نوٹ: اگر میڈیا اب بھی ظاہر ہوتا ہے تو ، آپ کو اپنی گیلری

ایک جیسے ایٹمز کو صاف کرنے کی ضرورت پڑسکتی ہے۔ یہ شاید تمام ڈیوائسس پر مستقل طور پر کام نہ کرے۔

- فائل مینیجر ایپ کا استعمال کرکے پوشیدہ فولڈرز کا بنانا جو کہ (a) سے شروع ہوتی ہے۔ آپ یا تو فائلوں کو دستی طور پر پوشیدہ فولڈر میں منتقل کرسکتے ہیں ، یا اگر آپ اوپن کیمرا جیسے کیمرہ ایپ کا استعمال کرتے ہیں تو ، آپ یہ بتاسکتے ہیں کہ آپ کا ریکارڈ کردہ میڈیا کہاں اسٹور ہوتا ہے۔ اپنی ترتیبات میں "چھپی ہوئی فائلیں دکھائیں" کے اختیار کو بند کرنا یقینی بنائیں تاکہ پوشیدہ فائلیں نظر نہ آئیں۔

- کچھ خصوصی دستاویزات ایپس جیسے، Tella اور Eyewitness to Atrocities دستاویزات کو الگ الگ انکرپٹ گیلریوں میں محفوظ کرتی ہیں جن کے مندرجات صرف ایپ میں ہی قابل رسا ہوتے ہیں ، جس سے آپ کے فون کی تلاشی لینے والے کسی بھی صورت میں واضح نہیں ہوتا۔ ان محفوظ گیلریوں میں دستاویزات کے لئے علیحدہ ایپ پاس کوڈ کی ضرورت ہوتی ہے ، لہذا یہ آپ کے فون انلاک ہونے پر بھی انکریپٹ رہتا ہے۔

آپ کے مواد کو چھپانے کے بارے میں اہم نوٹ

یہ نوٹ کرنا ضروری ہے کہ مذکورہ تراکیب کسی ایسے شخص کو دور کرنے کے لئے کافی نہیں ہوسکتی ہے جو صرف آپ کے فون پر تیزی سے سوائپ کررہا ہو ، لیکن **آپ کے مواد کو مؤثر طریقے سے کسی ایسے شخص سے چھپا نہیں سکے گا جو اچھے سے دیکھ رہا ہے۔**

یہ بھی ذہن میں رکھیں کہ کچھ ممالک کے پاس ایسے قوانین موجود ہیں جو سیکیورٹی ایپس کے استعمال کو محدود یا جرم بناتے ہیں جو آپ کے ڈیٹا کو خفیہ یا مسح کرتے ہیں۔ حکام کو اپنے ڈیٹا تک رسائی حاصل کرنے سے روکنے کے لئے ان کا استعمال شواہد کو ختم کرنا یا تفتیش میں رکاوٹ بنتے ہوئے دیکھا جاسکتا ہے ، اور یہ جرم کی حیثیت سے قابل سزا ہوسکتا ہے، اگر آپ کے پاس اپنے ملک کے قوانین کے بارے میں سوالات ہیں تو یہ نقشہ (جامع، لیکن 2017 سے) ایک اچھا آغاز فراہم کرتا ہے۔

آف لائن شیئرنگ مرتب کریں

ایسی صورتحال میں جب مواد حاصل کرنے کے بعد آپ کے پاس انٹرنیٹ موجود نہ ہو، تو آپ سیکیورٹی وجوہات کی بناء پر ، جگہ خالی کرنے ، یا دوسروں کے ساتھ اشتراک کرنے کے لئے اپنے فون سے دستاویزات ہٹانا چاہتے ہوں گے۔ آپ کے فون سے مستقل طور پر دستاویزات کو آف لوڈ کرنے سے یہ بھی کم کرنے میں مدد ملے گی کہ آپ کے فون کو جب کبھی ضبط کرکے اور ان لاک کردیا جائے تو کون سی معلومات اثر پذیر ہو۔

یہاں تک کہ اگر آپ انٹرنیٹ سے منسلک نہیں ہوسکتے ہیں، تب بھی آپ مقامی طور پر وائی فائی سے چلنے والے یا بلوٹوتھ سے چلنے والے ڈیواسیس جیسے کہ کوئی دوسرا فون یا وائی فائی USB ڈرائیو سے جڑ سکتے ہیں، ۔ آپ کا فون عام طور پر ایک ایپ/انٹرفیس کے ساتھ آنا چاہیے تاکہ آپ کنیکٹ اور ٹرانسفر کر سکیں۔ اگر آپ کا فون اس کو سپورٹ کرتا ہے، تو آپ USB On-The-Go (OTG) (OTG ڈرائیو یا کنیکٹر کو OTG ڈرائیو یا کسی اور ڈیوائس پر دستاویزات آف لوڈ کرنے کے لیے بھی لگا سکتے ہیں۔

ان طریقوں پر ہمارے ٹیوٹوریل اور ویڈیو "فائل شیئرنگ اور مواصلات انٹرنیٹ شٹ ڈاؤن کے دوران " میں مزید تفصیل سے تبادلہ خیال کیا گیا ہے۔

کسی بحران کی صورتحال میں ہونے سے پہلے مشق کریں

اگر آپ کے پاس انٹرنیٹ تک رسائی ہے تو ابھی فون کو مرتب کریں۔ روزمرہ کے حالات (جہاں سیکیورٹی سے متعلق کوئی خدشات نہیں ہیں) میں ایپس کے استعمال کی مشق کرنا شروع کریں تاکہ آپ ان کا استعمال کرنے سے واقف ہو اور سہولت ہوجاے۔ فون کی اچھی حفاظت کو اپنی طے شدہ عمل بنائیں۔ اس طرح کے طریقے دوسری نوعیت کے ہوں گے جب آپ کو کسی پریشانی کی صورتحال میں پریشان ہونے والی دوسری چیزوں کے ساتھ ہو۔

****

کیا مجھے یہ دستاویزی ایپ استعمال کرنا چاہئے؟

آخری جائزہ: 31 جنوری 2020

دستاویزکار بہت ساری ایپس کا استعمال کر کے ویڈیو کیپچر کرسکتے ہیں جن میں فون کا اپنا کیمرہ یا پھر مخصوص دستاویزی ایپس جیسے Eyewitness to Atrocities, Tella, ProofMode شامل ہیں ۔ کچھ ایپس کی خصوصیات انٹرنیٹ پر انحصار کرتی ہیں ۔ لہذا یہ بات ذہن میں رکھیں کہ مذکورہ خصوصیات انٹرنیٹ بندش کے دوران موجود نہیں ہوں گے

