المقدمة

من المفاهيم الخاطئة الشائعة أنه لا يمكنك منع الحكومة من التجسس عليك, بل تستطيع. لا تدع الخوف من القمع الحكومي يمنعك من التعبير عن آرائك. تم تصميم مجموعة أدوات خصوصية "رتسر" لمساعدتك في الحفاظ على سلامتك واعلامك.

كيف يعمل الإنترنت

تحتوي جميع أجهزة الكمبيوتر على الإنترنت على عنوان ال IP تستخدمه للتواصل مع بعضها البعض. تحتوي مواقع الويب أيضًا على عناوين ال IP ، ولكن لتسهيل تصفح الإنترنت ، لديها أيضًا أسماء نطاقات (مثل www.facebook.com او www.google.com) مرتبطة بعناوين IP الخاصة بها. عندما يريد جهاز الكمبيوتر الخاص بك بالانتقال إلى www.google.com لإجراء بحث ، فإنه يحصل على عنوان ال IP المرتبط به ويتصل بهذا الكمبيوتر للحصول على البيانات، وفي هذا المثال, نتائج بحث Google.

مزود خدمة الإنترنت الخاص بك هو ما يربط جهاز الكمبيوتر الخاص بك بالإنترنت. من المحتمل أن يكون لديك مودم متصل بشبكة مزود خدمة الإنترنت باستخدام الهاتف أو التلفزيون أو كابل الألياف البصرية. نظرًا لأن الإنترنت الخاص بك يمر عبر بنيتهم التحتية ، يمكنهم رؤية جميع البيانات التي تنقلها وعناوين ال IP التي ترسل إليها المعلومات.

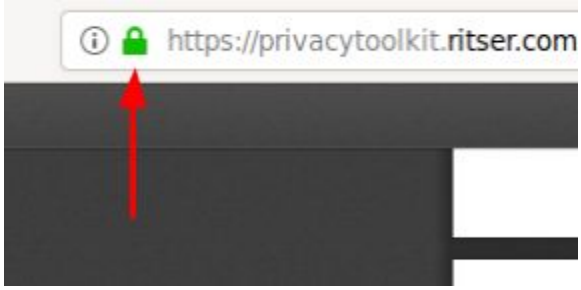
لكن هذا لا يعني أنه يجب عليهم معرفة صفحات الويب التي تزورها, إذا قمت بتشفير بياناتك باستخدام HTTPS أو Tor ، فلن يروا ما تقوم بفعله عبر الأنترنت، بما في هذا العنوان (www.google.com/search?q=news), سيعلمون عنوان ال IP الذي تتصل به ، ووقت الاتصال ، وحجم البيانات المشفرة التي ترسلها.

ماذا بامكان الحكومة ان تقوم بالتتبع بالفعل؟

لنراجع ماذا تتمكن الحكومة أو مزود خدمة الانترنت بالتتبع, بالافتراض ان كنت تستعمل HTTPS وليس Tor, تتمكن حكومتك بتتبع مواقع الويب ومتى, هذا يعني انهم سيكونون قادرين على معرفة زيارتك لموقع (www.facebook.com) في 7:30م, لكنهم لن يعرفوا الصفحات او الملفات الشخصية التي قمت بزيارتها, سيعلمون فقط أنك زرت (www.facebook.com).

اذا لم تقم باستعمال HTTPS, ستتمكن حكومتك أيضا من تتبع ما ترسله الى موقع الويب, ويتضمن ذلك كلمات المرور وعناوين ال URL.

كيف تعرف أنك تستخدم HTTPS؟. عادةً، سيعرض متصفح الانترنت الخاص بك رمز قفل كما هو موضح أدناه عندما تتصفح باستخدام HTTPS.



يعمل HTTPS عن طريق تشفير البيانات بين متصفح الانترنت الخاص بك وموقع الويب الذي تقوم بألوصول اليه. هذا يعني أنه يستخدم خوارزميات رياضية للتأكد من أن هذه البيانات غير قابلة للقراءة أثناء نقلها. تعتبر خوارزميات التشفير الحديثة آمنة ، حتى أن أقوى وكالات الاستخبارات غير قادرة على كسرها.

