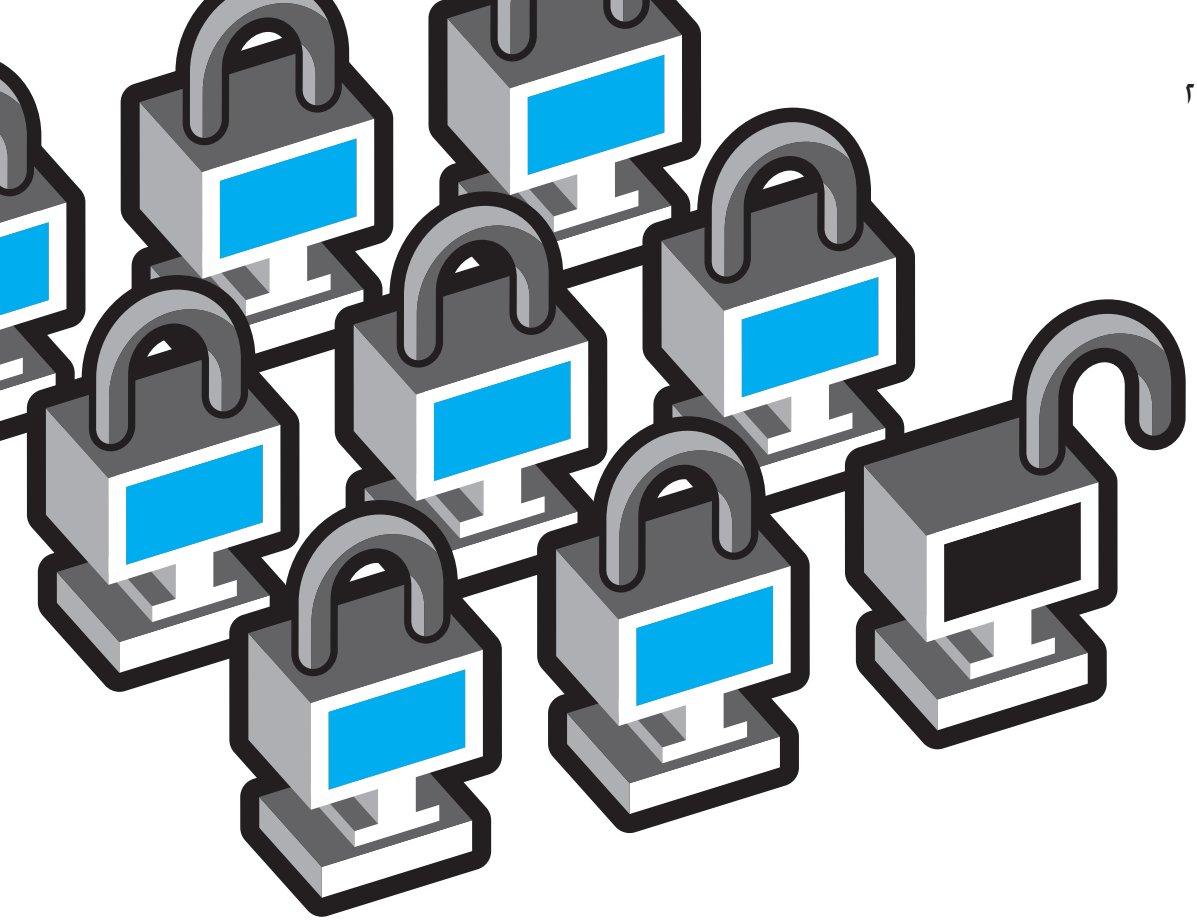


دليل عملي لحماية هويتك والحفاظ على سريتك أثناء تواجدك على الإنترنت وأثناء استخدامك للتليفون المحمول

