المحتويات

التوثيق أثناء حجب الانترنت
سلسلة تدوينات مع نصائح عملية

كتابة إيفون ن ج

بالتعاون مع أرول براكاش
تمت مراجعته في 31 يناير 2020

في يونيو 2019، ومع استمرار انتهاكات حقوق الإنسان والأزمة الإنسانية في ميانمار، قامت وزارة النقل والاتصالات هناك بإصدار تعليمات لشركات الاتصالات بحجب الإنترنت عبر الهاتف المحمول في أجزاء من ولاية راخين وولاية تشين المجاورة لها. ونقلا عن منطمتي "اضطرابات السلام" و "الأنشطة غير القانونية"، تزعم حكومة ميانمار أنها قامت بحجب الانترنت "لمصلحة الشعب".
وكان قد أثر الحجب على أكثر من مليون شخص ومنعهم من الوصول إلى المعلومات والاتصالات الأساسية مما نتج عنه تعطيل للجهود الإنسانية. وكما قال ماثيو سميث من مؤسسة Fortify Rights أن "هذا الإغلاق يحدث في سياق الإبادة الجماعية المستمرة ضد "الروهينجا" وجرائم الحرب ضد سكان "راخين" وحتى لو كان الهدف منه استهداف المسلحين ، فهو غير مناسب بشكل كامل".

تم رفع الحجب جزئيًا في خمس مدن في سبتمبر 2019 ، لكنه لا يزال مستمراً. وفي خلال الشهر نفسه وفي بنجلاديش المجاورة حيث فر إليها الكثير من الروهينجا، أمرت السلطات مشغلي الهاتف المحمول بحظر خدمات 3G و 4G في مخيمات اللاجئين الروهينجا والتوقف عن بيع بطاقات SIM للروهينجا. ومع دخولنا عام 2020 لا تزال أربع مدن في "راخين" معزولة عن العالم ولا تزال تواصل بنغلاديش الحد من خدمات الانترنت في مخيمات اللاجئين.

التوثيق خلال حجب الانترنت

أما على الصعيد العالمي تتزداد عمليات إغلاق الإنترنت. فوفقًا لحملة "#KeepItOn" والتي ترعاها مؤسسة AccessNow كان هناك 128 حجب متعمدًا للإنترنت في الفترة من يناير إلى يوليو 2019 ، مقارنة بـ 196 في عام 2018، و 106 في عام 2017 ، و 75 في عام 2016.
حول العالم تقوم الحكومات بالتعاون مع قطاع الاتصالات، بإغلاق الإنترنت بشكل متزايد كاستراتيجية لقمع المجتمعات، ومنع التعبئة وأيضًا وقف المعلومات المتعلقة بانتهاكات حقوق الإنسان من توثيقها ومشاركتها.

"حجب الانترنت وانتهاكات حقوق الإنسان يتعاونان سويا يد بيد."

بيرهان تايي - AccessNow

يمكن أن تتخذ عمليات حجب الانترنت أشكالًا متعددة، بما في ذلك العوائق التي تستهدف تطبيقات أو مواقع بعينها أو إيقاف تشغيل بيانات الهواتف الخلوية.
تهدف جميع أنواع حجب الانترنت إلى تعطيل القدرة على توصيل المعلومات وفضح الانتهاكات في الوقت الفعلي وغالبًا ما تحدث أثناء الاحتجاجات والانتخابات أو فترات عدم الاستقرار السياسي، وغالبًا ما تكون مصحوبة بقمع الدولة المتزايد والهجمات العسكرية والعنف.
وفي حين أن الحكومات قد تحاول تبرير الإغلاقات باسم "السلامة العامة" أو لأسباب أخرى، فإن محاولات حجب الانترنت تحدث بوضوح في لحظات تخشى فيها الدول القمعية فقدان السيطرة على شعوبها. تنتهك عمليات الحجب حقوق الإنسان وتعطل حياة الناس وسبل عيشهم بشدة كما أن لها تأثيرًا اقتصاديًا عالميًا.

توثيق انتهاكات حقوق الإنسان لا يقل أهمية عن أي وقت مضى أثناء حجب الإنترنت. حتى إذا كان يتعذر مشاركة المعلومات في الوقت نفسه، يمكن أن تكون الوثائق وسيلة للحفاظ على الأصوات التي تحاول السلطات إسكاتها، ولضمان الحصول على أدلة على الانتهاكات التي يمكن استخدامها للمطالبة بالمساءلة لاحقًا.
بطبيعة الحال، فإن السياق القمعي والعقبات التكنولوجية لإغلاق الإنترنت تجعل انتهاكات الوثائق - والحفاظ على تلك الوثائق بشكل آمن - أكثر تحديا وخطورة. tكيف يمكن للنشطاء التقاط مقاطع الفيديو الخاصة بهم والحفاظ عليها أثناء إيقاف التشغيل؟ وحتى مشاركتها دون اتصال بالإنترنت ، والقيام بذلك بطرق أكثر أمانًا؟

هذه السلسلة من التدوينات ستحاول الإجابة على تلك الاسئلة

من خلال عملنا مع النشطاء الذين عانوا من إيقاف تشغيل الإنترنت، تعلمنا بعض النصائح والنهج المفيدة لالتقاط والحفاظ على وثائق الفيديو أثناء عمليات إيقاف الإنترنت التي نشاركها في هذه السلسلة. قمنا بكتابتها مع وضع أجهزة Android في الاعتبار ولكن يمكن تطبيق النصائح على أجهزة iPhone أيضًا.
تتطلب بعض الاستراتيجيات التخطيط المسبق (وغالبًا الوصول إلى الإنترنت) ، لذلك من الجيد أن تقوم بمراجعتها وتنفيذ أي خطوات قبل أن تكون في موقف لا يتوفر لديك فيه الإنترنت وتحتاج إلى توثيق.
احفظ نسخة من أي من البرامج التعليمية حتى تتمكن من الرجوع إليها أو مشاركتها أثناء إيقاف التشغيل.
وأخيرًا ، ابدأ في ممارسة التقنيات والأساليب بشكل يومي حتى تصبح قبل أن تكون في حالة أزمة.

التجهيز :
تجهيز الهاتف المحمول للتوثيق في حالة حجب الانترنت

التصوير :
هل يجب أن استخدم هذا التطبيق للتوثيق؟

الحفاظ والصيانة :

الحفاظ على المادة الموثقة خلال فترة حجب الانترنت، ووجود نسخة آخرى احتياطية بدون أنترنت أو كومبيوتر.

المشاركة والنشر والتواصل :
مشاركة المواد والتواصل خلال انقطاع الانترنت.

من دليل #keepItOn

ملاحظة أخيرة: على الرغم من أن هذه النصائح يمكن أن تساعدك في الاستمرار في التوثيق في مواجهة حجب الانترنت إلا أننا نريد التأكيد على أن الحل النهائي يجب أن يكون لاستعادة الوصول إلى الإنترنت والدفاع عن حق الناس في التوثيق وحرية التعبير وتداول المعلومات.
هناك حركة عالمية تقودها مؤسسات مثل NetBlocks و AccessNow والعديد من المؤسسات الأخرى يقومون بمراقبة ومشاركة المعلومات حول عمليات الحجب بشكل نشط. وينخرط المحامون أيضاً على مستوى العالم في التقاضي الاستراتيجي ضد عمليات الحجب. وبالتأكيد نحن متضامنون مع عملهم لدعم حقوق الإنسان.

****

ضبط هاتفك للتوثيق أثناء حجب الإنترنت

سلسلة تدوينات التوثيق أثناء حجب الانترنت
بواسطة إيفون ن ج

هذه التدوينة جزء من سلسلة تدوينات التوثيق أثناء حجب الاننترنت

بالمشاركة مع أرول باركش

تمت مراجعته في *31* يناير *2020*

على الرغم من حجب الإنترنت، لا يزال بإمكان المهتمين بالتوثيق التقاط مقاطع الفيديو المهمة والتي يمكن مشاركتها أثناء عدم الاتصال بالانترنت أو عندما عند عودته مرة أخرى.

