الحفاظ على سريّة المعلومات كرّاسة للناشطات

- أو -

كيف نجعل حياة متعقبي معلوماتنا عبر الانترنت أكثر صعوبة

يوفال آدم ونوعام روتيم, CryptoParty, 2020

DO YOUR RIGHTS KNOW YOUR RIGHTS

האגודה לזכויות האזרח בישראל
جمعية حقوق المواطن في اسرائيل
The Association for Civil Rights in Israel

افتتاحية

ما هي هذه الكرّاسة؟

نقضي جزءًا كبيرًا من حياتنا في استخدام الإنترنت، وهناك نترك الكثير من المعلومات الشخصية. لكننا نادراً ما نتوقّف ونفكّر فيمن يستطيع الاطلاع على معلوماتنا وكيف نتعامل معه. تكشف التقنيات المتوفرة بين أيدينا معلوماتنا الشخصية وقد تعرض أمننا للخطر وتضر بنا بطرق مختلفة. يمكن للحكومات والسلطات، إلى جانب المؤسسات الخاصة والشركات التجارية والعديد من الأطراف المعنية الأخرى، دفن مهن ناجحة أو علاقات شخصية، وتتبعنا ونشر معلومات شخصية لا نرغب مشاركتها مع أي شخص، كل هذا بكبسة زر واحدة.

هل لدينا ما نفعله لتقليل مدى نشر معلوماتنا الشخصية على الإنترنت وتعريضها للملاحقة والاستغلال السيء؟ في هذه الكرّاسة، سنحاول ترتيب بعض الأمور وتقديم بعض التوصيات والنصائح لإجراء تغييرات طفيفة في سلوكنا والتي تجعل ملاحقتنا أكثر صعوبة.

من المهم التأكيد على أن ما يكتب هنا لا يمكن أن يعطي سوى فكرة أولية عن الموضوع، وأنه في حال الشعور بالتهديد فمن المهم استشارة الخبراء. إضافة الى ذلك، ستجدن في نهاية الكراسة روابط لمصادر أخرى حيث يمكنكن التعمق ومعرفة المزيد حول الموضوع.

ماذا يعني الحفاظ على الخصوصية في الانترنت؟

لا يوجد حل سحري للحفاظ على الخصوصية، وليست هناك حماية 100%. نحن نتحدث عن عملية تبني عادات وتصرفات ستجعل من مهمة ملاحقتنا غالي الثمن. لا جدوى من الحماية أمام *كل* التهديدات. نحن نحتاج إلى النظر في تهديدات محددة ذات صلة بنا، وضبط سلوكنا من أجل التعامل معها.

في هذه الكرّاسة سنوصي باستخدام عدد من الأدوات التي يمكن أن تساعدنا في الحفاظ على خصوصيتنا على الإنترنت. من المهم أن نفهم ما الذي تعطينا إياه كل "أداة خصوصية" - وعلى وجه الخصوص ما الذي *لا* تعطيه، وما هي نقاط ضعف كل أداة. على سبيل المثال: لن يساعدنا تشفير مرور المعلومات (أثناء تصفح الانترنت أو إرسال رسالة واتساب) في حال قيام شخص ما بأخذ جهاز الكمبيوتر أو الهاتف الخاص بنا. وكذلك، فإن تشفير المعلومات بصورة عامة (حفظ الملفات على القرص الصلب) لن يساعدنا في حال قام شخص ما بالتنصّت على اتصالاتنا.

ممارسات أساسية

كلمة المرور

يجب عدم استخدام نفس كلمة المرور مرتين. إذا استخدمت كلمة مرور معينة لدخول موقع ما، فلا تستخدميها أبدًا على موقع آخر. يتم تسريب كلمات المرور بانتظام من المواقع، والاستخدام المزدوج لكلمات المرور هو فتح مجال لسرقة كلمة المرور الخاصة بنا.

لا حاجة إلى تذكر كل كلمات المرور التي نستعملها، يمكن ويجب استخدام "مدير كلمات المرور"، مما يسهل علينا كثيرًا. يتم تثبيت مدير كلمات المرور داخل صفحة التصفّح (وأيضًا كتطبيق على الهاتف) وهو يقوم بحفظ جميع كلمات المرور بطريقة مشفرة. إضافة الى ذلك، فإنه يملأ خانة كلمات المرور تلقائيًا عندما نقوم بتصفح المواقع.