ہم آپ کو نہیں بتاسکتے ہیں کہ کون سی مخصوص ایپ آپ کے لئے سب سے موزوں ہے ، کیوں کہ یہ آپ کی صورتحال ، ضروریات اور خطرات پر منحصر ہے (اپنے خطرات کا اندازہ لگانے کے طریقے) جاننے کے بارے میں مزید معلومات کے لئے اس بلاگ پوسٹ کو چیک کریں۔ آپ کے خطرات کی جانچ پڑتال کے ساتھ ، ذیل میں یہ رہنمائی سوالات آپ کو اندازہ کرنے میں مدد کرسکتے ہیں کہ آپ کے لئے کون سا ویڈیو دستاویزی ایپ بہتر کام کرسکتا ہے۔

کس نے ایپ بنائی ہے اور کیا میں ان پر اعتماد کرتا ہوں؟

آپ کو ہمیشہ کسی بھی ایپ کے تخلیق کاروں پر غور کرنا چاہئے جو آپ اپنے ڈیوایس پر ڈاؤن لوڈ اور انسٹال کرتے ہیں ، اور یہ کہ کیا آپ ان پر اعتماد کرسکتے ہو کہ وہ جان بوجھ کر یا غیر ارادتا آپ کو خطرہ میں نہیں ڈالے گا۔

کچھ چیزوں پر غور کرنا جو یہ ہیں:

- کیا ایپ ڈویلپر نامور ہے؟ آپ کی جماعت اور وسیع تر نیٹ ورک کے لوگ ان کے اور ان کے ٹولز کے بارے میں کیا کہتے ہیں؟
- کیا ایپ ڈویلپر غیر محفوظ ہے؟ ان کے سیاق و سباق پر غور کریں اور ان امکانات پر کہ ان کو کس طرح مجبور کیا جاسکتا ہے کہ وہ آپ کا ڈیٹا حوالے کریں یا حکام کے لئے بیک ڈور بنائیں (یا کیا انہوں نے ماضی میں ایسا کیا ہو)۔ کس ملک میں ڈیٹا جمع ہے اور اس دائرہ اختیار میں عدالتی احکامات سے متعلق کیا قوانین موجود ہیں؟
- -- کیا ایپ ڈویلپر ایپ کو برقرار رکھے ہوئے ہے؟ غیربرقرارٹولز ایسے ہیکس کے لئے حساس ہیں جو دریافت خطرات کا استحصال کرتے ہیں۔ ڈویلپر کی ویب سائٹ یا ایپ کا گوگل پلے صفحہ "آخری بار اپڈیٹ" ہونے کی تاریخ چیک کریں۔
- -- ایپ ڈویلپر کتنا قائم ہے ، اور کیا ایسا لگتا ہے کہ وہ وقت کے ساتھ ساتھ ایپ کو برقرار رکھنے کے قابل ہوں گے
- -- کیا ایپ open-source ہے؟ وہ ایپس جو جانچ پڑتال کے لئے کھلی ہیں ان کے حفاظتی امور کو حل کرنے یا کم از کم شناخت کرنے کا زیادہ امکان ہے۔ کیا ڈویلپر ایپ کی افادیت اور حفاظت کے بارے میں شفاف ہے؟

- ۔۔ ایپ ڈویلپر کے کام کے لئے کون سے محرکات یا ترغیبات ہیں اور یہ ان کی قابل اعتمادیت کو کیسے متاثر کرسکتا ہے؟ مثال کے طور پر ، کیا وہ مشن پر مبنی ہیں؟ منافع کے لئے؟ کسی خاص فنڈر کے ذریعہ کفیل ہورہا؟
- اگرچہ اعتماد کے اعتبار کا براہ راست اشارے نہیں ، لیکن ایپ کی لاگت ایک اہم غور ہوسکتی ہے۔ کچھ ایپس میں اعلی ماہانہ سبسکرپشن فیس یا فی ویڈیو فیس ہوتی ہے۔

مزید ایپس کو منتخب کرنے کے لیے EFF سرویلنس سیلف ڈیفنس گائیڈ دیکھیں۔

ایپ کہاں سے ڈاؤن لوڈ کی قابل ہے؟

آپ کو ہمیشہ معتبر ایپ اسٹورز یا ویب سائٹ سے ایپس کو ڈاؤن لوڈ اور انسٹال کرنا چاہئے۔ یہاں تک کہ اگر آپ نے کسی ایپ کی ساکھ کا تعین کرنے کے لئے پوری طرح سے تحقیق کی ہے ، تو خاکے والے ایپ اسٹورز ان کے سامان کو غلط انداز میں پیش کرسکتے ہیں اور آپ کو مذموم مقاصد کے لئے تخلیق کردہ ایک ناجائز نقد کو ڈاؤن لوڈ کرنے کی راہنمائی کرسکتے ہیں۔ مثال کے طور پر ، پچھلے سال ڈیجیٹل رائٹس آرگنائزیشن SMEX نے "واٹس ایپ پلس" نامی ایپ کی مارکیٹنگ کرنے والی مختلف ویب سائٹوں کے بارے میں ایک انتباہ جاری کیا (واضح رہے کہ یہ واٹس ایپ پروڈکٹ نہیں ہے!) ، جو ممکنہ طور پر صارفین کے ڈیٹا کی سٹور اور فروخت کرسکتا ہے ، یا ان فونز کو فعال کرنا جو انسٹال کرتے ہیں اسے ہیک کیا جاتا ہے۔

سیکیورٹی سے متعلق کچھ ڈویلپر یہاں تک کہ کریپٹوگرافک کیز (cryptographic keys) فراہم کرتے ہیں جو آپ کو ان کی صداقت کی تصدیق کرنے کے اہل بناتے ہیں۔ وہ عام طور پر اس بات کی وضاحت فراہم کرتے ہیں کہ ان دستخطوں کی تصدیق کیسے کی جائے۔