للمواطنين في الشرق الأوسط وشمال أفريقيا

كُتِب هذا الدليل من أجل مواطني الشرق الأوسط وشمال أفريقيا الذين يريدون استخدام التكنولوجيا بصورة آمنة للتواصل، وتنظيم أنفسهم، وتبادل البيانات (التقارير الإخبارية، والمعلومات، والإعلام، إلخ.) فهو مكتوب لقاعدة عريضة من الجمهور ذو المعرفة المتواضعة بالكمبيوتر والذين يودون معرفة الخطوات التي يمكن اتخاذها ليكونوا في مأمن أثناء استخدامهم الإنترنت وأثناء استخدامهم أجهزة التليفون المحمول. يشتمل هذا الدليل على نصائح وقواعد لتقليل المراقبة والرصد، وحماية الخصوصية، والتعامل مع الرقابة. فهو يشمل: الاستخدام الآمن للبريد الإلكتروني والرسائل الفورية، وأفضل العادات لكلمة السر، وكيف تحافظ على جهازك خاليًا من الفيروسات وبرامج التجسس، وكيفية التحايل على حجب الإنترنت مع الإبقاء على هويتك مجهولة. (لو صادفت أية مشكلة في الدخول على أية من الروابط المكتوبة في هذه الوثيقة نتيجة إغلاق المواقع وبعد استخدامك لأدوات التحايل المذكورة أدناه، نرجو منك إرسال رسالة إلكترونية إلى info@accessnow.org وأخبرنا بما تريدنا إرساله لك بالبريد الإلكتروني.)

على الرغم من إن المعلومات المذكورة في هذا الدليل تعد دقيقة وراجعناها في يونيو ٢٠١١، غير أن الحماية على الإنترنت إجراء معقد يتغير مع التطور التكنولوجي ومع ظهور مكامن الضعف. فلا توجد طريقة سحرية تضمن لك السرية التامة والخصوصية المطلقة، لكن هذه الأدوات والاستراتيجيات ستساعدك بالتأكيد في تأمين نفسك بشكل أفضل.

صاغت عدة منظمات وبعض الأفراد المتخصصون في مجال آمان الإنترنت والمحمول هذا النص وقاموا على مراجعته لو واجهتك مشاكل في هذا النص أو عندك أية اقتراحات، أرجو إرسالها على البريد الإلكتروني info@accessnow.org

بعض الأسس الضرورية

تأمين البريد الإلكتروني:

يعد هوتميل «Hotmail» وجيميل «Gmail» من أكثر خدمات البريد الإلكتروني المجاني الذي يمنح خدمة بريد إلكتروني آمنة عن طريق توفير إنترنت مشفر بينك وبين مانح خدمة البريد الإلكتروني وهو ما يسمى بالتصفح الآمن (HTTPS). يحتوي Gmail الآن على التصفح الآمن HTTPS كأحد إعداداته الافتراضية، لكنك ستحتاج لتشغيلها في Hotmail لو لم تكن شغلتها قبل ذلك (إذهب إلى حسابي> خيارات أخرى> اتصال باستخدام التصفح الآمن HTTPS> استخدام التصفح الآمن HTTPS بشكل تلقائي.) وحاليًا ياهو ميل "Yahoo Mail" ليس مؤمنًا. رغم إنه أمر مزعج لكننا نوصي بإنشاء واستخدام حساب بريد إلكتروني بديل يشتمل على خصية التصفح الآمن HTTPS من أجل مراسلاتك وخاصة أية موضوعات حساسة. تذكر إن التصفح الآمن (HTTPS) يؤمن الاتصال بينك وبين مانح بريدك الإلكتروني فقط، ولايزال الوصول للوجهة النهائية ممكن يكون غير مشفرًا وعرضة للهجوم لو كان المتلقي لا يستخدم التصفح الآمن أو لو كان يستخدم بريد إلكتروني من شركة أخرى. توجد خيارات أخرى لخدمة البريد الإلكتروني الآمن مثل Riseup.net و Vaultletsoft. إضافة إلى ذلك، يوجد نظام ممتاز لتشفير بريدك الإلكتروني وتوقيعه رقميًا PGP وGPG (لمزيد من الإطلاع باللغتين الإنجليزية والعربية).

إذا كنت تستخدم Gmail وتود معرفة المزيد عن خصائصه الأمنية الأخرى (٢-عامل مصادقة، تاريخ بروتوكول الإنترنت)، أرجو الإطلاع على قائمة آمان Gmail. لو كنت تستخدم Hotmail، يمكنك معرفة المزيد عن خصائصه الأمنية هنا، بما في ذلك استخدام كلمة سر لمرة واحدة على أجهزة الكمبيوتر العامة.