تبدو الاتصالات غير المشفرة (HTTP بدون S) كما يلي:

من: 70.210.154.182

إلى: 103.190.246.203 (baidu.com)

الوقت: 4:42 م 02-09-2020

بيانات (70 بايت):

صفحة الويب التي تمت زيارتها: baidu.com/account

اسم المستخدم: alex2

كلمة المرور: password

تبدو الاتصالات المشفرة (HTTPS) كما يلي:

من: 70.210.154.182

إلى: 103.190.246.203 (baidu.com)

الوقت: 4:42 م 02-09-2020

بيانات (68 بايت):

o866)F(Yu~1]TEjP47h6(vIEs!dq_'|/Sl^ZMbFriN_"LejUyUYZ%d?sRx;F##Coq9M&

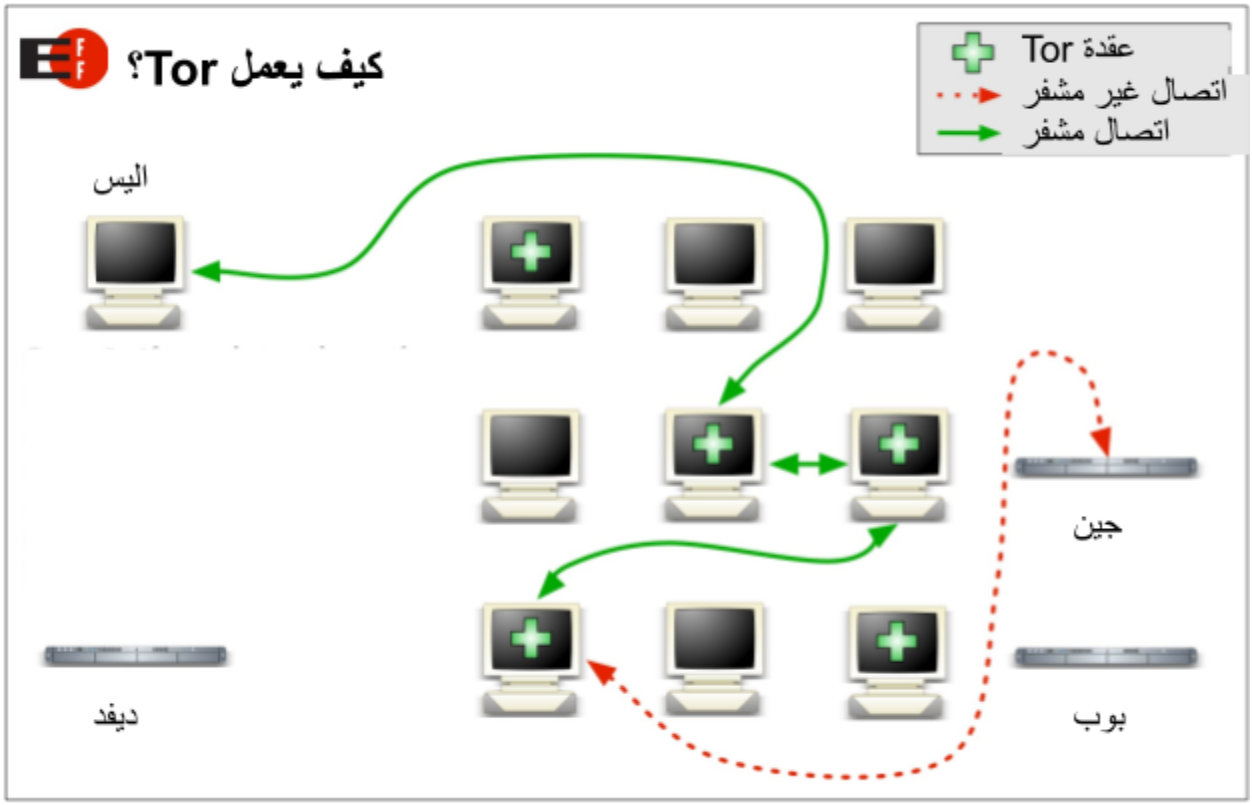
ما يمكن للحكومة تتبعه بمساعدة أصحاب المواقع الإلكترونية

ومع ذلك ، **لا** يمنع HTTPS موقع الويب من إعطاء بياناتك إلى الشرطة. يمكن لكل موقع ويب تقوم بالوصول إليه على الإنترنت رؤية عنوان ال IP الخاص بك. إذا قرر أحد مواقع الويب منح الحكومة عنوان ال IP خلف حسابك ، **فيمكنهم استخدامه للعثور على عنوانك الحقيقي**. من المهم التأكد من عدم تمكن السلطات من العثور على عنوان ال IP وراء حساباتك على الإنترنت.

