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

انٹرنیٹ بندشوں کے دوران دستاویزسازی

یہ پوسٹ انٹرنیٹ بندشوں کے دوران دستاویزسازی پہ سیریز کا ایک حصہ ہے۔
عربی اور ہسپانوی میں بھی دستیاب 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 آلہ ضبط ہوجاتا ہے تو غلطی سے آپ کے ڈیٹا اور دستاویزات کو حذف ، خراب ، یا گم نہیں کیا جا سکتا ۔ انٹرنیٹ بند 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 نہیں) کے ساتھ مطابقت رکھتی ہیں۔ 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 استعمال کرسکتے ہیں۔ OTG کی مدد سے ، آپ کا فون ڈرائیو کے لئے طاقت فراہم کرتا ہے

ڈرائیوز کے مشہور برانڈز میں سانڈیسک ، کنگسٹن اور سیمسنگ شامل ہیں ، اگرچہ بہت سارے اور بھی ہیں۔ OTG ذخیرہ کرنے کی گنجائش کے حساب سے ان کی قیمت عام طور پر ۸ سے ۲۵ 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۔یہ 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 ٹیم کے کسی دوسرے ممبر کے ساتھ ہے۔ نوٹ کریں کہ چونکہ وہ کسی آلہ سے طاقت نہیں کھینچ رہے ہیں ، لہذا وائرلیس ڈرائیوز بیٹری کی طاقت پر انحصار کرتی ہیں جو چارج کرنی پڑتی ہے۔

شاید SanDisk وائرلیس تھمب ڈرائیو کا سب سے مشہور برانڈ ہے ، حالانکہ وہاں اور بھی ہیں۔ عام طور پر وائرلیس تھمب کی ڈرائیو OTG ڈرائیوز سے زیادہ مہنگی ہوتی ہے ، اور اسٹوریج کی گنجائش کے حساب سے تقریبا ۲۵ سے ۱۰۰ امریکی ڈالر کی مالیت ہوتی ہے۔ بڑی وائرلیس بیرونی ہارڈ ڈرائیوز اسٹوریج کی گنجائش کے حساب سے قیمت لگ بھگ ۱۵۰ 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 بھی اس کا استعمال کرسکتے ہیں۔ جب تک کہ دونوں فونزآپسی فزیکل حد میں ہوں ، / Bluetooth, WiFi Direct, or Near Field Communication (NFC) Android Beam کا استعمال کرکے ایک سے دوسرے تک میڈیا کو مربوط اور کاپی کرسکتے ہیں۔ بلوٹوتھ اور وائی فائی ڈائریکٹ دونوں وائرلیس ٹیکنالوجیز ہیں جو دو آلات کا "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) 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 آلات 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 آلے کی تحقیقات کے لئے استعمال کیا جاسکتا ہے۔ درانداز آپ کے آلہ کے ساتھ جوڑا بنانے ، 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۔

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 استعمال کیا جاسکتا ہے۔ درانداز آپ کے آلہ کے ساتھ جوڑا بنانے ، 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 دستاویزات 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۔

اس سیریز کا آخری پوسٹ دیکھیں "انٹرنیٹ بند کے دوران مواصلت اور فائل شیرنگ"