جعل كلمة السر أكثر أماناً:

من أهم ما يمكنك فعله هو ابتكار كلمات سر جيدة وقوية واتباع عادات جيدة في التعامل معها. بعض النصائح الأساسية:

- فكر في جملة بدلًا من كلمة وحدها.
- إجعل جمل مرورك تتكون من ١٢ حرف أو أكثر؛ مما يُصَعِّب كسرها باللجوء للبرمجيات المختلفة.
- استخدم خليط من الرموز، والأرقام، والحروف الكبيرة، والحروف الصغيرة. وأحد الطرق هي الاشتمال على رموز وأرقام لكلمات وحروف في جملة المرور والتي ممكن أن تكون مقولة أو سطر في أغنية أو قصيدة.
- لا تستخدم نفس كلمة السر لكل حساب؛ لأن لو خُرقت كلمة سرك بسهولة عند إدخالها على الإنترنت في مكان لا يوفر التصفح الآمن HTTPS، فإنه يسهل خرق معلومات تسجيلك واستخدامها للدخول على حساباتك الأخرى.
- غير كلمة السر كل ٣ أشهر أو أقل لو كنت تستخدم أنظمة الإنترنت أو أجهزة الكمبيوتر في مقاهي الإنترنت أكثر من استخدامك لجهازك الشخصي.
- لو كانت لديك مشكلة في تذكر كلمات السر، فاستخدم برنامج آمن مشفر مثل KeePass لتتبعهم.
- تتعرض بعض الحسابات للخطر خلال تشغيل نُظُم استعادة كلمة السر المفقودة. فتأكد أنه ليس من السهل أو اليسير أو تخمين أسئلتك وإجاباتك السرية لحساباتك.

مكافحة الفيروسات وبرامج التجسس

أحد الموضوعات الحساسة عند أغلب مستخدمي الكمبيوتر هو استخدام البرامج المقرصنة، خاصة نظام مايكروسوفت ويندوز. فعندما تحصل على برمجيات عن طريق غير قانوني، فإنك توفر بضعة دولارات لكنك أيضاً تعرض نفسك لمكامن ضعف لا تُعالج نتيجة عدم تلقيك التحديثات والتصحيحات التي يصدرها مُصَنِّع البرنامج. فإذا لم تكن تستطيع الحصول على نسخ رسمية قانونية من البرمجيات ونظم التشغيل، فعلى الأقل ينبغي عليك تشغيل برنامج مكافح فيروسات قوي وبرنامج مكافح تجسس قوي لتقليل المخاطر. لكن لو كان متاح لك، فحاول الحصول على نسخ رسمية من البرمجيات من أجل أمنك الشخصي.

- فلو لم تكن بالفعل تشغل حاليًا مكافح فيروسات قوي، فإن برنامج Avast هو مكافح فيروسات ممتاز يساعد على حماية البيانات على جهازك من التلف أو الإصابة. برنامج مكافحة البرمجيات الخبيثة Malwarebytes هو برنامج آخر يعمل على الوضع الآمن إذا بالفعل أُصيب جهازك.
- الحصول على برنامج مكافحة التجسس بنفس درجة الأهمية، وهو يعمل على إيجاد وإزالة البرامج الضارة التي تستطيع تتبع كل نشاطاتك أثناء تواجدك على أو غيابك عن الإنترنت. أما برنامج Spybot هو برنامج لمكافحة برامج التجسس، مجاني وفعال.
- لتقليل تعرضك للفيروسات وبرامج التجسس، لا تفتح رسائل إلكترونية أو مرفقات من مصادر غير موثوق بها أو مجهولة. لو كنت غير واثقًا من آمان مرفقات، أو ملفات، أو موقعًا إلكترونيًا، يمكنك رفعه لاختباره على Virus Total أو إرسال في بريد إلكتروني إلى scan@virustotal.com مع كتابة عنوان الرسالة «SCAN» في خانة العنوان أو (SCAN + XML لو كنت تريد الحصول على نتائجك بصيغة XML)
- أحد نقاط الدخول الشائعة للشفرات الخبيثة هي السكريبتات scriptsالتي تتعرض لها أثناء تصفحك الشبكة. فنحن نوصي بشدة إنك تُنزِل على جهازك إضافة NoScript لاستخدامها مع متصفح فايرفوكس، والتي تمكنك من منع أغلب السكريبتات وتسمح فقط لتلك التي تثق بها.
- نقطة دخول أخرى شائعة للفيروسات وبرامج التجسس هو استخدام ذاكرة الفلاش USB ووسائط التخزين الأخرى. لا تضع أي ذاكرة أو وسيلة تخزين في جهازك إلا إذا كنت تعرف مصدرها وتثق به. كذلك يوصى باستخدام برنامج مكافحة الفيروسات وبرنامج مكافحة التجسس مثل Spybot و Avast لفحص الذاكرة قبل تشغيلها.