إليك بعض النصائح التي تعلمناها من الناشطين والخبراء لإعداد هاتفك للتوثيق في وضع عدم الاتصال. لاحظ أن بعض الخطوات تتطلب الاتصال بالانترنت، لذلك يجب أن يتم ذلك قبل حدوث الحجب أو خلال فترات عودة الانترنت. أيضًا، لا تنتظر حتى تكون في موقف حرج أو ليس لديك الكثير من الوقت لتفعيل هذه الخطوات ؛ افعلها الآن ، واستغرق كل الوقت الذي تحتاجه في استعمال هاتفك قبل أن تضطر إلى استخدامه أثناء أزمة.

غالبًا ما تتزامن عمليات الإغلاق مع زيادة الرقابة على المعلومات والقيود المفروضة على حرية التعبير والتجمع. إذا كنت تحاول التوثيق، فعليك اتخاذ احتياطات إضافية لحماية نفسك ومعلوماتك خلال هذه الفترات. إذا كان هناك خطر من قيام السلطات بمصادرة هاتفك، أو إجبارك على فتحه والكشف عن محتوياته (أثناء حجب الانترنت أو في أي وقت آخر)، ففكر مثلا في استخدام هاتف منفصل للتوثيق من هاتفك الشخصي الأساسي. يمكن أن يساعد هذا في تقليل المعلومات التي تحملها والتي يمكن اختراقها (مثل جهات الاتصال

والحسابات والرسائل وغيرها). إذا لم تتمكن من استخدام جهاز آخر، فلا يزال بإمكانك اتباع هذا الدليل لتقليل كمية البيانات الحساسة وتحسين مستوى الأمان على هاتفك الأساسي.

لو كنت ستقوم باستخدام هاتف قديم فعليك مسحه أولاً.

لمسح هاتفك قم بإعادة ضبط المصنع.

ملاحظة: أظهرت الدراسات أن تشغيل إعادة ضبط المصنع على هاتفك لا يؤدي بالضرورة إلى مسح جميع البيانات. في الواقع ، فإن الطريقة الآمنة 100٪ فقط لمسح البيانات هي تدمير الهاتف ، لكن هذه الطريقة ليست خيارًا إذا كنت ترغب في إعادة استخدام الهاتف! في هذه المقالة يقترح مهندس Android التأكد من تشفير محتويات جهازك قبل إعادة ضبط المصنع. التشفير هو الافتراضي على معظم الهواتف الحالية على أي حال ، ولكن في حالة عدم التشفير ، انتقل إلى الإعدادات> الأمان> تشفير الهاتف ثم إعادة الضبط المصنع وبهذه الطريقة، يتم فقد مفتاح التشفير ، وحتى إن كان هناك أي مواد لم يتم مسحها فلن تكون قابلة للقراءة.

تعود على ممارسة أدوات الأمان الأساسية في هاتفك

هناك ممارسات عامة للأمان خاصة بالهاتف المحمول ويمكن أن تكون فعالة في كل المواقف ، سواء كنت تقوم بالتوثيق أثناء حجب الانترنت أو لا. فيما يلي بعض المصادر المفيدة من المنظمات الأخرى. مع التنبيه بأن لا شيء يضمن الأمن بنسبة 100 ٪
بعض النصائح الرئيسية تشمل:
تأكد من تشفير هاتفك. تحتوي الهواتف الأحدث على تشفير افتراضيًا. إذا لم تكن متأكدًا من إذا كان هاتفك مشفر أم لا، فقم بالتحقق من إعدادات الأمان على هاتفك.
قم بتشغيل تحديثات نظام التشغيل (OS) بشكل منتظم ، لأنها تعمل غالبًا على إصلاح الثغرات الأمنية.
قم بتحديث تطبيقاتك المهمة (مثل تطبيقات المراسلة) بانتظام.
قم بتعيين رمز مرور قوي للهاتف يحتوي على 6 أرقام على الأقل ولا يعتمد على البصمة / اللمس أو معرف الوجه.
إعداد قفل الشاشة
قم بإيقاف تشغيل خدمات الموقع GPS إذا لم تكن في حاجة إليها، وقم بالتحقق أيضا من أذونات ال GPS للتطبيقات الفردية.
قم بإيقاف تشغيل Bluetooth و WiFi عندما لا تحتاج إليها ، لتجنب تتبع الجهاز.
قم بإيقاف تشغيل الهاتف عندما لا تستخدمه.
قم تثبيت تطبيقات وثائق مفيدة

بالنسبة إلى وثائق الصور أو الفيديو ، يمكنك استخدام تطبيق الكاميرا الموجود على هاتفك ، أو يمكنك استخدام تطبيق وثائق أكثر تخصصًا ، مثل **ProofMode** أو غيره ، مما يتيح التقاط بيانات تعريفية أكثر قوة وتحديد الهوية والمصادقة والتشفير ومميزات آخرى يتيحها التطبيق.

يعد تطبيق OONI Probe أحد التطبيقات المفيدة لتوثيق حجب الانترنت نفسه ، هو تطبيق مفتوح المصدر يقوم بإجراء اختبارات من هاتفك لقياس ما إذا كانت المواقع أو الأنظمة الأساسية محظورة أم لا. يمكن أن يوضح لك كيف يتم حظر المواقع ومتى وأين ومن يقوم حظرها. تأكد من فهم المخاطر المحتملة قبل استخدام هذا التطبيق.

لست متأكد من تطبيقات التوثيق المناسبة لك؟ في هل يجب أن استخدم تلك التطبيقات للتوثيق نقوم ستجد بعض الإجابات التي قد تفيدك.

متأكدًا من التطبيق أو التطبيقات الخاصة بالتوثيق الذي يجب استخدامه؟ نقدم بعض الأسئلة التوجيهية في البرنامج التعليمي الخاص بنا ، "هل يجب استخدام تطبيق الوثائق هذا؟".

قم بتحميل تطبيقات عادية

وجود القليل جدًا من البيانات وعدد قليل من التطبيقات المتخصصة على هاتفك قد يثير الشك. لجعل الجهاز يظهر كما لو كان هاتفًا عاديًا ، قم بتثبيت بعض التطبيقات اليومية الشائعة في المنطقة التي تقوم بتوثيقها، والتقط بعض الصور غير الضارة لكي تكون في معرضك.

بالنسبة لتطبيقات مواقع التواصل الاجتماعي ، قد ترغب في إنشاء حسابات بديلة وتسجيل الدخول إليها ، على الرغم من مراعاة أن الحسابات المزيفة تنتهك شروط الخدمة لمعظم المواقع، وقد يكون التحقق من تلك المواقع يصعب من إنشاء حسابات مزيفة. بالإضافة إلى ذلك ، ستحتاج إلى قضاء بعض الوقت في إنشاء محتوى وإضافة أصدقاء إليه ، مما قد يكون شاقًا.

تحميل التطبيقات أثناء حجب الانترنت

من المؤكد أن تحميل التطبيقات وتثبيتها دون الوصول إلى الإنترنت يمثل تحديًا. تحتاج إلى تنزيل التطبيقات مسبقًا إذا كنت تتوقع حدوث حجب للانترنت .

تتمثل إحدى الإستراتيجيات التي يمكن أن تساعدك أنت والآخرين لاحقًا في تنزيل وحفظ ملف apk.) Android Package) للتطبيق على مساحة تخزين هاتفك أو على آداة تخزين أخرى. يتيح وجود ملفات APK هذه في وضع عدم الاتصال لك أو للآخرين لمشاركة التطبيقات عندما لا يكون هناك إنترنت.

على الرغم من أننا لم تتح لنا الفرصة لتجربة هذه التجربة ، فإن تطبيق F-Droid يوفر واجهة لتبادل ملفات APK في وضع عدم الاتصال بالانترنت. هنا هو البرنامج التعليمي.

حافظ على كل معلومات الحساسة والخاصة بعيدا عن هذا الهاتف.

حاول تخصيص الجهاز للقيام بالوثائق. لا تستخدمه للبريد الإلكتروني أو المكالمات الهاتفية أو الرسائل مع جهات اتصال شخصية أو مع النشطاء، فقد تعرضهم وتعرض نفسك للخطر، ولا تقم بتوصيل هذا الجهاز بأي من حساباتك الأساسية الحقيقية.

