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 استعمال 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 اینڈروئیڈ 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 نقاَص 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 Content Lock (LG)) 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 ڈیواسس 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 انکرپٹ 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 (OTG (OTG (USB On-The-Go 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۔

اس سلسلے کی اگلی پوسٹ دیکھیں ، "کیا مجھے یہ دستاویزی ایپ استعمال کرنا چاہئے؟"