فكر في التحويل إلى نظام تشغيل Linux Ubuntu «أوبونتو لينكس» إلا إذا كان عندك سبب هام لاستمرار استخدامك ويندوز. يسمح أوبونتو بتشغيل الأقراص الصلبة المشفرة بصورة افتراضية وخاصة إنه خالي من الفيروسات والبرمجيات الخبيثة. بعيداً عن الهجوم المستهدف، فإن مستخدم أوبونتو في مأمن أكثر من مستخدم نسخة ويندوز غير الأصلية أو المقرصنة أو القديمة. بالإضافة إلى ذلك فإن Mint هو نظام تشغيل آخر قائم على أوبونتو يتيح استخدام نطاق أكبر من البرامج.

الرسائل الفورية الآمنة:

يعد برنامج سكايب والدردشة على جوجل داخل نظام جيميل المؤمن بالتصفح الآمنHTTPS من الخيارات الجيدة لو كنت تعلم إن حسابك لن يستهدفه القناصة. يوجد خيار أكثر أماناً وهو استخدام Pidgin للدخول على عدد من برامج الرسائل الفورية (الرسائل الفورية على جوجل، إلخ.) إن استخدامك إضافة Off The Record OTR يضمن لك إنك حتى مع المفاتيح المشفرة، فإن أية بيانات تسجيل دخول مسبقة ستكون ليست ذي أهمية. اقرأ المزيد عن الخصائص الأمنية عند OTR لكي تفهم مثل الخصوصية من خلال تصميم النظام.

الأمان على الإنترنت:

هناك رقابة مشددة على الإنترنت في العديد من دول المنطقة مثل البحرين والكويت وعمان والإمارات وقطر وسوريا والسعودية. وهي أيضا مرصودة وليس معروفًا لأي مدى. لو تمكنت من إبطال الرقابة، فهذا لا يعني إنك أبطلت الرصد وهو الشق الأصعب. عليك محاولة استخدام بروكسي آمن لإخفاء هويتك مع افتراض إن نشاطاتك قد تكون مرصودة ومسجلة. إضافة إلى ذلك، نحن ننصحك بشدة بعدم استخدام Internet Explorer كمتصفحك على الإنترنت؛ إذ إن به عدد من مكامن الضعف، خاصة مع نسخ البرامج غير المرخصة. في حين إن مزيللا فايرفوكي يعد بديلًا آخر ممتازًا ومزود بعدد من إضافات البرامج المفيدة.

تشفير نشاطاتك على الإنترنت باستخدام التصفح الآمن HTTPS:

لو كنت مشاركًا في نشاط على الإنترنت، فمن المهم أن تفعل ذلك بطريقة تحافظ على هويتك وكلمة السر خاصتك في مأمن. رأينا في تونس مؤخرًا تنفيذ حملات تصيد هائلة استخدموا فيها مكامن الضعف لجمع أسماء التسجيل وكلمات السر للمواطنين الذين يدخلون على فيسبوك. لحسن الحظ أن فيسبوك استجاب بتفعيل التصفح الآمن HTTPS فكان بالفعل مفيداً. يجب عليك دائما استخدام التصفح الآمن HTTPS عندما يتثنى لك. لو لم تكن تستطيع استخدام التصفح الآمن HTTPS فمن الضروري استخدام نظام بروكسي آمن. يستطيع المراقب استهداف مستخدم معين أو موقع معين ويمنع الدخول لمواقع التصفح الآمن HTTPS. لو كنت تستخدم بروكسي لإخفاء هويتك مثل Tor، سيكون من الصعب جدًا إن لم يكن مستحيلًا القيام بمثل هذا الهجوم الاستهدافي.