استخدم المميزات الموجودة لإخفاء المحتوى

في حالة البحث في هاتفك ، قد يكون من المفيد جعل نواياك أقل وضوحًا أو يصعب العثور على المحتوى الخاص بك. تحسبا للمواقف التي سيتم فيها فحص هاتفك بشكل سطحي وسريع فقط ، يمكنك استخدام أساليب بسيطة مثل:

تغيير أسماء وأيكونات واختصارات التطبيق الخاص بك باستخدام تطبيق Launcher (مثل Nova Launcher ، ولكن هناك الكثير منها) فذلك يجعل بعض التطبيقات أقل وضوحًا وأكثر صراحةً.

- أيضاً قم باستخدام خاصية الـ Private Mode المتوفرة في هواتف سامسونج أو Content Lick المتوفرة في هواتف LG فهي تساعد كثيراً في الحفاظ على المعلومات في الأوقات الحرجة.
- وضع ملف فارغ باسم ".nomedia" داخل أي مجلد لمنع ظهور الوسائط في مجلد في معرض الصور الخاص بك. ملاحظة: إذا استمرت ظهور الوسائط ، فقد تحتاج إلى مسح ذاكرة التخزين المؤقت للمعرض. هذا قد لا يعمل باستمرار على جميع الأجهزة.

إنشاء مجلدات مخفية (المجلدات التي تبدأ بـ ".") باستخدام تطبيقات مدير الملفات File Manager App. يمكنك نقل الملفات إلى المجلد المخفي يدويًا ، أو إذا كنت تستخدم تطبيق كاميرا مثل Open Camera ، فيمكنك تحديد مكان تخزين hالملقات التي تسجلها. تأكد من إيقاف تشغيل خيار "إظهار الملفات المخفية" في إعداداتك حتى لا تكون الملفات المخفية مرئية.

- تقوم بعض تطبيقات التوثيق المتخصصة، مثل Tella أو Eyewitness to Atrocities ، بتخزين الوثائق في معارض منفصلة مشفرة يمكن الوصول إلى محتوياتها داخل التطبيق فقط ، مما قد يجعل الأمر أقل وضوحًا بالنسبة لشخص يبحث في هاتفك. تتطلب الوثائق الموجودة في هذه المعارض الآمنة رمز مرور تطبيق منفصل ، لذلك يبقى مشفرًا حتى إذا كان هاتفك غير مؤمّن.

<u>ملاحظة مهمة حول إخفاء المحتوى الخاص بك</u>

من المهم أن نلاحظ أن التقنيات المذكورة أعلاه قد تكون كافية للتخلص من شخص ما يقوم بسرعة بالبحث في هاتفك ، ولكنه لن يخفي المحتوى الخاص بك بشكل فعال عن شخص يبحث بالفعل ولديه وقت أطول.

ضع في اعتبارك أيضًا أن بعض الدول قد يكون لديها قوانين تقيد أو تجرم استخدام تطبيقات الأمان التي تشفر بياناتك أو تمسحها. قد يعتبر استخدامها لمنع السلطات من الوصول إلى بياناتك بمثابة تدمير للأدلة أو عرقلة التحقيق، وقد يعاقب عليها كجريمة.

<u>إعدادات المشاركة في وضع عدم الإتصال</u>

عندما لا يتوفر لديك فيها الإنترنت بعد التقاط المحتوى، لا يزال من الأفضل نقل الوثائق التي قمت بتوثيقها من هاتفك سواء كان لأسباب أمنية أو لتوفير مساحة أو لمشاركتها مع الآخرين. سيساعد أيضًا إلغاء تحميل المستندات بانتظام من هاتفك على تقليل المعلومات التي يتم اختراقها إلى الحد الأدنى في حالة مصادرة هاتفك وإلغاء قفله.

حتى إذا لم تتمكن من الاتصال بالإنترنت ، فلا يزال بإمكانك الاتصال بالأجهزة التي تدعم تقنية wifi أو الأجهزة التي تدعم تقنية Bluetooth بشكل محلي، مثل هاتف آخر أو USB محمول. يجب أن يأتي هاتفك عادةً مع تطبيق أو واجهة لتتمكن من الاتصال والنقل. إذا كان هاتفك يدعمه ، فيمكنك أيضًا توصيل محرك USB أو موصل OTG (On-The-Go) لنقل الوثائق إلى محرك OTG أو جهاز آخر.

تدرب ومارس قبل أن تكون في موقف أزمة

قم بإعداد الهاتف الآن إذا كان لديك اتصال بالإنترنت. ابدأ في ممارسة استخدام التطبيقات في المواقف اليومية (حيث لا توجد أية مخاوف أمنية) حتى تصبح متمرسا لها ولاستخدامها. اجعل أمان الهاتف الأساسي الجيد هو الممارسة الافتراضية. وبهذه الطريقة ، ستكون الطرق ذات طبيعة ثانية عندما تكون في موقف أزمة مع أشياء أخرى تقلقك.
(آكتشف التدوينة التالي في هذه السلسلة ، "هل يجب استخدام تطبيق الوثائق هذا؟
****

هل ينبغى أن أستخدم هذه التطبيقات للتوثيق؟

من سلسلة تدوينات التوثيق أثناء حجب الإنترنت

هذه التدوينة جزء من سلسلة التوثيق أثناء حجب الإنترنت، أيضاً سنقوم بإصدار بيان به مقارنة للعديد من تطبيقات التوثيق قريباً

بمشاركات من أرول باركاش

تمت مراجعته في *31* يناير *2020*

هناك العديد من التطبيقات التي يمكن أن يستخدمها الموثقين لتصوير الفيديو، بدءًا من تطبيق الكاميرا الأصلي لهاتفك، إلى تطبيقات أكثر تخصصا مثل ProofMood أو Tella أو Eyewitness to Atrocities.

تحتوي بعض التطبيقات على مميزات تعتمد على الاتصال بالإنترنت، لذلك ضع في اعتبارك أن هذه الميزات قد لا تكون متاحة في حالة حجب الانترنت أو إيقاف تشغيله.

لا يمكننا إخبارك إي تطبيق بيعنه هو الأنسب لك، حيث يعتمد ذلك على موقفك واحتياجاتك ومخاطرك . ولكن يمكن أن تساعدك هذه الأسئلة الإرشادية أدناه في تقييم التطبيق الأنسب لك.

من قام بصنع هذا التطبيق وهل أثق به؟

يجب أن تفكر دائمًا في مصدر أي تطبيق تقوم بتنزيله وتثبيته على جهازك، وما إذا كان بإمكانك الوثوق بالمطورين الذين قامو بتطويره أو لا حتى لا تتعرض بسببه للخطر ، عن قصد أو عن غير قصد.

بعض الأشياء التي يجب البحث عنها:

ما هي سمعة مطور التطبيق ماذا يقول الناس في مجتمعك عنهم وعن أدواتهم؟

هل مطور التطبيق ضعيف؟ فكر في سياقها ومدى احتمال إجبارهم على تسليم بياناتك أو الرضوخ للسلطات (أو ما إذا كانوا قد فعلوا ذلك بالفعل في الماضي). ما هي الدولة التي يتم تخزين البيانات فيها وما هي القوانين المتعلقة بأوامر المحكمة في تلك الدولة؟

هل يحافظ مطور التطبيق على التطبيق؟ ويحدثه باستمرار ويؤمن ثغراته؟ يمكنك الكشف عن ذلك من خلال صفحة التطبيق على سوق جوجل.

ما حجم مطور التطبيق ، وهل يبدو أنه سيكون بإمكانه الحفاظ على التطبيق مع مرور الوقت؟

هل التطبيق مفتوح المصدر؟ من الأرجح أن تعالج التطبيقات التي تكون مفتوحة للتدقيق أو يتم تحديدها على الأقل. هل المطور قام بتطوير التطبيق والتأكد من أمانه؟

ما هي الدوافع أو الحوافز التي تدفع عمل مطور التطبيق ، وكيف يمكن أن يؤثر ذلك على جدارته بالثقة؟ على سبيل المثال ، هل هي للربح أو برعاية ممول معين؟

على الرغم من عدم كونه مؤشرًا مباشرًا للثقة أو لا ، إلا أن تكلفة التطبيق قد تكون أحد الاعتبارات المهمة. تحتوي بعض التطبيقات على رسوم اشتراك شهرية عالية أو رسوم لكل فيديو.