ڈیٹا کو کہاں محفوظ کیا جائے گا؟

کچھ دستاویزات ایپس صرف آپ کے ڈیٹا اور دستاویزات کو مقامی طور پر آپ کے ڈیوایس پر اسٹور کرتی ہیں ، جبکہ کچھ صرف یا اضافی طور پر آپ کے ڈیٹا کو کہیں اور بھیج کر اور محفوظ کرتے ہیں۔ بہت سے معاملات میں یہ ایپ کے ڈیزائن اور مقصد کے ساتھ مابعد ہوتا ہے ، جیسے کہ Eyewitness to Atrocities ایپ ، جو آپ کی دستاویزات کی ایک غیر رجسٹرڈ کاپی Lexis Nexis اسٹوریج سہولت کو بھیجتی ہے تاکہ عینی شاہد حراست اور استحکام کی زنجیر کی ضمانت دے سکے۔ آپ اپنے میڈیا کو Eyewitness ایپ کے اندر موجود خفیہ کردہ گیلری سے باہر برآمد کرسکتے ہیں جب اسے حفاظت کے لئے بھیجا جاتا ہے۔

یہ آپ پر منحصر ہے کہ آیا آپ کو صرف اپنے ڈیوایس پر رہنے کے لئے آپ کی دستاویزات کی ضرورت ہے ، چاہے آپ کو کسی قریبی دور دراز مقام پر بھیجنے اور اسٹور کرنے کی ضرورت ہو (جیسا کہ Tella کے ساتھ ایک آپشن ہے) ، یا اسے بیرونی بھیجنے کی ضرورت ہے یا نہیں تنظیم / پلیٹ فارم جو آپ اپنے دستاویزات تک رسائی اور استعمال کرنے کی اجازت دیتے ہیں۔ یہ بات ذہن میں رکھیں کہ انٹرنیٹ بند ہونے کے دوران ، آپ انٹرنیٹ پر اپنی دستاویزات منتقل نہیں کرسکیں گے ، لہذا آپ کو ایک ایسی ایپ درکار ہوگی جو کم سے کم عارضی طور پر آپ کو مقامی طور پر اپنے دستاویزات کو اسٹور (اور مثالی طور پر بیک اپ) کرنے کے قابل بنائے۔ دیکھیں(انٹرنیٹ یا کمپیوٹر کے بغیر فون میڈیا کا بیک اپ ایپ)۔

اگر آپ کا ڈیٹا دور دراز مقام پر بھیجا جائے، تو اس بات سے آگاہ رہیں کہ ڈیٹا کس ملک بھیجا جائے گا۔ ان ممالک میں ڈیٹا کو ظاہر کرنے کا کتنا خطرہ ہے؟ چاہے وہ عدالتی احکامات یا دوسرے ذرائع سے ہو۔ آپکا ڈیٹا ظاہر کرنے کی صورت میں آپ کو کیا خطرہ لاحق ہوسکتا ہے؟

کیا ایپ میرے میڈیا کو انکرپٹ کرتی ہے؟

کچھ ایپس ، جیسے Tella and Eyewitness to Atrocities ، آپ کی دستاویزات کے لئے فائل انکرپشن اور / یا انکرپٹڈ اسٹوریج مہیا کرتے ہیں ، جو کہ آپ کے فون گیلری اور آپ کے فون کے انکرپشن سے الگ ہوتے ہیں ، تاکہ آپ کے میڈیا اور میٹا ڈیٹا کو کبھی بھی آپ کے ڈیوایس پر غیر خفیہ کاری نہیں کی جائے جب تک کہ اس تک رسائی حاصل نہ ہو آپ کے پاس کوڈ تک، اس کا مطلب یہ ہے کہ یہاں تک کہ اگر آپ کا فون غیر مقفل ہے تو ، آپ کی دستاویزات کو خفیہ شدہ نہیں رکھا جائے گا۔ یہ آپ کی دستاویزات کے لئے ایک اضافی سطح کا تحفظ فراہم کرسکتا ہے۔

اگر آپ کے انٹرنیٹ کی بحالی کے بعد ایپ آپ کے میڈیا کو کسی ریموٹ مقام پر بھیجتی ہے اور اسٹور کرتی ہے تو ، اس پر بھی غور کریں کہ آیا آپ کو اپنے ذرائع ابلاغ کو ٹرانزٹ میں رہتے ہوئے اور ریموٹ لوکیشن میں رہتے ہوئے ، مثال کے طور پر EyeWitness ایپ کے ذریعہ انکرپٹ کرنے کی ضرورت ہے۔

یہ بات ذہن میں رکھیں کہ جب کہ زیادہ تر مقامات پر خفیہ کاری قانونی ہے ، کچھ ممالک کے پاس ایسے قوانین ہوسکتے ہیں جو اس کے استعمال کو محدود یا مجرم بناتے ہیں۔ اگر آپ کے ملک میں قوانین کے بارے میں سوالات ہیں تو ، یہ نقشہ (جامع ، لیکن 2017 سے) ایک اچھی شروعات کا مقام فراہم کرتا ہے۔

کیا ایپ نے اہم میٹا ڈیٹا (انٹرنیٹ کے بغیر) حاصل کیا ہے؟

میٹا ڈیٹا وہ ڈیٹا ہے جو آپ کے ویڈیو یا تصویر کے وقت تاریخ اور مقام کی وضاحت کرتا ہے ۔ یہ معلومات کسی خاص واقعے کی دستاویزات کے بطور اپنے ویڈیو یا تصویر کی شناخت ، سمجھنے ، توثیق کرنے اور اس کی تصدیق کےلئے اہم ہے۔ انٹرنیٹ بند ہونے کے تناظر میں ، کسی ایپ کی خود بخود کچھ خاص میٹا ڈیٹا جمع کرنے کی صلاحیت اور / یا آپ کو موقع پر ہی مفید وضاحتی معلومات آسانی سے ان پٹ کرنے کی اجازت دینا خاص طور پر مفید ہے ، کیوں کہ دستاویزات کو شیئر کرنے سے پہلے آپ کو طویل عرصہ ہوسکتا ہے۔ کسی کے ساتھ (وہ وقت جس کے دوران تفصیلات کو فراموش کیا جاسکتا ہے ، حالات بدل سکتے ہیں وغیرہ وغیرہ)۔

زیادہ تر خصوصی دستاویزات کے ایپس جیسے ProofMode ، نے میٹا ڈیٹا کی خصوصیات میں اضافہ کیا ہے ، اور یہ ایک عام بلٹ-ان کیمرا ایپس سے زیادہ میٹا ڈیٹا اکٹھا کرتے ہیں۔ بہتر کردہ میٹا ڈیٹا میں مختلف سینسر ڈیٹا ، قریبی وائی فائی یا بلوٹوتھ سگنلز ، ڈیوایس کا ڈیٹا ، کریپٹوگرافک ہیش ، اور صارف کی فراہم کردہ معلومات شامل ہوسکتی ہیں ، جو بعد میں میڈیا کی توثیق اور تصدیق میں آسانی پیدا کرسکتی ہیں۔