مقترحات لاستخدام مدير كلمات مرور:

https://www.lastpass.com
https://1password.com
https://keepassxc.org

مصادقة ثنائية المصدر – التحقق بخطوتين

المصادقة ثنائية المراحل (Two-Factor Authentication) هي آلية مصممة لضمان عدم دخول حسابك الخاص حتى لو سرق شخص ما كلمة المرور الخاصة بك. الفكرة من وراء هذه الآلية هي أنه من أجل الوصول إلى مكان معين فأنت بحاجة إلى الدمج بين "شيء أعرفه" (مثل كلمة المرور) مع "شيء أملكه" (مثل هاتف محمول معي).

من السهل ويوصى باستخدام المصادقة ثنائية المراحل على حساب بريدك الإلكتروني أو حسابات الشبكات الاجتماعية، في حالة كهذه ستبقى حساباتك محمية حتى لو حصل شخص ما على كلمة مرورك.

شرح حول عملية المصادقة ثنائية المراحل

منع الإعلانات

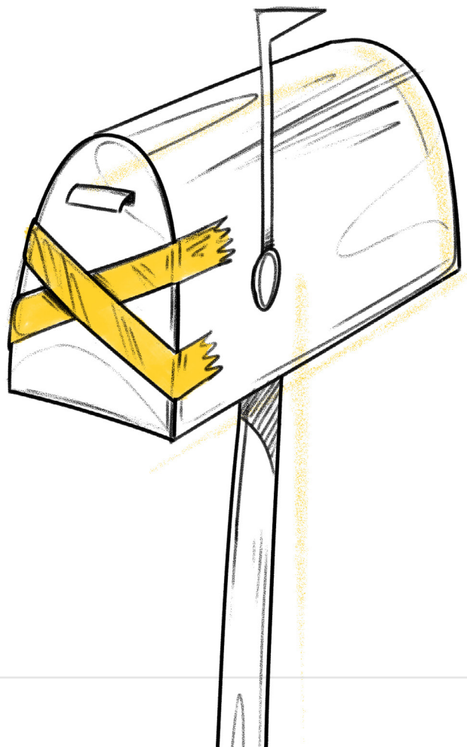
في كل موقع نزوره هناك العشرات وأحيانًا المئات من آليات المراقبة والرصد، بعضها يظهر كإعلانات وبعضها لا نراه بتاتًا. تقوم هذه الآليات بجمع وأرشفة معلومات شخصية يمكن أن تستخدم لتصنيفنا، وتتبع كل النشاطات التي نقوم بها على الشبكة. من خلال تشغيل أداة منع الإعلانات، يمكننا التأكد من أن المعلومات الخاصة بنا لن يتم إرسالها إلى قواعد بيانات مختلفة ولن يتم بيعها للشركات التي تتداول معلوماتنا الشخصية.

نصيحة:
تثبيت uBlock Origin في المتصفح الخاص بك

منع برمجيات التجسس (Spyware) والبرمجيات الخبيثة (Malware)

برامج التجسس والتخريب (احداث الضرر للجهاز) هي برامج خبيثة. يمكن لهذه البرامج سرقة المعلومات الشخصية والحساسة ومراقبة نشاطنا على الشبكة.

إحدى الطرق الشائعة لتتبع المستخدمين تكمن في تثبيت برامج التجسس على أجهزتهم، هذه البرامج ترسل إلى المتابع تحديثًا حول كل تحركات "الضحية" وكل ككبسة زر تقوم بها على لوحة المفاتيح، وكل شاشة يتم فتحها، وأي معلومات تدخل وتخرج من الجهاز. أفضل طريقة لتقليل مخاطر هذه البرامج هو تثبيت الأشياء الضرورية فقط من المصادر الموثوق بها، وعدم الانجرار وتثبيت برامج أو تطبيقات غير ضرورية من مصادر مشكوك فيها.



مصطلحات يجب معرفتها

التشفير

يسمح لنا التشفير بحماية المعلومات مثل حفظ أي شيء في مكان آمن: بدون وجود مفتاح أو رمز السري لا توجد طريقة لمعرفة ما بداخل المكان الآمن. يسمح لنا التشفير بحفظ المعلومات الشخصية أو السرية، مما يتيح الوصول للمعلومات فقط لمن نثق بهم.