حول اختيار التطبيقات للمزيد EFF (تحقق من دليل الدفاع عن النفس للمراقبة (؟؟؟

أين يمكن تحميل البرنامج؟

يجب عليك دائمًا تنزيل التطبيقات وتثبيتها فقط المتاجر الرسمية (متجر جوجل مثلا) أو مواقع الويب ذات السمعة الطيبة. حتى إذا كنت قد قمت بإجراء بحثًا شاملاً لتحديد مدى مصداقية أحد التطبيقات ، فإن التحميل من المواقع سيئة السمعة قد تضرك أو تؤدي بك إلى تنزيل مخادع غير شرعي تم إنشاؤه لأغراض ضارة. على سبيل المثال ، أصدرت مؤسسة الحقوق الرقمية SMEX في العام الماضي تحذيراً حول العديد من مواقع الويب التي تقوم بتسويق تطبيق يسمى "WhatsApp Plus" (للتوضيح ، هذا ليس WhatsApp!) ، مما قد يؤدي إلى حفظ بيانات المستخدمين وبيعها ، أو تجهيز الهواتف التي تثبيته ليتم اختراقها.

يوفر بعض مطوري البرامج الواعين للأمان تشفيرات تتيح لك التحقق من صحتها. سيقدمون عادة شرحًا لكيفية التحقق من هذه التشفيرات.

أين سيتم تخزين الداتا ؟

تخزن بعض التطبيقات بياناتك ووثائقك محليًا على جهازك فقط ، بينما يقوم البعض الآخر بإرسال بياناتك وتخزينها في مكان آخر. في كثير من الحالات ، يكون هذا متأصلًا في تصميم التطبيق والغرض منه ، مثل تطبيق Eyewitness to Atrocities ، الذي يرسل نسخة غير قابلة للتغيير من مستنداتك إلى مرفق تخزين Lexis Nexis حتى يتسنى لشاهد Eyewitness أن يشاهد المادة. لا يمكنك تصدير الوسائط الخاصة بك إلا من المعرض المشفر داخل تطبيق Eyewitness بعد.

الأمر متروك لك لتحديد ما إذا كنت بحاجة إلى الاحتفاظ بمستنداتك على جهازك فقط، أو ما إذا كنت بحاجة إلى إرسالها وتخزينها إلى موقع بعيد تتحكم فيه (كما هو الحال مع Tella) ، أو ما إذا كنت بحاجة لإرساله إلى خارج النظام الأساسي التي تسمح بالوصول إلى وثائقك واستخدامها. ضع في اعتبارك أنه أثناء إيقاف تشغيل الإنترنت، لن تتمكن من إرسال مستنداتك عبر الإنترنت على الفور ، لذلك ستحتاج إلى تطبيق تسطيع من خلاله مؤقتًا تخزين مستنداتك محليًا (راجع النسخ الاحتياطي للوسائط الهاتف دون الإنترنت أو الكمبيوتر).

إذا تم إرسال بياناتك إلى موقع بعيد ، فاحرص على تحديد البلدان التي ستتواجد بها البيانات. ما مدى تعرض البيانات للكشف في تلك البلدان ، سواء بأمر من المحكمة أو بوسائل أخرى؟ ما هي المخاطر التي من الممكن أن تواجهل من خلال كشف بياناتك؟

هل يقوم التطبيق بتشفير المادة الموثقة؟

توفر بعض التطبيقات ، مثل Tella و Eyewitness to Atrocities ، تشفير الملفات و / أو التخزين المشفر لوثائقك ، منفصلة عن معرض هاتفك الرئيسي وتشفير هاتفك ، بحيث لا يتم تشفير الوسائط والبيانات الوصفية على جهازك ما لم يتم الوصول إليها من خلال التطبيق مع رمز المرور. هذا يعني أنه حتى لو كان هاتفك غير مؤمّن ، فإن وثائقك تظل مشفرة. يمكن أن يوفر هذا مستوى إضافيًا من الحماية لمستنداتك.

إذا كان التطبيق يرسل ويخزن الوسائط الخاصة بك إلى موقع بعيد بعد عودة الاتصال بالإنترنت، ففكر أيضًا في ما إذا كنت بحاجة إلى تشفير الوسائط الخاصة بك أثناء النقل، كما يفعل تطبيق EyeWitness ، على سبيل المثال.

ضع في اعتبارك أنه على الرغم من أن التشفير قانوني في معظم البلدان، فقد يكون لدى البعض منهن قوانين تقيد استخدامه أو تجرّمه.

هل يقوم التطبيق بتخزين البيانات الوصفية (metadataa) أثناء عدم الاتصال بالإنترنت

البيانات الوصفية أو ال metadata هي بيانات تصف الفيديو أو الصورة ، مثل الوقت والتاريخ أو الموقع. تعتبر هذه المعلومات ذات قيمة لتحديد الفيديو أو الصورة وفهمها والمصادقة عليها والتحقق منها كوثائق لحدث معين. في سياق حجب الإنترنت ، تعد قدرة التطبيق على جمع بيانات وصفية معينة تلقائيًا و / أو السماح لك بإدخال معلومات وصفية مفيدة على الفور مفيدة بشكل خاص ، حيث قد تكون هناك فترة طويلة من الوقت قبل أن تتمكن من مشاركة الوثائق مع أي شخص (الوقت الذي يمكن فيه نسيان التفاصيل ، قد تتغير الظروف ، وما إلى ذلك).

تحتوي معظم تطبيقات الوثائق المتخصصة ، مثل ProofMode ، على ميزات بيانات وصفية محسّنة ، وتجمع بيانات وصفية أكثر من تطبيقات الكاميرا المضمنة النموذجية. قد تشمل البيانات الوصفية المحسّنة بيانات استشعار مختلفة ، وإشارات WiFi أو Bluetooth قريبة ، وبيانات الجهاز، والمعلومات التي يوفرها المستخدم ، وكل ذلك يمكن أن يسهل التأكد من مصداقية المادة والتحقق من الوسائط في وقت لاحق.

ضع في اعتبارك أنه أثناء إيقاف تشغيل الإنترنت، ستحتاج إلى تطبيق لا يتطلب إرسال البيانات من أجل إنشاء البيانات الأولية أو تسجيلها. قد تعتمد بعض التطبيقات على الإنترنت ، بدلاً من أجهزة استشعار الأجهزة ، لجمع بيانات تعريف معينة. على سبيل المثال قد تعكس البيانات التعريفية الموقع الأخير حيث كان الجهاز متصل بالانترنت، بدلاً من الموضع الفعلي للجهاز. يجب أن يسمح لك التطبيق أيضًا بتخزين البيانات الوصفية محليًا بدون الإنترنت ، بما في ذلك حفظ أي النماذج التي تملأها (على سبيل المثال ، "الوضع غير المتصل لـ Tella").

هل استطيع إخراج المادة من التطبيق؟

اعتمادًا على نواياك فيما يتعلق بالتوثيق والوثائق، قد يكون من الضروري أن تكون قادرًا على نقل وثائق الفيديو وبيانات التعريف الخاصة به من التطبيق ، بتنسيق لا يمتلكه التطبيق فقط لتتمكن أنت والآخرين من عرض المادة بدون الحاجه للتطبيق. ويمنحك مهلة أكبر في العمل مع المضي قدمًا في المحتوى. ضع في اعتبارك أن بعض البيانات الوصفية - *metadata* - قد لا تكون مفهومة.

لاحظ أن بعض التطبيقات قد يكون لديها حراسة مغلقة المتعمدة ولا تسمح للمستخدمين بنقل المادة أو إخراجها من التطبيق، بينما قد لا يتم تصميم بعض التطبيقات مع مراعاة إخراج المادة بالشكل المراد. عليك أيضًا أن تدرك أن بعض التطبيقات ، مثل *Eyewitness to Atrocities* ، قد لا تسمح لك بإخراج المادة حتى تقوم بتحميلها إلى خادم - سيرفر - *(*والتي تحتاج إلى الإتصال بالإنترنت للقيام بها*)* ، وقد تسمح لك بعض التطبيقات بتصدير الوسائط، ولكن ليس البيانات التعريفية *(*بخلاف البيانات التعريفية الموجودة في الملف نفسه*)*.