التصفح الآمن HTTPS:

خاصية ممتازة وبسيرة الاستخدام هي التصفح الآمن HTTPS Everywhere. فهي خاصية من خصائص فايرفوكس تجبر الموقع على استخدام التصفح الآمن HTTPS إذا كان متاحاً. يجب أن تُنَزِل هذا بمثابة أول الأشياء التي تبدأ في استخدامها للحصول على تشفير على طول الطريق من البداية إلى النهاية لمواقع مثل فيسبوك، وتويتر، والبحث على جوجل، وغيرهم الكثير. ستقلل كذلك قابلية سرقة كلمة السر خاصتك عند مشاركتك في شبكات الواي فاي المفتوحة أو غير المؤمنة.

- حَمِّل أحدث نسخة من فايرفوكس إذا لم تكن قمت بذلك بالفعل، ثم نَزِل التصفح الآمن HTTPS Everywhere و/أو Force TLS، ثم أعد تشغيل فايرفوكس وأعدّ تفضيلاتك. ملحوظة: يمتلك التصفح الآمن HTTPS Everywhere عدد من المواقع الافتراضية التي يمكن تضبيطها حسب رغبتك. يقتضي Force TLS تضبيطات أكثر حيث يطلب من المستخدم عمل قائمة بالمواقع لفرض التصفح الآمن HTTPS عليها.
- لو كنت تستخدم جوجل كروم (Google Chrome)، نَزِل على جهازك KB SSL Enforcer Extension (ملحوظة: فهذا ليس فعّالًا مثل إضافات فايرفوكس المذكورة أعلاه؛ إذ لا تزال توجد بعض الأخطاء في SSL Enforcer، على الرغم من إننا نفترض إنه سيتحسن بمرور الوقت.))

فيسبوك: على الرغم من إن خاصية فايرفوكس المشروحة أعلاه تفرض التصفح الآمن HTTPS على عدد من المواقع، إذا استخدمت فيسبوك كثيرًا، فإنه من المرجح التأكد من أن فيسبوك معد على التصفح الآمن HTTPS افتراضيًا، خاصة إذا كنت تدخل عليه من عدة أجهزة كمبيوتر.

- من أجل تفعيل التصفح الآمن HTTPS على فيسبوك، اذهب إلى حسابي أعلى الصفحة على الركن اليمين > الإعدادات > من أيقونة الإعدادات اختر أمان الحساب «تغيير» > اختار خيار تصفح آمن (HTTPS)»
- استخدام بعض الألعاب أو إضافات الفيسبوك الأخرى ستبطل استخدام التصفح الآمن HTTPS.
- لدي فيسبوك الآن خصائص أمنية أخرى يمكنك استخدامها، بما في ذلك التحكم في الخروج عن بعد وإنذار التسجيل التي تمكنك من الحد من عدد الأجهزة التي تستطيع الدخول على حسابك. يمكنك مشاهدة الفيديو الذي يعرض خصائصهم الأمنية على موقعهم. يمكن العثور على دليل إرشادي شامل آخر هنا عن كيفية استخدام فيس بوك بطريقة آمنة

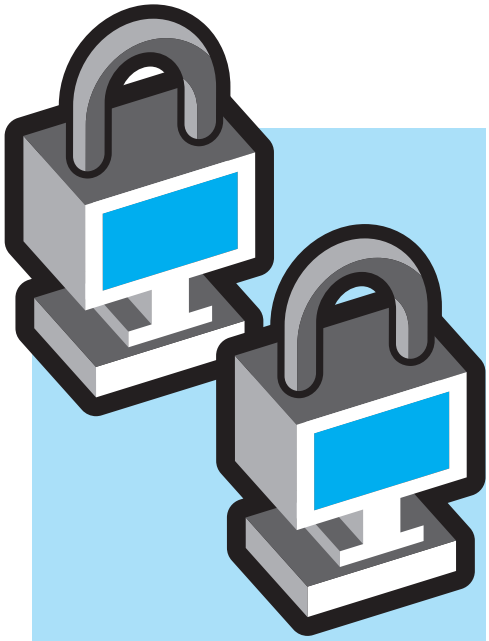
تويتر: على الرغم من أن إضافات فايرفوكس المشروحة أعلاه ستفرض التصفح الآمن HTTPS على برنامج تويتر هو الآخر، لكن من المرجح تغيير إعدادات حسابك على تويتر إلى التصفح الآمن HTTPS ليكون من الإعدادات التلقائية كلما تتصل بحسابك، خاصة لو كنت تدخل على حسابك في تويتر من أجهزة كمبيوتر متعددة أو عامة.

