الحكومات تستطيع اختراقك .. هذا ما يمكنك فعله

كتبه نون بوست | 25 أكتوبر, 2013

طرحت التسريبات الأخيرة لإدوارد سنودن من أن وكالة الأمن القومي الأمريكية يمكنها اختراق غالبية وسائل التشفير المستعملة على الانترنت عبر العالم، أسئلة حول مدى استطاعة المستخدمين تأمين بياناتهم وخصوصياتهم، خاصة حين نتحدث عن النشطاء والصحفيين، المعرضين بشكل شبه دائم لمخاطر مستمرة في عالمنا العربي.

التسريبات باختصار تتحدث عن أن وكالة الأمن القومي تستخدم بوابات خلفية لدى معظم برامج وتطبيقات الشركات الكبرى تمكنها من اختراق حسابات المستخدمين والاطلاع على بياناتهم، حيث تنفق الوكالة ما يزيد على ٢٥٠ مليون دولار سنويا لـ"تشجيع شركات التكنولوجيا والبرمجيات على جعل برامجها قابلة للاستغلال" من قبل أجهزة الأمن الأمريكية.

إلى حد ما، ليس من المُستغرب أن نسمع أن جهازا أمنيا أو وكالة مخابرات تقوم بالتجسس! هذا هو عملهم على كل حال. لكن المقلق أن ما تستطيع وكالة الاستخبارات الأمريكية فعله فيما يتعلق باختراق الخصوصية، غالبا تستطيع دول وأجهزة أخرى فعله، لذلك فقد ذكرت مؤسسة بيو أن ٩٠٪ من مستخدمي الانترنت يتخذون خطوات لتجنب المراقبة بشكل أو بآخر.

رغم كل شيء، ما زال باستطاعة المستخدمين اتخاذ بعض الإجراءات لتقليل خطر اختراق بياناتهم، جميع التقارير لم تقل لنا ما هي التكنولوجيا التي تستطيع وكالة الأمن القومي اختراقها، لسنا دولا حتى يمكننا أن ننشيء إنترنت خاص بنا، لكن ما يمكننا فعله هو التقليل من احتمالات إمكانية الاختراق.

مفتاح الحل يمكن في كلمة واحدة: **البرمجيات مفتوحة المصدر**

الآن ندرك أن الشركات الكبرى يعملون مع وكالة الأمن القومي لبناء بوابات خلفية تمكن الاستخبارات وأجهزة الأمن من التسلل لبياناتك، لذلك فعلينا ألا نثق كثيرا بالشركات الكبرى وأدواتها، هناك بعض التطبيقات والبرامج مفتوحة المصدر التي يشارك في تأمينها المبرمجون عبر العالم وتخضع بشكل دائم للتدقيق واختبار فعاليتها وتأمينها.

إليك بعض التطبيقات الذي يمكنك عبر استخدامها تقليل احتمالات تعرضك للاختراق:

Truecrypt هو برنامج يمكنك من حماية أصغر الوثائق، و ملفاتك الحساسة، أو حتى قطاعات كاملة في القرص الصلب

GPG هو تطبيق مفتوح المصدر يُستخدم لتشفير الاتصالات عبر البريد الإلكتروني، في كل الأحوال، وللعلم، لن يمكنك من تأمين اتصالاتك بنسبة ١٠٠٪ أبدا.

TAILS هو نظام تشغيل مفتوح المصدر، وهو توزيعة من نظام تشغيل لينكس، أعدها مهتمون بالخصوصية، يمكنك استخدامها عبر قرص مدمج أو ذاكرة يو اس بي ما يعني أنه بمجرد إغلاق حاسوبك فإنه لن يكون هناك أثر لما فعلت. استخدم TAILS حين تريد ألا تترك أثرا على الانترنت! فجميع اتصالاتك تمر عبر TOR "تور" وهي مجموعة تطبيقات بالاضافة لشبكة مفتوحة تمكنك من إجراء اتصالاتك بالشبكة بدون ترك أي أثر عن مكانك، وتكاد تكون تلك TAILS بالإضافة إلى TOR هي أكثر الحلول أمانا، ولذلك فهي أكثرها صعوبة نسبية.

Off-the-record messaging, OTR هو برنامج آخر مفتوح المصدر يعني بتشفير جميع اتصالاتك عبر برامج المحادثة الفورية التي تدعم ذلك البرنامج.

لهؤلاء الذين يفضلون بقاء معظم بياناتهم في الـcloud أو على الشبكة حيث يمكن الاحتفاظ بالمعلومات بعيدا عن مخاطر الاحتفاظ بها على حاسب أو هاتف نقال معرض للسرقة والتلف، يمكنهم استخدام BoxCryptor الذي يعطيهم القدرة على الاستفادة من مزايا الـcloud computing بالإضافة لميزات التشفير والتأمين مجانا أو عبر خطط دفع مختلفة

يمكنك كذلك من استخدام VPN والذي يُعد نفقا يمكنك من الدخول إلى الانترنت بشكل آمن وبدون أثر، كما أنه مفيد للغاية عند الدخول إلى شبكات مغلقة من على بعد، حيث تمر اتصالاتك بوسيط يخفي معلوماتك عن المواقع والشبكات التي تزورها.

لا يمكننا أن نقول أن تأمين معلوماتك هو أمر ممكن بنسبة ١٠٠٪، لكن في المعركة مع الحكومات حول خصوصية الأفراد، علينا أن نستمر في المحاولة.

رابط المقال : https://www.noonpost.com/789/