إذا كنت تحتاج إلى إخراج المادة، فمن الأفضل أن يسمح لك التطبيق بتصدير نسخة من الوسائط دون أي تغييرات أو تحويلات ونسخة من البيانات الوصفية - الـ *metadata* - بتنسيق نصي مقروء موحد. على سبيل المثال ، يتم تخزين بيانات *Tella* الوصفية في تشفير معرض *Tella* ، ولكن يمكن إخراجها بتنسيق *CSV*. بالإضافة إلى ذلك، أثناء عدم الاتصال الإنترنت، من الضروري وجود خيارات للنقل إلى التطبيقات غير المتصلة بالإنترنت أو الخدمات التي لا تعتمد على الإنترنت. تحتوي معظم التطبيقات التي تسمح لك بالتصدير على "زر" المشاركة الذي يقوم بتشغيل قائمة مشاركة، والتي يسجلها *Android* من قائمة من التطبيقات على هاتفك قادرة على التعامل مع هذا النوع من المحتوى. للأسف، يمكن لمطوري التطبيقات تخصيص قوائم مشاركتهم ولا يوجد تناسق بين التطبيقات.

أما إذا كانت كمية أكبر من الملفات، قد يكون الوصول إلى الملفات المخزنة أكثر فعالية من خلال تطبيق مدير الملفات ونسخ الملفات من هناك، على الرغم من أنك قد لا تتمكن من الوصول إلى البيانات الوصفية - الـ*metadata* - المخزنة في قاعدة بيانات التطبيق بهذه الطريقة. هذا الخيار غير متاح أيضًا للتطبيقات التي توفر معارض آمنة خاصة بها، حيث سيتم تشفير الملفات أثناء التخزين. وبالنسبة لهذه التطبيقات ، من الضروري وجود خيار للمشاركة داخل التطبيق.

اطلع على التدوينة التالية في هذه السلسلة ، "الحفاظ على الوسائط القابلة للتحقق أثناء إيقاف تشغيل الإنترنت" ومخططنا المقبل للوثائق
****

الحفاظ على المادة القابلة للإثبات أثناء حجب الانترنت

سلسلة تدوينات التوثيق أثناء حجب الانترنت

بواسطة إيفون ن ج
هذه التدوينة جزء من سلسلة تدوينات التوثيق أثناء الانترنت
بمشاركات من أرول باركاش
تمت مراجعته في 31 يناير 2020

غالبًا ما يعتمد المدافعون عن حقوق الإنسان والمحققون والباحثون والصحفيون على وثائق مباشرة يصورها شهود لمراقبة انتهاكات حقوق الإنسان والإبلاغ عنها ومعالجتها. لضمان أن عملهم ودفاعهم مبنى على معلومات صحيحة ، يتخذ هؤلاء المستخدمون خطوات لإثبات والتأكد الوثائق التي يتلقونها، وهي عملية يمكن أن تكون مضنية وتستغرق وقتًا طويلاً.

كموثق، هناك أشياء بسيطة يمكنك القيام بها لتسهل على الآخرين التحقق والتأكد من المادة التي قمت بتوثيقها، بحيث يمكن استخدامها بطرق فعالة وفي الوقت المناسب. تعتبر هذه الخطوات الإضافية القليلة أكثر قيمة أثناء حجب الإنترنت

مع مراعاة أن:

إذا لم تتمكن من البث المباشر ، فإن تاريخ النشر ومعلومات الموقع التي توفرها وسائل التواصل الاجتماعي ليست مفيدة لإظهار أنه تم تصوير الفيديو الخاص بك في أو قبل تاريخ معين أو في موقع معين.

إذا لم يتمكن الآخرون من التحميل، فقد يكون هناك عدد أقل من المواد المتاحة بشكل عام والتي يمكن استخدامها لتأكيد الفيديو الخاص بك.

إذا كنت بحاجة إلى تمرير الفيديو الخاص بك عبر العديد من الأيدي دون الاتصال بالإنترنت للوصول إلى وجهته ، فقد يكون من الصعب على الآخرين تتبع مصدر الفيديو.

إذا كنت بحاجة إلى حذف الفيديو الأصلي من هاتفك بسبب الأمان أو أن سعة التخزين محدودة مع عدم وجود نسخة احتياطية في -الكلاود - ، أو إذا كان عليك التخلص من الهاتف ، فقد يكون من الصعب تأكيد صحة الفيديو.

إذا نسيت تفاصيل مقطع فيديو معين والتطبيق الذي تستخدمه لا يلتقط / يسجل البيانات الوصفية الـ metadata دون الوصول إلى الإنترنت ، فقد لا يتمكن الآخرون من التعرف عليها لاحقًا.

يمكن أن تساعدك النصائح التالية في الحفاظ على مقطع الفيديو الخاص بك أثناء حجب الإنترنت لزيادة إمكانية التحقق منه وسهولة استخدامه كوثائق في وقت لاحق.

قم بتصوير أو توفير معلومات تعريفية في الفيديو

حاول تضمين التفاصيل في مقطع الفيديو الخاص بك مما يسهل على الباحث أو الصحفي تحديد الوقت والمكان لاحقًا، مثل المعالم الفريدة وعلامات الشوارع وواجهات المتاجر ولوحات الترخيص والأعلام والساعات والصفحات الأولى في الصحف وما إلى ذلك. يمكن أيضًا سرد المعلومات الأساسية مثل اسمك ومعلومات الاتصال الخاصة (إذا كان ذلك آمنًا) ، والوقت والتاريخ والموقع / إحداثيات GPS (أو الكتابة على قطعة من الورق وتصوير الورقة). كلما زادت التفاصيل التي تتضمنها سيكون من الأسهل على شخص آخر البحث عن الفيديو والتحقق منه لاحقًا، حتى لو لم يكن يعرفك أو من أين جاء الفيديو. راجع نصائحنا حول الممارسات الأساسية لالتقاط الصور وتخزينها ومشاركتها لمزيد من المعلومات.

قم بإضافة وصف أو بيانات وصفية - الـ metadata

استفد من أحد تطبيقات الوثائق المتخصصة العديدة التي تسحب بيانات التعريف المحسنة - الـ metadata - أو المعلومات الفنية من هاتفك، وتتيح لك إدخال معلومات وصفية إضافية يدويًا. ضع في اعتبارك أنك تحتاج ، أثناء حجب الانترنت إلى تطبيق لا يعتمد على الاتصال بالإنترنت لتسجيل أو تخزين بيانات التعريف هذه. تحقق من "هل ينبغي أن استخدم هذه التطبيقات للتوثيق؟" لمعرفة المزيد حول كيفية اختيار تطبيق مناسب.

بعض البيانات الوصفية التي يعرضها تطبيق Proofmode

حتى إذا كنت لا تستخدم تطبيق وثائق متخصص ، فلا يزال بإمكانك إنشاء معلومات تكميلية في شكل ملاحظات أو خرائط أو صور على هاتفك. يمكنك تنسيق الفيديو الخاص بك مع هذه المعلومات الإضافية باستخدام تطبيق مدير الملفات المفضل لديك. المعلومات التكميلية الرئيسية التي يجب تضمينها هي الوقت والتاريخ وموقع الحادث الذي تم تسجيله، وكذلك مصدر التسجيل (أي اسمك ومعلومات الاتصال) إذا كان من الآمن تضمينها. قم بإخراج البيانات التعريفية وقم بتضمينها مع الفيديو (يمكنك وضعها في مجلد ثم ضغطها) عند مشاركتها مع الآخرين.

فيديو مع معلومات إضافية في ملفات آخرى

تأكد من وجود نسخة احتياطية

يمكنك إجراء نسخة احتياطية للوسائط من هاتفك بانتظام ، ومن الناحية المثالية في جهازين منفصلين. يمكنك ، على سبيل المثال ، توصيل On-the-Go (OTG) أو أقراص تخزين، حتى بدون وجود جهاز كمبيوتر. ستضمن النسخ الاحتياطي احتفاظك بنسخة من الفيديو الخاص بك في حالة فقد هاتفك أو كسره ، أو إذا كنت تحتاج إلى حذف مقاطع الفيديو من هاتفك. إن امتلاك نسخة آمنة من الفيديو الأصلي الخاص بك يُمكّن أيضًا المحقق أو الصحفي الذي يرى الفيديو الخاص بك من الحصول على الفيديو منك مباشرةً في وقت لاحق، مما يؤدي إلى إنشاء أقصر وأكثر سلسلة كاملة من الملكية للمادة الموثقة.