التشفير من طرف إلى طرف هو عملية تشفير يتم فيها تحديد مفاتيح التشفير وتخزينها فقط بواسطة أجهزة المستخدمين (الهواتف الذكية أو أجهزة الكمبيوتر). هذا على عكس الاضطرار إلى الاعتماد على بعض الخوادم الموجودة بين المستخدمين، وإنشاء المفاتيح لهم، ولكنه يتيح أيضًا مراقبة بعض التحركات "المشفرة".

المعلومات والبيانات الوصفيّة

إذا كانت المعلومات مشفرة هل كل شيء على ما يرام؟ بالطبع لا. يحمي التشفير محتوى الاتصالات، ولكنه لا يحمي تفاصيل أخرى للاتصالات (Metadata). على سبيل المثال، إذا أرسل شخص ما رسالة مشفرة فلن يتمكن أي شخص يحاول متابعتها من معرفة محتوى الرسالة، لكنهم يعرفون لمن أرسلها، وكيف، ومتى، وكثير من بيانات الاتصال الأخرى التي قد تكشف قدرًا كبيرًا من معلوماتنا وتنتهك خصوصيتنا.

رئيس وكالة الأمن القومي الأمريكية (NSA) السابق مايكل هايدن قال: "إننا نقتل الناس بناء على بيانات ما فوق المعلومات". تكفي معرفة اجراء اتصال بين طرفين، حتى دون الكشف عن محتواه، للمس جديًا بكلا الطرفين.

رمز مفتوح/مغلق ولمَ من المهم استخدام الرمز المفتوح أكثر ما يمكن

يتيح لنا استخدام برنامج مع رمز مفتوح معرفة المكان الذي تتعرض فيه خصوصيتنا للخطر.

رمز مغلق هو رمز برنامج مكشوف فقط أمام الشركة التي توزع البرنامج، لذلك ليس لدينا طريقة لمعرفة كيف تم بناء البرنامج (أو التطبيق)، وهل لديه مداخل متوارية تسمح للشركة أو للآخرين بالوصول إلى معلوماتنا، سواء كانت معلوماتنا مشفرة ومحمية ام لا.

الرمز المفتوح هو رمز تم بناؤه بشكل جماعي من قبل المطورين من جميع أنحاء العالم. هو رمز مرئي على الشبكة وبالتالي يتيح لمجتمع أمن المعلومات الدولي بفحصه والتأكد من أنه لا توجد فيه ثغرات تسمح لأجسام/ أجهزة غريبة الوصول إليه دون إذن منا. عندما نستخدم الرمز المفتوح نحن لسنا ملزمات بالاعتماد على وعود شركة تجارية التي يعتبر خط الربح فيها أكثر أهمية من خصوصية مستخدميها.

الهواتف الخلوية

تطبيقات ارسال الرسائل

هناك عدد من التطبيقات المنتشرة لإرسال الرسائل، لكن هناك واحدة فقط يمكنها ان تحافظ حقًا على خصوصية مستخدميها.