یاد رکھیں کہ انٹرنیٹ بند ہونے کے دوران ، آپ کو ایسی ایپ کی ضرورت ہوگی جس میں میٹا ڈیٹا بنانے یا ریکارڈ کرنے کے لئے ڈیٹا منتقل کرنے کی ضرورت نہیں ہوتی ہے۔ کچھ ایپس کچھ میٹا ڈیٹا جمع کرنے کے لئے ہارڈ ویئر سینسر کی بجائے انٹرنیٹ پر انحصار کرسکتی ہیں۔ مثال کے طور پر ، اگر محل وقوع کا ڈیٹا ڈیوایس پر دیکھنے کے لئے پکڑا جاتا ہے تو ، میٹا ڈیٹا آخری جگہ کی عکاسی کرسکتا ہے جہاں ڈیوایس میں ہارڈ ویئر کی اصل حیثیت کے بجائے ڈیٹا کا رابطہ ہوتا تھا۔ ایپ کو مثالی طور پر آپ کو بغیر انٹرنیٹ کے میٹا ڈیٹا کو مقامی طور پر اسٹور کرنے کی اجازت دینی چاہئے ، جس میں آپ جس فارم کو بھر رہے ہیں اسے بچانا بھی شامل ہے (جیسے Tella کا "offline mode")۔

کیا میں ایپ سے ڈیٹا برآمد کرسکتا ہوں؟

دستاویزات کے لئے آپ کے ارادوں پر منحصر ہے ، یہ ضروری ہوسکتا ہے کہ ویڈیو دستاویزات اور اس کا میٹا ڈیٹا ایپ سے برآمد کریں۔ اس شکل میں جو ایپ کو ملکیتی نہیں ہے۔ یعنی ، ایپ کے باہر میڈیا اور میٹا ڈیٹا کو کھولنے ، دیکھنے اور استعمال کرنے کے قابل ہو۔ ایکسپورٹ کرنے کی صلاحیت کا مطلب یہ ہے کہ آپ اور دوسروں کو کسی دستاویزات تک رسائی حاصل کرنے کے لئے کسی ایک اپلی کیشن یا خدمت فراہم کنندہ پر انحصار نہیں کرنا ہے ، اور آپ کو آگے والے مواد کے ساتھ کام کرنے میں مزید آسانی فراہم کرتی ہے۔ یاد رکھیں کہ اگر آپ کے پاس اعداد کی ترجمانی کرنے کے لئے کچھ ڈیٹا بیس یا تبادلوں کے چارٹس تک رسائی حاصل نہیں ہے تو کچھ میٹا ڈیٹا قابل فہم نہیں ہوسکتا ہے (مثال کے طور پر ، سیل ٹاور آئی ڈی یا وائی فائی نیٹ ورکس کی صورت میں)۔

نوٹ کریں کہ کچھ ایپس کی جان بوجھ کر تحویل میں بند سلسلہ ہوسکتا ہے اور صارفین کو برآمد کرنے کی اجازت نہیں ہوسکتی ہے ، جبکہ کچھ ایپس کو صرف برآمدی استعمال کے معاملے کو ذہن میں رکھتے ہوئے نہیں بنایا جاسکتا ہے۔ یہ بھی جان لیں کہ کچھ ایپس ، جیسے کہ Eyewitness to Atrocities ، آپ کو ایکسپورٹ نہیں کرنے دے سکتے ہیں جب تک کہ آپ میڈیا کو کسی ریموٹ سرور (جس کے لئےآپ کو انٹرنیٹ تک رسائی حاصل کرنے کی ضرورت ہو) پر اپ لوڈ نہ کردیں ، اور کچھ ایپس آپ کو میڈیا ایکسپورٹ کرنے کی اجازت دے سکتی ہیں ، لیکن میٹا ڈیٹا نہیں (کسی بھی میٹا ڈیٹا کے علاوہ جو فائل میں ہی رہتا ہے)۔

اگر آپ کو برآمد کرنے کی ضرورت ہے تو ، مثالی طور پر آپ کی ایپ کو آپ کو بغیر کسی تبدیلی کے میڈیا کی ایک کاپی برآمد کرنے کی اجازت دینی چاہئے ، اور میٹا ڈیٹا کی ایک کاپی کو معیاری پڑھنے کے قابل متن فارمیٹ میں برآمد کرنا چاہئے۔ مثال کے طور پر ، Tella میٹا ڈیٹا Tella گیلری میں خفیہ شدہ ذخیرہ ہے ، لیکن CSV کے بطور برآمد کیا جاسکتا ہے۔ اضافی طور پر ، انٹرنیٹ بند ہونے کے دوران ، آف لائن ایپس یا غیر انٹرنیٹ پر منحصر خدمات کو برآمد کرنے کےلئے آپشنز رکھنے کی ضرورت ہے۔ زیادہ تر ایپس جو آپ کو برآمد کرنے کی اجازت دیتی ہیں ان میں کسی نہ کسی طرح کا "شیئر" بٹن ہوتا ہے جس سے ایک شیئر مینو شروع ہوتا ہے ، جو اینڈرائڈ آپ کے فون پر ایسی ایپس کی فہرست تیار کرتا ہے جو اس قسم کے مواد کو ہینڈل کرنے کی اہلیت رکھتے ہیں۔ بدقسمتی سے ایپ ڈویلپرز اپنے شیئر مینو کو اپنی مرضی کے مطابق تبدیل کرسکتے ہیں اور ایپس کے مابین کوئی مستقل مزاجی نہیں ہے۔

فائلوں کی ایک بڑی مقدار کے لئے ، فائل مینیجر ایپ کے ذریعے ذخیرہ شدہ فائلوں تک رسائی حاصل کرنا اور وہاں سے فائلوں کی کاپی کرنا زیادہ موثر ہوسکتا ہے ، حالانکہ آپ اس طرح کسی ایپ کے ڈیٹا بیس میں محفوظ میٹا ڈیٹا تک رسائی حاصل نہیں کرسکتے ہیں۔ یہ اختیارات ان ایپس کے لئے بھی دستیاب نہیں ہیں جو اپنی محفوظ گیلریوں کی فراہمی کرتے ہیں ، کیونکہ فائلوں کو اسٹوریج میں خفیہ کیا جائے گا۔ ان ایپس کے لئے ضروری ہے کہ ایپ میں اشتراک کرنے کا آپشن ہو۔