قم بنسخ الوسائط احتياطيًا من هاتفك ، كما هو الحال مع محرك أقراص OTG أو وحدة التخزين اللاسلكية.
أتطلع على التدوينة التالية في هذه السلسلة ، النسخ الاحتياطية بدون الاتصال بالانترنت".

****

النسخ الاحتياطي للمواد الموجودة على التليفون بدون أنترنت أو كمبيوتر من سلسلة تدوينات التوثيق أثناء حجب الانترنت

بواسطة أيفون ن ج

بمشاركات من أرول باركاش

تمت مراجعته في 31 يناير 2020

النسخ الاحتياطي هو المفتاح لضمان عدم فقد المواد التي قمت بتصويرها أو أي بيانات آخرى سواء عن طريق الخطأ أو إذا تمت مصادرة جهازك. أثناء حجب الانترنت قد لا تتمكن من تشغيل النسخة الاحتياطية السحابية - The Cloud - العادية أو إرسال المستندات الخاصة بك إلى موقع آمن خارج موقعك. يعتبر التحميل على كمبيوتر أو لابتوب إحدى طرق النسخ الاحتياطي، ولكن نظرًا لأن الأشخاص غالبًا ما لا يستطيعون الوصول إلى أحد هذه الخيارات في كل الأوقات فإليك بعض الخيارات والنصائح الخاصة بنسخ الوسائط والوثائق الخاصة بك احتياطيًا من هاتفك أثناء إيقاف تشغيل الإنترنت بدون جهاز كمبيوتر.

استخدم محرك OTG أو محرك لاسلكي

OTG هي اختصار لجملة معناها - اثناء الحركة وهي عبارة نوعا من أقراص الـ USB المتوافقة مع العديد من أجهزة Android (ولكن ليس كلها). يمكنك توصيل محرك أقراص الإبهام OTG مباشرة في هاتفك ، أو استخدام محول OTG إلى USB لتوصيل هاتفك بمحرك أقراص USB ثابت عادي.

تشمل العلامات التجارية الشهيرة لمحركات SanDisk OTG و Kingston و Samsung ، على الرغم من أن هناك العديد من المنتجات الأخرى. عادة ما تتراوح تكلفتها بين 8 دولارات و 25 دولارًا أمريكيًا حسب سعة التخزين.

استخدم محرك OTG لإجراء نسخ احتياطي للوسائط من الهاتف.

تشبه محركات الأقراص الثابتة ولكنها لاسلكية ولا تحتاج إلى كابل محركات الأقراص الثابتة العادية فيما عدا أنها لا تتطلب كابلات. يتيح لك هذا توصيل الأجهزة التي لا تتصل عادة بالأقراص الصلبة مثل هاتفك. تتمثل ميزة محرك الأقراص اللاسلكي عبر محرك OTG في أنه يمكنك توصيل عدة مستخدمين بنفس محرك الأقراص اللاسلكي في نفس الوقت. قد يكون ذلك مفيدًا في بعض الأوقات على سبيل المثال في حالة الاحتجاج أو المظاهرات عندما تقوم بالتصوير كفريق واحد - يمكن نسخ مقاطع الجميع احتياطيًا على محرك أقراص ثابت يحمله عضو آخر في الفريق. لاحظ أنه نظرًا لعدم استخلاص الطاقة من أي جهاز ، تعتمد محركات الأقراص اللاسلكية على طاقة البطارية وتحتاج إلى الشحن.

SanDisk هي على الأرجح العلامة التجارية الأكثر شعبية لوحدات التخزين اللاسلكية ، على الرغم من وجود غيرها. تعد محركات الإبهام اللاسلكية أغلى من محركات OTG ، وتتراوح ما بين 25 إلى 100 دولار أمريكي تقريبًا حسب سعة التخزين. تبدأ محركات الأقراص الصلبة الخارجية اللاسلكية الأكبر بحوالي 150 دولارًا أمريكيًا حسب سعة التخزين.

الهاتف والتخزين عبر الـ wifi
استخدم محرك أقراص الإبهام اللاسلكي لنسخ الوسائط والمواد احتياطيًا من الهاتف
بديل : يمكنك استخدام هاتف قديم أو غير مستخدم

إذا لم يكن لديك محرك OTG أو محرك لاسلكي ، ولكن لديك هاتفًا قديمًا لا يزال يعمل ولم تعد تستخدمه ، يمكنك أيضًا إعادة استخدامه للنسخ الاحتياطي. طالما أن كلا الهاتفين قريبين من بعض، يمكنك توصيل ونسخ الوسائط من واحد إلى الآخر باستخدام Bluetooth أو WiFi Direct أو Near Field Communication (NFC) / Android Beam. تعد كل من Bluetooth و Wifi Direct من التقنيات اللاسلكية التي يمكنها "إقران" جهازين بدون الحاجه لجهاز ثالث أو نقطة وصول أخرى بينهما. يوفر WiFi Direct نطاقًا أوسع ونقلًا أسرع للبيانات من تقنية Bluetooth ، ولكنه يستهلك طاقة أكبر بكثير. وفي الوقت نفسه ، يحتوي NFC على نطاق أقصر بكثير (حوالي 4 سم) وسرعات نقل أبطأ بكثير من تقنية Bluetooth أو WiFi Direct ، ولكنه يتصل بشكل أسرع ويستخدم طاقة أقل ، لذلك يمكن أن يكون مفيدًا لعمليات النقل الصغيرة السريعة عندما يكون لديك كلا الجهازين سهل الوصول إليهم.

قد يحتوي هاتفك على تطبيقات أو مميزات مثل WiFi direct مدمجة تسمح لك باختيار الأجهزة القريبة للإقتران بها أو لمشاركة الملفات معها. إذا كان كلا الهاتفين مثبتين بواسطة Files Google ، فيمكنك أيضًا مشاركة الملفات في وضع عدم الاتصال بالانترنت باستخدام هذه التقنيات في التطبيق.
اثنين من الهواتف باستخدام الملفات لتبادل الملفات

إرسال الملفات دون اتصال عبر Files من Google.

هام: الجانب السلبي لسهولة الاتصال التي توفرها هذه الخدمات هو أنها غير آمنة تماما. يمكن استخدام إشارات Bluetooth وواي فاي لتتبع موقعك أو استكشاف جهازك للحصول على معلومات. قد يحاول المتسللون الاقتران بجهازك، أو يرسلون إليك الملفات غير المرغوب فيها، أو حتى يسيطروا على جهازك إذا كان ضعيفًا. لكي تكون أكثر أمانًا ، قم بإيقاف تشغيل هذه الخدمات عندما لا تستخدمها وقم بتشغيلها فقط عندما تكون في أماكن آمنة، وقصر أذونات التطبيق على ما تحتاج إليه التطبيقات فقط، وتمارس أمانًا جيدًا على الهاتف مثل تشغيل التحديثات والحصول على خدمة قوية رمز عبور.
قم بتضمين أي وصف / بيانات وصفية الـ metadata منفصلة

عند نسخ الوسائط إلى محرك OTG أو محرك أقراص لاسلكي أو هاتف قديم ، من المفيد تضمين أي معلومات وصفية أو بيانات وصفية الـ metadata قد تكون منفصلة عن الوسائط. تقوم العديد من تطبيقات الوثائق ، على سبيل المثال ، بإنشاء مستندات نصية بتنسيق CSV أو JSON تتضمن بيانات وصفية تم سحبها من الجهاز (مثل تحديد الموقع الجغرافي والوقت والتاريخ) وأي وصف أدخله المستخدم يدويًا. تأكد من نقل مستندات البيانات الأولية هذه وإدراجها في النسخ الاحتياطية أيضًا.
ملفات البيانات الوصفية metadata على الهاتف
ملفات بيانات تعريف إضافية تم إنشاؤها باستخدام تطبيق ProofMode.
كلمة السر حماية وحدات التخزين

يمكن أن تكون العديد من وحدات التخزين اللاسلكية محمية بكلمة مرور من خلال تطبيق جوال يأتي مع وحدة التخزين. لاحظ أن حماية كلمة المرور ليست هي نفسها التشفير (لا تعمل معظم محركات الأقراص اللاسلكية أو محركات OTG على تمكين تشفير وحدة التخزين بالكامل باستخدام هاتف محمول فقط، على الرغم من أنه قد يتم تشفيرها بالكامل باستخدام الكمبيوتر.
كلمة السر حماية محركات الأقراص الخاصة بك.