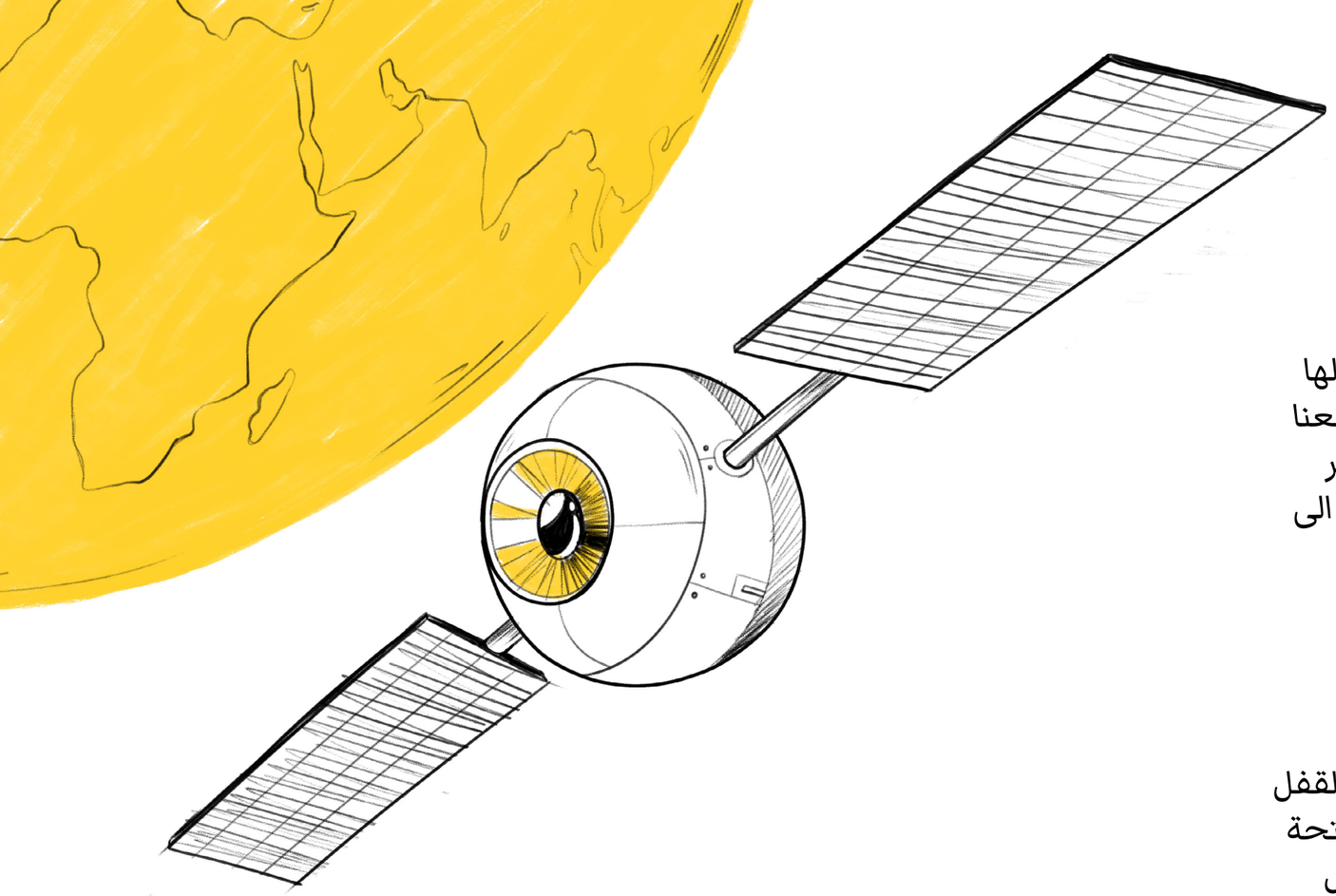
Signal هو تطبيق مصمم كمفتوح المصدر والذي يقوم بتشفير الرسائل بشكل تام ولا يقوم بتخزين المعلومات أو البيانات الوصفية للمستخدمين. في الحالات التي أصدرت فيها سلطات تنفيذ القانون في الولايات المتحدة أمرًا قضائيًا يأمر Signal بالإفصاح عن معلومات الاتصال في حساب معين، تلقوا صفحة فارغة، ولذلك لأن التطبيق لم يقم بتخزين أي معلومات.

لماذا لا تعتبر WhatsApp و Telegram تطبيقات آمنة؟

تدعي الشركات التي تدير تطبيقي WhatsApp وTelegram أن الرسائل مشفرة بشكل تام، ولكن نظرًا لأن هذه البرامج عبارة عن برنامج مغلق المصدر والذي لا يمكننا الوصول إليه، لا يمكن فحص مدى صحة ادعاء الشركات حول سرية المعلومات.

بكل الاحوال، لا يزال بإمكان الشركات المشغلّة لهذين التطبيقين الوصول إلى البيانات الوصفية لكل رسالة، ويمكنهم الاحتفاظ بالرسائل إلى الأبد، حتى تتمكن الشركة من معرفة من يتحدث مع من ومتى. هذه الإمكانيات كافية لتوصيل شخص إلى آخر وفي الوقت ذاته انتهاك خصوصية وحقوق كل مستخدم بشكل خطير.

بالإضافة إلى ذلك، لا يتم تشفير المكالمات العادية والمكالمات الجماعية على Telegram على الإطلاق. للحصول على تشفير تام في Telegram، يلزمك فتح نافذة محادثة خاصة.



