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.