إذا كنت بحاجة إلى تخزين ملفاتك بشكل أكثر أمانًا ، فقد تفكر في تشفير النسخ الاحتياطية. بينما قد لا تتمكن من تشفير معظم وحدات التخزين اللاسلكية أو OTG بهاتف محمول ، يمكنك تشفير الملفات بنفسها قبل نقلها إلى وحدة التخزين. بعض التطبيقات التي يمكنها تشفير الملفات على Android تشمل ZArchiver و RAR. كن على علم بأنه يجب عليك تذكر كلمات مرور التشفير الخاصة بك. لا توجد وسيلة لاستعادة الملفات المشفرة إذا فقدت كلمة المرور.

التشفير عن طريق تطبيق ZIP
ضغط وتشفير الملفات باستخدام ZArchiver على الهاتف قبل الانتقال إلى النسخ الاحتياطي.

ضع في اعتبارك أن بعض البلدان قد يكون لديها قوانين تقيد أو تجرم استخدام التشفير. قد يعتبر استخدامها لمنع السلطات من الوصول إلى بياناتك بمثابة تدمير للأدلة أو عرقلة التحقيق ، وقد يعاقب عليها كجريمة.

عمل نسخ احتياطية 2 في مواقع منفصلة.

نسخة احتياطية واحدة ليست دائما كافية. على سبيل المثال ، قد تفقد جهاز النسخ الاحتياطي أو تتلفه أو قد يتوقف عمله بشكل عشوائي. ينصح خبراء تقنية المعلومات عادة بالحصول على نسختين احتياطيتين (ليصبح الإجمالي 3 نسخ بالنسخة الاصلية) ، على أجهزة منفصلة محفوظة في مواقع منفصلة. هذا يساعد في تخفيف مجموعة متنوعة من المخاطر على أي نسخة معينة.

أطلع على التدوينة الأخيرة في هذه السلسلة ، "مشاركة الملفات والاتصالات أثناء حجب الإنترنت".

****

مشاركة الملفات والتواصل أثناء حجب الانترنت

سلسلة تدوينات التوثيق أثناء حجب الانترنت

بواسطة إيفون ن ج

هذه التدوينة جزء من سلسلة تدوينات التوثيق أثناء حجب الانترنت
بمشاركات من أرول باركاش
تمت مراجعته في 31 يناير 2020

كان لحجب الإنترنت المتواصل والقمع في كشمير والذي يعتبر أطول إغلاق للإنترنت تم فرضه على الإطلاق في ظل نظام ديمقراطي ، تأثير كارثي على حياة الناس في المنطقة ,مما زاد الطين بلة أنه في ديسمبر *2019* ، تم إلغاء حسابات *WhatsApp* من كشمير بسبب *120* يومًا من عدم نشاط المستخدمين وفقًا لسياسات *WhatsApp*.

في وقت كتابة هذا التقرير في يناير 2020 ، قضت المحكمة العليا الهندية بأن الإغلاق غير المحدد في كشمير غير قانوني واعتبرته إساءة استخدام للسلطة. تمت عودة الانترنت في بعض المناطق، ولكن فقط مواقع معينة كانت متاحة للتصفح.

تم تصميم عمليات إيقاف الإنترنت لمنع الأشخاص من مشاركة المعلومات والتواصل (وكذلك دفع الأشخاص إلى أشكال اتصال أقل أمانًا مثل الهاتف المحمول والرسائل النصية القصيرة ، والتي يسهل على السلطات اعتراضها ومراقبتها). لا توجد دائمًا حلول جيدة أثناء حجب الانترنت الكامل. على سبيل المثال خلال أقسى فترات الإغلاق في كشمير لجأ الناس إلى استخدام الخطابات المكتوبة بخط اليد والسعاة لتوصيل الرسائل إلى أحبائهم.

ليست لدينا طرق مؤكدة للتحايل على جميع العوائق ، ولكن من خلال المحادثات مع النشطاء والأصدقاء، تعلمنا بعض الأساليب والمناهج الخاصة بالمشاركة والتواصل أثناء حجب بالإنترنت والتي قد تفيدك، وفقًا للظروف. لاحظ أن بعض هذه الخيارات تتطلب إعداد الإنترنت مبدئيًا (على سبيل المثال لتنزيل التطبيقات ، إلخ)..

مشاركة الملفات مباشرة مع Bluetooth أو Wifi Direct أو NFC

لا تحتاج إلى اتصال بالإنترنت لتوصيل هاتفك بجهاز آخر قريب عبر Bluetooth أو Wifi Direct أو Near Field Communication (NFC) (تسمى أحيانًا Android Beam على الأجهزة القديمة). تعد كل من Bluetooth و Wifi Direct كلاهما من التقنيات اللاسلكية التي يمكنها "إقران" جهازين بدون جهاز توجيه أو نقطة وصول أخرى بينهما.

يوفر WiFi Direct نطاقًا أوسع ونقلًا أسرع للبيانات من تقنية Bluetooth ، ولكنه يستهلك طاقة أكبر بكثير. وفي الوقت نفسه ، يحتوي NFC على نطاق أقصر بكثير (حوالي 4 سم) وسرعات نقل أبطأ بكثير من تقنية Bluetooth أو WiFi Direct ، ولكنه يتصل بشكل أسرع ويستخدم طاقة أقل ، لذلك يمكن أن يكون مفيدًا لعمليات النقل الصغيرة عندما يكون الجهازان في يديك.

ميزات Bluetooth المدمجة و WiFi Direct و Android Beam

من المحتمل أن يكون لديك ميزات Bluetooth و WiFi Direct و NFC مضمنة في هاتفك والتي تظهر في خيارات المشاركة. بالإضافة إلى ذلك ، فإن التطبيقات التي تحتوي على مشاركة الملفات ، مثل Files By Google ، تدمج هذه التقنيات أيضًا.

مشاركة دون اتصال في ملفات Google

هام: الجانب السلبي لسهولة الاتصال التي توفرها هذه الخدمات هو أنها غير آمنة. يمكن استخدام إشارات Bluetooth أو Wifiلتتبع موقعك أو استكشاف جهازك للحصول على معلومات. قد يحاول المتسللون الاقتران بجهازك ، أو يرسلون إليك الملفات غير المرغوب فيها ، أو حتى يسيطروا على جهازك إذا كان ضعيفًا. لكي تكون أكثر أمانًا ، قم بإيقاف تشغيل هذه الخدمات عندما لا تستخدمها وقم بتشغيلها فقط عندما تكون في أماكن آمنة ، وقم بتحديد أذونات التطبيق إلى ا تحتاج إليه فقط ، وفعل وسائل الأمان جيدًا على الهاتف مثل تنزيل التحديثات وتفعيل كلمة سر قوية للهاتف.

مشاركة الملفات مع وحدات التخزين اللاسلكية أو عبر شبكة محلية لاسلكية (WLAN)

يمكن استخدام وحدات التخزين الثابتة اللاسلكي أو وحدات التخزين المتحركة لمشاركة الملفات بين مجموعة من الأشخاص في وقت واحد. عادة ما يأتي وحدة تخزين wifi مع إرشادات أو تطبيق لتوصيل هاتفك لوحدة التخزين، وهو سهل الاستخدام نسبيًا. تذكر اختيار كلمة مرور على وحدة التخزين لزيادة الأمان.

إذا لم يكن لديك وحدة تخزين لاسلكية، يمكنك أيضًا مشاركة الملفات على محرك أقراص USB عادي عن طريق توصيله بموجه لاسلكي. ويعد جهاز التوجيه اللاسلكي - الراوتار - المزود بمنفذ USB غير مكلف نسبيًا وسهل الحركة. يمكن للمستخدمين الاتصال بمحرك وحدات USB عبر شبكة محلية - WLAN - (لا تحتاج إلى الإنترنت). للوصول إلى الملفات الموجودة على وحدات USB المتصل على هاتفك ستحتاج إلى استخدام تطبيق مدير الملفات الذي يمكنه الاتصال بالتخزين الشبكي الجماعي ، مثل Solid Explorer. يمكن العثور عادةً على عنوان IP لجهاز التوجيه الخاص بك في إعدادات wifi المتقدمة لهاتفك.