منع تحديد موقع الهاتف الخلوي

من المؤكد أن الأجهزة الخلوية التي نحملها هي أداة مفيدة، ولكن نظرًا لاتصالها مع الهوائيات الخلوية المثبتة في كل مكان حولنا، تعرف الشركات الخلوية موقعنا الجغرافي الدقيق في كل لحظة. تحديد الموقع يتم بكل الأحوال - بغض النظر عن وجود نظام GPS على الهاتف. هذه المعلومات الخاصة يمكن ان تتسرب الى جهات عدة وتنقل معلومات حولنا لا نريد الكشف عنها.

قفل الهواتف الخلوية

توفر الهواتف الذكية اليوم عددًا من الطرق المختلفة لقفل الجهاز. انتبهوا أن القفل بواسطة بصمات الأصابع أو التعرّف على الوجه هو قفل يمكن اجباركن على فتحة في حال مورست ضدكن القوة. لذلك فإن القفل الموصى به هو رمز سري طويل ومعقد.

يُنصح بعدم اصطحاب جهاز الهاتف الخلوي الخاص عند التواجد في فعاليات او أماكن حساسة. إذا لزم الأمر حمل هاتف خلوي يمكنك استخدام هاتف رخيص مع بطاقة SIM يمكن التخلص منها بعد الاستخدام.

تصفّح الانترنت

التصفح المشفر (HTTPS)

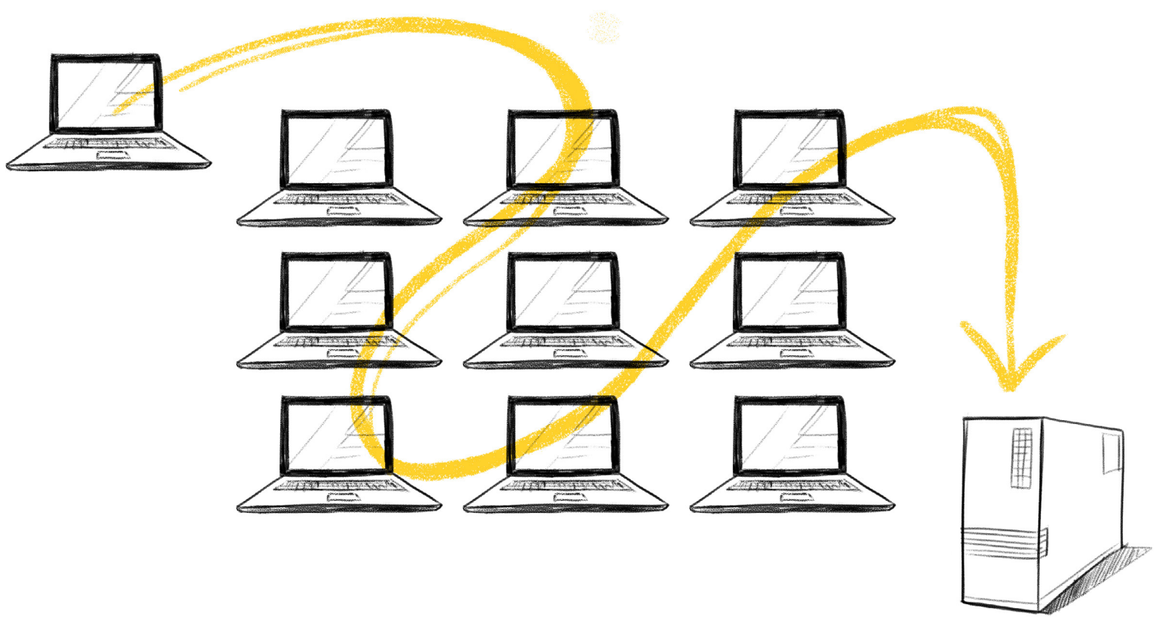
على الرغم من أن كلمة "تشفير" تبدو معقدة للغاية إلا أن جميع المتصفحات الحديثة تدعمها دون أي إجراء إضافي من قبلنا. إذا كان العنوان في المتصفح يبدأ https (بدلاً من http) وإذا كان هناك قفل أخضر بجانب الأحرف الأولى، فهذا يعني أن حركة المرور بين المتصفح وخادم الانترنت الذي نتواصل معه يتم تشفيرها.