اس سیریز کی اگلی پوسٹ اور دستاویزی ایپس کا ہمارا موازنہ چارٹ دیکھیں۔

****

انٹرنیٹ بندش کے وقت قابل تصدیق میڈیا کو برقرار رکھنا

یہ پوسٹ انٹرنیٹ بندشوں کے دوران دستاویزسازی کے سیریز کا ایک حصہ ہے۔

آخری جائزہ: 31 جنوری 2020

انسانی حقوق کے محافظین ، تفتیش کار ، محققین ، اور صحافی اکثر گواہوں کی جانب سے دیئے گئے دستاویزات پہ انحصار کر کے انسانی حقوق کی خلاف ورزیوں کی نگرانی اور ان کی اطلاع دیتے ہیں اس بات کو یقینی بنانا کہ وہ صحیح معلومات پر کام کررہے ہیں ، صارفین ان دستاویزات کی تصدیق اور توثیق کرنے کے لئے اقدامات کرتے ہیں جو انھیں موصول ہوتے ہیں ، جو ایک ایسا عمل ہے جس میں نہایت ہی محنت اور وقت لگتا ہے۔

- بحیثیت دستاویزکار، آپ دستاویزات کی توثیق اور تصدیق دوسروں کے لئے آسان بنانے کے لئے آپ بہت سادہ چیزیں کرسکتے ہیں ، تاکہ وہ بروقت اور موثر طریقوں سے استعمال ہوسکے۔ انٹرنیٹ بندش کے دوران یہ چند اضافی اقدامات مزید قیمتی ہو سکتے ہیں ،

- اگر آپ فوراً اپ لوڈ نہیں کرسکتے ہیں تو ، سوشل میڈیا کے ذریعہ فراہم کردہ اشاعت کی تاریخ اور مقام کی معلومات اتنا مددگار ثابت نہیں ہونگی کہ آپ کا ویڈیو کسی خاص تاریخ سے پہلے یا کسی خاص جگہ پر ریکارڈ کیا گیا تھا۔

- اگر آپ فوراً اپ لوڈ نہیں کرسکتے ہیں تو ، سوشل میڈیا کے ذریعہ فراہم کردہ اشاعت کی تاریخ اور مقام کی معلومات اتنا مددگار ثابت نہیں ہونگی کہ آپ کا ویڈیو کسی خاص تاریخ سے پہلے یا کسی خاص جگہ پر ریکارڈ کیا گیا تھا۔

- اگر دوسرے بھی اپ لوڈ نہیں کر سکتے تو ،ان دستاویزات کی تعداد کم ہوگی جو آپ کے ویڈیو کی تصدیق کے لئے استعمال ہوسکتی ہیں۔

- اگر آپ کو اپنے ویڈیو کو اپنی منزل تک پہنچنے کے لئے بہت سارے ہاتھوں سے آف لائن گزرنے کی ضرورت ہے تو ، دوسروں کے لئے اصل میں ویڈیو کے منبع کا سراغ لگانا مشکل کام ہوسکتا ہے۔

- اگر آپ کو کلاؤڈ بیک اپ کی بغیر موجودگی یا سخت سیکیورٹی یا محدود گنجائش کی وجہ سے اپنے فون سے اصل ویڈیو کو حذف کرنے کی ضرورت پڑھ رہی ہے ، یا اگر آپ کو فون سے چھٹکارا حاصل کرنا ہے، تو ویڈیو کی صداقت کی اصلیت کا پتہ کرنا مشکل تر ہوسکتا ہے۔

- اگر آپ کسی خاص ویڈیو کے بارے میں تفصیلات بھول جاتے ہیں اور جو ایپ آپ استعمال کر رہے ہیں وہ انٹرنیٹ کے بغیر میٹا ڈیٹا کیپچر / ریکارڈ نہیں کرتی تو دوسرے لوگ اس کی بعد میں شناخت نہیں کرسکتے ہیں۔

مندرجہ ذیل معلومات آپ کو انٹرنیٹ بَندش کے دوران اپنے ویڈیو کو برقرار رکھنے میں مدد کرسکتی ہیں تاکہ بعد میں دستاویزات کی حیثیت سے اس کی تصدیقیت اور افادیت کو زیادہ سے زیادہ بنایا جاسکے۔

ویڈیو میں شناخت کرنے والی تفصیلات فلم کریں یا فراہم کریں

اپنے ویڈیو میں ایسی تفصیلات شامل کرنے کی کوشش کریں جس سے تفتیش کار یا صحافی کے لئے بعد میں وقت اور جگہ کی شناخت کرنا آسان ہوجائے، جیسے منفرد نشانیوں، اسکائی لائنز، اسٹریٹ لائنز، اسٹور فرنٹس، لائسنس پلیٹوں، جھنڈوں، گھڑیاں، اخبار کے اگلے صفحات وغیرہ۔ آپ بنیادی معلومات جیسے کہ اپنا نام، پتہ (اگر ایسا کرنا محفوظ ہو

تو)، وقت، تاریخ اور جگہ بھی بیان کرسکتے ہیں (یا ایک کاغز پر لکھ کر اس کی فلم لے سکتے ہیں)۔ آپ جتنی زیادہ تفصیلات شامل کریں گے اتنا ہی ویڈیو کی تحقیق اور تصدیق کرنا دوسروں کے لئے آسان ہوگا، چاہے کہ وہ آپ کو نہیں جانتے ہو یا ان کو نہیں پتہ کہ ویڈیو کہاں سے آئی ہے، کیپچرنگ، اسٹورنگ اور شیرنگ کے بنیادی طریقوں پر ہماری معلومات ضرور دیکھیں:

تفصیل شامل کریں/ میٹا ڈیٹا شامل کریں

دستاویزات کی بہت سی ایپس میں سے ایک سے فائدہ اٹھائیں جو آپ کے فون سے بہتر میٹا ڈیٹا یا تکنیکی معلومات کھینچتے ہیں ، اور آپ کو اضافی وضاحتی معلومات دستی طور پر ڈالنے کی اجازت دیتے ہیں۔ یاد رکھیں کہ ، ایک بندش کے دوران ، آپ کو ایک ایسی ایپ کی ضرورت ہوگی جو اس میٹا ڈیٹا کو ریکارڈ کرنے یا اسٹور کرنے کے لئے انٹرنیٹ پر انحصار نہ کرے۔ پڑتا ل کریں "کیا مجھے یہ دستاویزی ایپ استعمال کرنا چاہئے؟ مناسب ایپ کو منتخب کرنے کے طریقہ کے بارے میں مزید معلومات حاصل کریں۔