مواقع الويب الكبيرة مثل Facebook و Reddit و Google لديها إجراءات مطبقة للتعامل مع الطلبات الحكومية لبيانات المستخدم. عادة ما تكون هذه العملية شفافة وعادلة إلى حد ما ، لأنها تتجاهل عمومًا قوانين الحكومات الاستبدادية. Google، على سبيل المثال ، عالجت 3 طلبات بيانات مستخدمين مصريين بين عامي 2014 و 2018. لقد رفضوها جميعها.

كيفية إخفاء هويتك عن المواقع الإلكترونية

ومع ذلك ، ليس من الذكاء أن تضع سلامتك في أيدي شركات متعددة الجنسيات الهادفة للربح. إذا كنت تعيش في بلد تكون سلامتك فيه معرضة للخطر إذا تم الكشف عن هويتك، فمن الجيد استخدام Tor (المتضمنة في مجموعة الأدوات هذه). يخفي Tor عنوان ال IP الخاص بك عن طريق إرسال حركة المرور على الإنترنت من خلال أجهزة كمبيوتر أخرى قبل أن يصل إلى موقع الويب. سيتمكن موقع الويب من رؤية عنوان ال IP الخاص بآخر جهاز كمبيوتر بدلاً من عنوان ال IP الخاص بك. ستعرف حكومتك أنك تستعمل Tor ، لكنها لن تعرف ما الذي ترسله من خلاله أو مع من تتواصل.



فائدة أخرى لاستخدام Tor هي أنه نظرًا لأن مزود خدمة الإنترنت لا يعرف مواقع الويب التي تقوم بالوصول إليها ، فلا يمكنه حظرها.

تور ليس معصومًا عن الخطأ. إذا كانت الحكومة تعرف موقعك التقريبي وأخبرهم مالك موقع الويب أنك تستخدم Tor ، فيمكنهم التحقق من وصل إلى Tor في ذلك المكان في نفس الوقت الذي شاهدت فيه موقع الويب للحصول على هويتك الحقيقية. لقد فعل مكتب التحقيقات الفيدرالي هذا من قبل ، لكن نادرًا ما يكون مشكلة. إذا كنت قلقًا بشأن هذا الأمر ، فيمكنك استخدام شبكة WiFi عامة.

ملاحظة جانبية: الشبكات الافتراضية الخاصة ليست فعالة مثل Tor في إبقائك مجهولاً على الإنترنت.

الواضح

عادة سبب القبض على الأشخاص ليس أن الحكومة تحصل على عنوان ال IP الخاص بهم. بل إنها إرسال شيء ما إلى الإنترنت يكشف عن هويتهم أو يكشف عن هويتهم لصديقهم. الأخطاء الغبية هي ما توقع الناس. فيما يلي بعض الأمثلة على الأشياء التي يجب عليك القيام بها دائمًا:

1. عند إرسال القصص ، كن غامضًا واختلق التفاصيل. يمكن استخدام جزء صغير من المعلومات ، مثل عدد الأشقاء لديك ، للكشف عن هويتك.
2. كن حذرًا جدًا عند إرسال الصور إلى الإنترنت. امسح كل بيانات ال EXIF من جميع الصور التي تحملها وتحقق من عدم وجود تفاصيل يمكن استخدامها لتحديد هويتك.
3. إذا كان هناك أشخاص آخرون يستخدمون جهاز الكمبيوتر الخاص بك، فتأكد من عدم حفظ سجل التصفح. لا تحفظ أي شيء على جهاز الكمبيوتر قد يكشف عن هويتك.
4. لا تستخدم اسمك الحقيقي للاشتراك في الحسابات التي تستخدمها لهويتك المجهولة.

5. لا تكشف عن هويتك المجهولة للأشخاص الذين تعرفهم في الحياة الواقعية.
6. لا تكشف عن هويتك الحقيقية للأشخاص الذين تعرفهم من خلال هويتك المجهولة.

الخاتمة

إذا قمت بإنشاء حسابات مجهولة على Reddit أو Facebook، فيمكنك أحيانًا البقاء آمنًا. لكن قد لا ترغب في الوثوق بهذه الشركات إذا كانت حياتك تعتمد عليها. إذا كنت تريد أن تظل مجهول الهوية بثقة، فاستخدم Tor.

PrivacyTools هو مورد جيد للبرامج الأخرى الموجهة نحو الخصوصية.

وتذكر: أنت وحدك المسؤول عن سلامتك.