ملاحظة: حركة المرور المشفرة تمنع قراصنة الحواسيب والانترنت من قراءة المعلومات لكنها لا تعني أن المعلومات آمنة بشكل تام. على سبيل المثال، على الرغم من أن خدمة البريد الإلكتروني الخاصة بنا تحتوي على قفل، فإن الشركة التي تدير بريدنا الالكتروني لديها قدرة للوصول إلى محتوى الرسالة، وكذلك كل جسم لديه صلاحية للاطلاع على الأنظمة التي يتم تخزين الرسائل فيها.

التصفّح مجهول الهوية - TOR

إذا كانت اتصالاتنا معرّضة للمراقبة باستمرار فكيف يمكن الحفاظ على سريّة هوية المتصفح عبر الإنترنت؟ لهذا الغرض تم ابتكار مشروع -Torوهو متصفح مشابه جدًا لمتصفح فايرفوكس (Firefox) ولكنه يسمح بالتصفح المجهول والآمن. يعمل التصفّح باستخدام Tor مثل لعبة "نقل الرزمة" (Package Pass) الشهيرة، حيث تعرف كل حلقة في السلسلة ممن تلقت المعلومة ولمن سترسلها فقط، دون معرفة ما سبق وصول المعلومة اليها او ما سيلي نقل المعلومة منها بعد ذلك. وبهذه الطريقة؛ حتى إذا كشف قراصنة الانترنت أحد الروابط؛ فإن المصدر والوجهة لا يزالان آمنين وغير معروفين.

https://www.torproject.org



لماذا يعتبر VPN غير آمن؟

يتم تقديم خدمة Virtual Private Network أو باسمها المشهور VPN كأداة تصفح مجهولة المصدر. عادةً ما يتم توفير خدمة VPN من قبل شركة تجارية تقدم الخدمة بدفع رسوم أو مجانًا، حيث تعرض مسار تصفح آمن من خلال خوادم الشركة الموجودة عادةً في بلد آخر.

في حين أن VPN يمكن أن تحاكي التصفح من بلد آخر، هناك مشكلتان رئيسيتان في استخدامه. الأولى هي أن سوق VPN معروف بسوء السمعة وبيع المعلومات الشخصية للمستخدمين. والثانية الأكثر خطورة هي أن VPN لا تضمن عدم الكشف عن الهوية: أثناء التصفح على شبكة Tor، يتم التصفح من خلال ثلاثة خوادم مختلفة، على VPN يتم الاتصال من خلال خادم واحد فقط، وهذا لا يكفي لضمان عدم الكشف عن هوية المتصفح/ة الحقيقية.

أدوات متطورة

تشفير الملفات

عندما نعمل مع ملفات حساسة بشكل منتظم قد لا نريد أن تكون هذه الملفات متاحة على جهاز الكمبيوتر الخاص بنا في أي وقت. في هذه الحالة يمكننا استخدام برنامج تشفير يسمى VeraCrypt والذي يسمح لنا بإنشاء ملف مشفر يتم فتحه فقط باستخدام كلمة مرور. عند قفل الملف، لن يتمكن أي جسم من فتح الملفات أو تعديلها، ولن يتمكن حتى من رؤية الملفات الموجودة داخل مجلد مشفر.

انتبهوا الى ان حل التشفير هذا يقوم بتشفير الملفات على جهاز الكمبيوتر الخاص بنا فقط، وبالتالي فإن أي إرسال للملفات المفتوحة أو تحميلها على مجلدات مشتركة قد يؤدي إلى تسريب المعلومات.

https://www.veracrypt.fr

مساحة عمل مؤقتة - Tails

Tails هي مساحة عمل مشفرة ومؤقتة تتيح لمستخدميها العمل على جهاز كمبيوتر بشكل "نظيف" حتى إذا تم تثبيت برامج تجسس على الجهاز. يتم تشغيل نظام Tails عن طريق تشغيل الكمبيوتر باستخدام ذاكرة خارجية خاصة تقوم بحذف كل معلومات الاستخدام بعد الانتهاء من العمل.

هذا الحل المتقدم يعطي الأولوية القصوى للأمان على سهولة الاستخدام. لذلك، من المستحسن التعامل مع هذا الحل بانتظام، ولكن إذا كانت هناك مسألة تتطلب الكثير من الخصوصية، مثل كتابة أو إرسال ملف حساس بشكل خاص فإن Tails هو الحل المناسب.

https://tails.boum.org

للاستزادة

https://ssd.eff.org

https://holistic-security.tacticaltech.org

https://datadetoxkit.org