یہاں تک کہ اگر آپ ایک خصوصی دستاویزات ایپ کا استعمال نہیں کررہے ہیں ، تب بھی آپ اپنے فون پر نوٹوں ، نقشوں یا تصاویر کی شکل میں اضافی معلومات تشکیل دے سکتے ہیں۔ آپ اپنی پسندیدہ فائل مینیجر ایپ کا استعمال کرکے اس ویڈیو کو اس اضافی معلومات کے ساتھ ترتیب دے سکتے ہیں۔ کلیدی اضافی معلومات میں وقت ، تاریخ ، ریکارڈ شدہ واقعے کا مقام اور اسی طرح ریکارڈنگ کا ذریعہ (یعنی آپ کا نام اور رابطہ کی معلومات) شامل کرنا ضروری ہیں۔ جب آپ اسے شیئر کرے تو میٹا ڈیٹا ایکسپورٹ کریں اور ویڈیو کے ساتھ شامل کریں (آپ یہ سب فولڈر میں ڈال سکتے ہیں اور زپ کرسکتے ہیں)۔

بیک اپ رکھیں

اپنے فون سے میڈیا کو باقاعدگی سے 2 الگ اسٹوریج آلات پر بیک اپ بنالے ۔ آپ مثال کے طور پر ، کمپیوٹر کے بغیر بھی ، (On-the-Go OTG) یا وائرلیس تھمب ڈرائیو کو اپنے فون سے جوڑسکتے ہیں ۔ مزید تفصیلات کے لئے "انٹرنیٹ یا کمپیوٹر کے بغیر فون میڈیا کا بیک اپ بنانا" پر ہمارے نکات دیکھیں۔ بیک اپ کرنا اس بات کو یقینی بنائے گا کہ اگر آپ اپنا فون کھو جاتا ہے یا توڑ جاتا ہے، یا آپ کو اپنے فون سے ویڈیوز کو ڈیلیٹ کرنے کی ضرورت ہوتی ہے تو آپ اپنے ویڈیو کی کاپی برقرار رکھ سکتے ہیں۔ آپ کی اصل ویڈیو کی محفوظ کاپی ہونا ایک تفتیش کار یا صحافی کو بھی قابل بناتا ہے جو آپ کے ویڈیو کو کسی اور ذریعہ سے دیکھتا ہے کہ بعد میں آپ سے براہ راست ویڈیو حاصل کر سکے (جب تک کہ وہ اس کو آپ تک تلاش کرنے میں کامیاب ہوجائیں) ، جس سے ایک مختصر اور زیادہ مکمل سلسلہ پیدا ہوتا ہے۔

****

انٹرنیٹ یا کمپیوٹر کے بغیر فون میڈیا کا بیک اپ (بیک اپ) بنانا

یہ پوسٹ انٹرنیٹ بندشوں کے دوران دستاویزسازی پہ سیریز کا ایک حصہ ہے۔
آخری جائزہ: 31 جنوری 2020

بیک اپ (Back-up) اس بات کی یقین کرنے کے لئے کلیدی حیثیت رکھتا ہے کہ اگر آپ کا ڈیوایس ضبط ہوجاتا ہے تو غلطی سے آپ کے ڈیٹا اور دستاویزات کو حذف ، خراب ، یا گم نہیں کیا جا سکتا ۔ انٹرنیٹ بندش یا سست روی کے دوران ، آپ اپنا باقاعدہ کلاؤڈ بیک اپ نہیں چلا پائیں گے یا اپنی دستاویزات کو کسی محفوظ جگہ پر نہیں بھیج سکیں گے ۔ ڈیسک ٹاپ یا لیپ ٹاپ کمپیوٹر پر آف لوڈ کرنا بیک اپ کا ایک طریقہ ہے، لیکن چونکہ اکثر لوگوں کو اس تک رسائی حاصل نہیں ہوتی ہے ، لہذا کمپیوٹر انٹرنیٹ بندش کے دوران اپنے میڈیا سے بیک اپ حاصل کرنے کے لئے کچھ اختیارات اور نکات یہ ہیں۔

او ٹی جی (OTG) یا وائرلیس ڈرائیو استعمال کریں

و ٹی جی ، یا on-the-go ، ڈرائیوز ایک قسم کی USB ڈرائیو ہیں جو بہت سے اینڈرائڈ (Android) (لیکن سبھی اینڈرائڈ کے ساتھ نہیں۔ آپ OTG تھمب ڈرائیو کو براہ راست اپنے فون میں پلگ کرسکتے ہیں ، یا اپنے فون کو باقاعدہ USB ہارڈ ڈرائیو سے مربوط کرنے کے لئے OTG-to-USB اڈاپٹر کا استعمال کرسکتے ہیں۔ OTG کی مدد سے، آپ کا فون ڈرائیو کے لئے طاقت فراہم کرتا ہے۔

OTG ڈرائیوز کے مشہور برانڈز میں سانڈیسک، کنگسٹن اور سیمسنگ شامل ہیں، اگرچہ بہت سارے اور بھی ہیں۔ ذخیرہ کرنے کی گنجائش کے حساب سے ان کی قیمت عام طور پر 8 سے 2 امریکی ڈالر تک ہوتی ہے۔

وائرلیس تھمب ڈرائیوز / ہارڈ ڈرائیوز عام ہارڈ ڈرائیوز کی طرح ہیں سوائے اس کے کہ ان کو کیبل کی ضرورت نہیں پڑتی ہے۔ اس کی وجہ سے آپ ایسے آلات Hard drives سے جوڑ سکتے ہیں جو عام طور پر نہیں جڑتے جیسے آپ کا فون۔ OTG ڈرائیو پر وائرلیس ڈرائیو کا فائدہ یہ ہے کہ آپ ایک ہی بار میں متعدد صارفین کو اسی وائرلیس ڈرائیو سے جوڑ سکتے ہیں جو کہ مفید ثابت ہوسکتا ہے ، مثال کے طور پر ، جب آپ ایک ٹیم کی حیثیت سے احتجاج کی صورت حال میں فلم بندی کر رہے ہو- ہر شخص کی فوٹیج کا بیک اپ کسی بھی دوسرے ٹیم ممبر کی ہارڈ ڈرائیو میں لیا جاسکتا ہے جو کہ کسی دوسرے ممبر کے ساتھ ہے۔ نوٹ کریں کہ چونکہ وہ کسی ڈیوایس سے چارج نہیں کھینچ رہے ہیں ، لہذا وائرلیس ڈرائیوز بیٹری کی چارج پر انحصار کرتی ہیں جو چارج کرنی پڑتی ہے۔