استخدم تطبيق مدير الملفات (Solid Explorer الموضح هنا) للاتصال بالشبكة على هاتفك.

وفي الوقت نفسه ، هناك خيار آخر هو PirateBox ، وهو خيار جيد لأنه يوفر برامج مرخصة مجانًا. يمكن للمستخدمين مشاركة الملفات كما أوضحنا، ولكن Piratebox يتيح لهم القيام بذلك بشكل مجهول ، ويشمل أيضًا ميزات الدردشة والرسائل. يتطلب إعداد Piratebox تنزيل بعض البرامج وتثبيتها وإعدادها. التعليمات موجودة على موقع Piratebox.

تحديث : مشروع Pirate Box يغلق ببطء. لا يزال موقع الويب ومستودع Github متصلين بالإنترنت ، لكن المطور الرئيسي للمشروع لم يعد يقوم بصيانتهما بشكل فعال.

التواصل عبر الدردشة من نظير إلى نظير

تطبيقان جديدان لتراسل الرسائل من نظير إلى نظير أصبحنا على علم بهما من خلال شبكات الناشطين هما Briar و Bridgefy. لم نجربهم بعد ، لكننا نعرف من يقومون بتجربتهم..

Briar عبارة عن تطبيق مراسلة مشفر مفتوح المصدر لا يعتمد على خادم مركزي ، ولكن بدلاً من ذلك تتم مزامنة الرسائل بين أجهزة المستخدمين (لذلك المحتوى يعيش على جهاز كل مستخدم). يمكنه المزامنة حتى في حالة عدم وجود إنترنت باستخدام Bluetooth أو WiFi (عندما يكون هناك إنترنت ، يقوم التطبيق بمزامنة الأجهزة عبر شبكة Tor). يضم Briar أيضًا مجموعات خاصة ومنتديات عامة ومدونات. عند استخدامه أثناء عدم الاتصال بالانترنت، يقتصر نطاقك على نطاق Bluetooth أو WiFi (بحد أقصى 100 متر).

في هذه الأثناء ، يعتبر Bridgefy تطبيق مراسلة مشفّر (باستثناء عند استخدام ميزة "الرسائل الجماعية") يستخدم Bluetooth لإرسال الرسائل. على عكس Briar ، يمكن للرسائل أن تنقل مسافات أطول من خلال التنقل عبر شبكة من مستخدمي Bridgefy الآخرين (فقط المستلم المقصود يمكنه قراءة الرسالة). يفتقر Bridgefy إلى مجموعات Briar الخاصة والمنتديات والمدونة ، لكن لديه وضع البث الذي يمكنك من خلاله إرسال رسالة إلى ما يصل إلى 7 من مستخدمي Bridgefy ضمن النطاق ، والذين لا يحتاجون إلى أن يكونوا جهات اتصالك (ليست بالضرورة أن تكون الرسائل الجماعية بالضرورة مشفرة).

التواصل عبر الرسائل النصية المشفرة

يتم إرسال الرسائل النصية القصيرة عبر الشبكات الخلوية ولا تعتمد على الإنترنت ، لذلك قد لا تزال تعمل أثناء إيقاف تشغيل الإنترنت. ومع ذلك ، تعتبر الرسائل القصيرة غير آمنة للغاية. على عكس التطبيقات المعتمدة على الإنترنت مثل WhatsApp أو Signal ، لا يتم تشفير الرسائل القصيرة من طرف إلى طرف. هذا يعني أنه يمكن للحكومات وشركات المحمول قراءة الرسائل النصية (وبياناتها الوصفية) أو اعتراضها من قراصنة الإنترنت. يمكن أيضًا أن تكون الرسائل النصية القصيرة "مزيفة" ، بمعنى أنه يمكن للمرسل معالجة معلومات عنوانه لانتحال هوية مستخدم آخر.

إذا كنت بحاجة إلى استخدام SMS ، فإن Silence هو تطبيق يقوم بتشفير الرسائل النصية من طرف إلى طرف. إنه مفتوح المصدر ويستخدم بروتوكول تشفير الإشارة. بينما لم نجربها بأنفسنا ، فقد سمعنا أن الآخرين قد استخدموها. يحتاج كل من المرسل والمستلم إلى تثبيته وتبادل المفاتيح مع بعضهما البعض. نظرًا لأن الرسائل النصية القصيرة تمر عبر خوادم الاتصالات الخاصة بك ، حتى مع وجود Silence ، فأنت تقوم بإرسال رسالة مشفرة والبيانات الوصفية حول رسالتك إلى شركة الاتصالات.

الحجب الجزئي للانترنت: تطويق المواقع المحجوبة

غالبًا ما لا يعني "حجب الإنترنت" حجب الإنترنت بالكامل ، بل منع الوصول إلى مواقع ويب معينة أو منصات وسائط التواصل الاجتماعي. يمكن للحكومات ، عبر مزودي خدمة الإنترنت (ISP) ، حظر المواقع استنادًا إلى عنوان IP أو المحتوى أو عبر عمليات البحث عن DNS. غير متأكد إذا تم حظر موقع؟ تقوم منظمات مثل Open Observatory of Network Interference و Netblocks بمراقبة وقياس اضطرابات الإنترنت والرقابة في جميع أنحاء العالم.

لحسن الحظ طالما لديك إمكانية الوصول إلى الإنترنت ، فهناك بعض الطرق لمحاولة الالتفاف على القطع الجزئية. كما هو الحال مع التشفير ضع في اعتبارك أن التحايل على المواقع المحجوبة قد يكون تم تجريمه في بلدك.

VPN

تتمثل إحدى الطرق لتجاوز الحجب القائم على حجب الـ IP أو القائم على المحتوى في استخدام شبكة افتراضية خاصة أو VPN ، مثل ProtonVPN أو TunnelBear. عند الاتصال عبر VPN ، يتم تشفير حركة المرور على الإنترنت وتوجيهها عبر خادم VPN في موقع آخر ، كما هو الحال في بلد آخر ، وبالتالي إخفاء الوجهة الحقيقية ومحتوى حركة المرور الخاصة بك إلى مزود خدمة الإنترنت الخاص بك.

ضع في اعتبارك أن بعض الحكومات تحظر استخدام VPN أو قد تحاول اكتشاف اتصالات VPN وحظرها. من المهم أيضًا استخدام موفر VPN موثوق ، ويفضل أن لا يقوم بتخزين البيانات أو السجلات ، لأن مزود الخدمة سيكون قادرًا على رؤية نشاطك على الإنترنت. كن على دراية بالبلد الذي يوجد به موفر VPN ، والعمليات القانونية التي قد يخضعون لها بناءً على قوانينهم. ضع في اعتبارك أيضًا أن شبكات VPN المعتمدة من الحكومة قد تمكن بالفعل من مراقبة وفحص بياناتك.

خوادم DNS

تعمل خوادم DNS عن طريق ترجمة أسماء النطاقات أو عناوين URL التي يكتبها المستخدم إلى مستعرض إلى عناوين IP الرقمية التي يستخدمها الإنترنت لتحديد صفحات الويب. يمكن لمزود خدمة الإنترنت تعديل خوادم DNS التي يتحكم فيها لحظر بعض المواقع، أو لإرجاع صفحة غير صحيحة تفيد بأن الموقع غير موجود. في عام 2014 ، حاول رئيس الوزراء التركي رجب طيب أردوغان منع تويتر أثناء الانتخابات التركية باستخدام هذه التقنية. لقد تم إحباط الحظر بسرعة من قبل النشطاء الذين شاركوا نصائح خطوة بخطوة حول كيفية استخدام VPN وتغيير خوادم DNS.

يمكنك تغيير خادم DNS الافتراضي في شبكة الهاتف أو إعدادات wifi. بدلاً من خادم DNS الافتراضي ، يمكنك استخدام خوادم DNS البديلة مثل Google Public DNS أو CloudFlare للالتفاف على الكتل المستندة إلى DNS. لدى Cloudflare أيضًا تطبيق يسمى 1.1.1.1 والذي يسمح للمستخدمين بالتبديل إلى خادم Cloudflare DNS من خلال واجهة تطبيق بسيطة.

هذه طريقتان فقط للتحايل على أكثر تقنيات الحجب شيوعًا. راجع أدلة مفيدة من Internet Society و Access Now و Security-in-a-Box و EFF لمزيد من المعلومات المتعمقة.