سانڈیسک وائرلیس تھمب ڈرائیو کا سب سے مشہور برانڈ ہے ، حالانکہ یہاں اور بھی برانڈز ہیں۔ عام طور پر وائرلیس تھمب کی ڈرائیو OTG ڈرائیوز سے زیادہ مہنگی ہوتی ہے، اور اسٹوریج کی گنجائش کے حساب سے تقریبا 25 سے 100 امریکی ڈالر کی مالیت ہوتی ہے۔ بڑی وائرلیس بیرونی ہارڈ ڈرائیوز اسٹوریج کی گنجائش کے حساب سے قیمت لگ بھگ 150 امریکی ڈالر سے شروع ہوتی ہیں۔

متبادل: پرانا غیر استعمال شدہ فون استعمال کریں

اگر آپ کے پاس OTG یا وائرلیس ڈرائیو نہیں ہے، لیکن آپ کے پاس ایک پرانا فون ہے جو اب بھی کام کرتا ہے جسے آپ اب استعمال نہیں کرتے ہیں، آپ بیک اپ کے لئے اس بھی کا استعمال کرسکتے ہیں۔ جب تک کہ دونوں فونزآپسی فزیکل حد میں ہوں، Bluetooth, Wi-Fi Direct, or Near Field Communication (NFC) / Android Beam کا استعمال کرکے ایک سے دوسرے تک میڈیا کو شیئر اور کاپی کرسکتے ہیں۔ بلوٹوتھ اور وائی فائی ڈائریکٹ دونوں وائرلیس ٹیکنالوجیز ہیں جو کسی دوسرے روٹر یا رسائی کے نقطہ کے بغیر دو ڈیواسس کو "کنکٹ" کرتئ ہیں، 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) ہے اور کم تر منتقلی کی رفتار ہے ، لیکن تیز رفتار سے جڑتا ہے اور کم طاقت

کا استعمال کرتا ہے ، لہذا جب آپ کے پاس دونوں آلات ہاتھ میں ہوں تو فوری طور پر چھوٹی چھوٹی منتقلی کے لئے مفید ثابت ہوسکتی ہے۔

آپ کے فون میں شاید بلٹ-ان بلوٹوتھ ، وائی فائی ڈائرکٹ ، یا این ایف سی ایپس / خصوصیات ہیں جو آپ کو اشتراک کرنے کے لئے قریبی ڈیوایسس کا انتخاب کرنے کی سہولت دیتے ہیں۔ اگر دونوں فونز میں Files By Google انسٹال ہے تو، آپ ایپ میں ان ٹیکنالوجیز کا استعمال کرکے فائلیں آف لائن بھی شیئر کرسکتے 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 ڈیوایسس کی تحقیقات کے لئے استعمال کیا جاسکتا ہے۔ دراندازِ شاید آپ کے ڈیوایس کے ساتھ کنکشن بنانے اور ناپسندیدہ فائلیں بھیجنے یا وہ آپ کے آلے کو اپنے کنٹرول میں لے سکتے ہیں، محفوظ تر بننے کے لئے، **یہ خدمات ان کے عدم استعمال میں بند کرسکتے ہیں اور جب آپ محفوظ مقامات پہ ہو تو ان کو پھر سے آن کرسکتے ہیں ، ایپ کی اجازت کو اپنی ضرورت کے حساب سے محدود کرے ، اور اپ ڈیٹ کو چلانے اور اچھے فون سیکیورٹی اورمضبوط پاس کوڈ رکھنے پر عمل کریں۔**

کوئی الگ تفصیل / میٹا ڈیٹا شامل کریں

جب میڈیا کو کسی او ٹی جی ڈرائیو، وائرلیس ڈرائیو، یا کسی پرانے فون میں کاپی کرنا ہو تو، کوئی ایسی وضاحتی معلومات یا میٹا ڈیٹا شامل کرنا مفید ہے جو میڈیا سے الگ ہو ۔ بہت سے دستاویزی ایپس، مثال کے طور پر، CSV یا JSON ٹیکسٹ دستاویزات تیار کرتی ہیں جس میں آلہ سے نکالا ہوا میٹا ڈیٹا (جیسے جغرافیائی محل وقوع، وقت، تاریخ) اور صارف کی طرف سے دستی طور پر داخل کردہ کوئی بھی تفصیل شامل ہے۔ ان میٹا ڈیٹا دستاویزات کو اپنے بیک اپ میں بھی شامل کرنا اور برآمد کرنا یقینی بنائیں۔

پاس ورڈ سے ڈرائیو کی حفاظت کریں

بہت سی وائرلیس ڈرائیوز موبائل ایپ کے ذریعے پاس ورڈ سے محفوظ ہوسکتی ہیں جو ڈرائیو کے ساتھ آتی ہیں۔ نوٹ کریں کہ پاس ورڈ سے تحفظ انکرپشن کی طرح نہیں ہے (نیچے ملاحظہ کریں) زیادہ تر وائرلیس یا OTG ڈرائیو صرف موبائل فون کا استعمال کرتے ہوئے فل ڈسک انکرپشن کو حاصل نہیں کرپاتی، حالانکہ یہ کمپیوٹر کے استعمال سے فل ڈسک انکرپشن پا سکتی ہے۔

فائلوں کو خفیہ کرنے پر غور کریں

اگر آپ کو اپنی فائلوں کو زیادہ محفوظ طریقے سے اسٹور کرنے کی ضرورت ہے تو ، آپ اپنے بیک اپ کو انکرپٹ کرنے پر غور کر سکتے ہیں۔ اگرچہ آپ زیادہ تر وائرلیس یا OTG ڈرائیوز کو موبائل فون سے انکرپٹ نہیں کرسکتے، لیکن فائلوں کو ڈرائیو پر منتقل کرنے سے پہلے آپ ان کو خود انکرپٹ کرسکتے ہیں۔ کچھ ایپس جو Android پر فائلوں کو انکرپٹ کرسکتی ہیں ان میں ZArchiver ، اور RAR شامل ہیں۔ خیال رہےکہ آپ اپنے انکرپشن پاس ورڈ کو ضرور یاد رکھے۔ اگر آپ پاس ورڈ کھو دیتے ہیں تو انکرپٹ کردہ فائلوں کی بازیافت کا کوئی راستہ نہیں ہے۔

یہ بات ذہن میں رکھیں کہ کچھ ممالک میں ایسے قانون ہوسکتے ہیں جو انکرپشن کے استعمال کو محدود یا جرم بناتے ہیں۔ حکام کو اپنے ڈیٹا تک رسائی حاصل کرنے سے روکنے کے لئے ان کا استعمال شواہد کو ختم کرنا یا تفتیش میں رکاوٹ بنتے ہوئے دیکھا جاسکتا ہے، اور یہ جرم کی حیثیت سے قابل سزا ہوسکتی ہے۔ یہ 2017 کا نقشہ پرانا ہوسکتا ہے لیکن اگر آپ کے ملک میں قوانین کے بارے میں سوالات ہیں تو وہ اچھی شروعات کا موقع فراہم کرتا ہے۔

علیحدہ مقامات پر 2 بیک اپ بنائیں۔

ایک بیک اپ ہمیشہ قابل اعتماد نہیں ہوتا ہے۔ مثال کے طور پر ، آپ بیک اپ آلہ سے محروم ہو سکتے ہیں ، اسے نقصان پہنچا سکتے ہیں ، یا یہ سیدھے ناکام ہوسکتا ہے۔ آئی ٹی ماہرین عام طور پر لوگوں کو علیحدہ مقامات پر رکھے ہوئے علیحدہ آلات پر 2 بیک اپ (یعنی کل 3 کاپیاں) رکھنے کا مشورہ دیتے ہیں۔ اس سے کسی ایک خاص کاپی کے لئے خطرہ کو کم کرنے میں مدد ملتی ہے۔

****

انٹرنیٹ بندش کے دوران فائل شیئرنگ اور مواصلت

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, Wi-Fi Direct, or NFC** کے ساتھ شیئر کریں

بلوٹوتھ ، وائی فائی ڈائرکٹ (Wifi Direct)، یا نزدیک فیلڈ مواصلات (Android Beam) (NFC) کے ذریعے اپنے فون کو قریبی ڈیوایس 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 "کنکٹ" کر 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 چارج 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 چارج 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۔ دارنداز 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۔

اس کے علاوہ ، دوسرا آپشن PirateBox بھی ہے ، do-it-yourself پروجیکٹ جو آزادانہ طور پر لائسنس یافتہ سافٹ ویئر فراہم کرتا ہے۔ صارفین 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۔ Piratebox ہدایات 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.

پیئر ٹو پیئر چیٹ کے ذریعے بات چیت کریں۔

دو نئی پیئر ٹو پیئر میسجنگ ایپس جن کے بارے میں ہم ایکٹیوسٹ نیٹ ورکس کے ذریعے واقف ہوئے ہیں وہ ہیں برئیر (Briar) اور برج فائی (Bridgefy)۔ ہم نے انہیں ابھی تک آزمایا نہیں ہے، لیکن ہم دوسروں کو جانتے ہیں جو ان کی جانچ کر رہے ہیں۔

برئیر Briar ایک اوپن سورس، اینڈ ٹو اینڈ انکرپٹڈ میسجنگ ایپ ہے جو کسی مرکزی سرور پر انحصار نہیں کرتی ہے، بلکہ اس کے بجائے صارفین کے آلات کے درمیان پیغامات کو ہم آہنگ کرتی ہے (لہذا مواد ہر صارف کے آلے پر رہتا ہے)۔ یہ بلوٹوتھ یا وائی فائی کا استعمال کرتے ہوئے انٹرنیٹ نہ ہونے پر بھی مطابقت پذیر ہوسکتا ہے (جب انٹرنیٹ موجود ہو تو ایپ ٹور نیٹ ورک پر آلات کو ہم آہنگ کرتی ہے)۔ برئیر میں نجی گروپس، عوامی فورمز اور بلاگز بھی شامل ہیں۔ آف لائن استعمال کرتے وقت، آپ کی رینج آپ کے بلوٹوتھ یا وائی فائی کی حد (زیادہ سے زیادہ ~ 100 میٹر) تک محدود ہے۔
جبکہ، Bridgefy ایک اینڈ ٹو اینڈ انکرپٹڈ (سوائے "براڈکاسٹ" فیچر استعمال کرنے کے وقت) میسجنگ ایپ ہے جو پیغامات بھیجنے کے لیے بلوٹوتھ کا استعمال کرتی ہے۔ برئیر Briar کے برعکس، پیغامات دوسرے برج فائی Bridgefy صارفین کے میش نیٹ ورک کے ساتھ ہاپ کر کے طویل فاصلے تک سفر کر سکتے ہیں (صرف مطلوبہ وصول کنندہ ہی پیغام پڑھ سکتا ہے)۔ Bridgefy میں Briar کے پرائیویٹ گروپس، فورمز اور بلاگ کی خصوصیات کا فقدان ہے، لیکن اس میں براڈکاسٹ موڈ ہے جس کے ذریعے آپ حد کے اندر Bridgefy 7 صارفین کو پیغام بھیج سکتے ہیں، جنہیں آپ کے رابطے ہونے کی ضرورت نہیں ہے (براڈکاسٹ پیغامات ضروری نہیں ہیں خفیہ کردہ)۔

انکرفٹڈ کے ذریعے بات چیت کریں۔

ایس ایم ایس ٹیکسٹ پیغامات سیل نیٹ ورکس پر بھیجے جاتے ہیں اور انٹرنیٹ پر انحصار نہیں کرتے، اس لیے انٹرنیٹ بند ہونے کے دوران بھی کام کر سکتے ہیں۔ تاہم، ایس ایم ایس کو بہت غیر محفوظ سمجھا جاتا ہے۔ واٹس ایپ یا سگنل جیسی انٹرنیٹ پر منحصر ایپس کے برعکس، ایس ایم ایس اینڈ ٹو اینڈ انکرپٹڈ نہیں ہے۔ اس کا مطلب ہے کہ ٹیکسٹ پیغامات (اور ان کا میٹا ڈیٹا) حکومتیں اور موبائل کیریئرز پڑھ سکتے ہیں، یا ہیکرز کے ذریعے روکا جا سکتا ہے۔ ایس ایم ایس کو "جعلی" بھی کیا جا سکتا ہے، مطلب یہ ہے کہ بھیجنے والا دوسرے صارف کی نقالی کرنے کے لیے اپنے پتے کی معلومات میں ہیرا پھیری کر سکتا 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۔

جزوی شٹ ڈاؤنز: مسدود سائٹس کو روکنا:

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؟ کچھ 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۔

وی پی این (VPN)

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 یا 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۔
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۔

ڈی این ایس سرورز DNS SERVERS

ڈی این ایس (DNS) سرورز ان ڈومین ناموں کا جو صارفاین براوزر 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 جنھوں 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

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