- من أجل تفعيل التصفح الآمن على تويتر، انقر قائمة تويتر خاصتك التي تندرج تحت اسم حسابك في الركن الأيمن أعلى الصفحة > إعدادات> إنزل إلى أسفل الصفحة وأختر المربع إلى جوار «دائمًا استخدم التصفح الآمن HTTPS».
- ملحوظة: تغيير إعدادات حسابك على تويتر إلى «دائما استخدم التصفح الآمن HTTPS» لا يفرض في الوقت الحالي التصفح الآمن HTTPS على أجهزة التليفون المحمول كذلك، وحتى معالجة هذه النقطة، عليك دائمًا الذهاب إلى https://mobile.twitter.com .

أمِّن تواجدك على الإنترنت بطرق أخرى:

- من أجل الحفاظ على هويتك سرية عند المشاركة في نشاطات النشطاء، يمكنك ابتكار أسماء مستعارة عندما تُسأل عن تعريف نفسك على الإنترنت على الشبكات الاجتماعية والمواقع الإعلامية. يرجع لك مدى درجة إخفاء هويتك: من الشائع استخدام اسم لا ينم عنك على تويتر، لكن أغلب الناس يملكون حسابات بأسمائهم الحقيقية لمواقع الشبكات الاجتماعية مثل فيسبوك. هذا يرجع لك وإلى إحساسك باحتمالية استهدافك على الإنترنت أو وقوعك فريسة للمراقبة. من المهم أن تعلم أن عليك اتخاذ اسمًا زائفًا مقنعًا على فيسبوك بدلًا من كلمة مستعارة زائفة، والتي سيلغيها فيسبوك لأن هذا خرقًا لاتفاقية شروط الخدمة الخاصة بهم.
- لو قررت استخدام اسمك الحقيقي على فيسبوك واستخدام التصفح الآمن HTTPS للدخول على الموقع أو استخدامه، فمن المهم ألا تمنح مقاطع إضافية حساسة عن بياناتك الشخصية مثل رقم هاتفك.
- هناك خيارات متزايدة لاستخدام تكنولوجيا نظام تحديد المواقع (GPS) لشرح موقعك الجغرافي أثناء تواجدك على الإنترنت. من الممكن تصبح أداة قوية عند استخدامها جزءً من حملة منسقة لرسم تقارير من على أرض الواقع باستخدام التليفون المحمول أثناء أزمة أو حدث كبير، لكنها أيضاً تعطي بيانات غاية في الحساسية عن موقعك ونشاطاتك. فنحن نوصي بغلق خصية تتبع GPS لبرامج مثل تويتر وبامبيوزر (Bambuser) إلا إذا كان ذلك بشكل مؤقت وضروري لمشروع نشط تعمل عليه. حتى لو كان GPS غير ظاهر على الشاشة، فمن الضروري إبطال جمع هذه المعلومات في متصفح الشبكة أو أي برامج أخرى.
- عندما ترسل معلومات حساسة لآخرين، ضع في اعتبارك إنهم قد لا يكونوا آمنين؛ فيمكن رصد قائمة اتصالاتهم، رسائلهم الإلكترونية، واتصالاتهم الأخرى. كن حذرًا بالأخص عند التواصل مع أطراف لم تتأكد من هويتهم بعد. بالإضافة لذلك يمكن قراءة أية رسائل مباشرة ترسلها لشخص (معروف أو مجهول) عبر فيسبوك وتويتر لو الطرف الآخر لم يأخذ خطوات معينة (اقرأ المزيد عن التصفح الآمن HTTPS وأدوات التحايل في الجهة اليمنى.)
- استخدام برامج الطرف الثالث التي تدخل على حساباتك بشكل محدود أو لا تستخدمها على الإطلاق (على سبيل المثال البرامج التي تدخل على حسابك في تويتر، وفيسبوك، وجيميل، إلخ.) فمن مساوئها ضعف العامل الأمني وتُستخدم هذه البرامج لاختراق حسابات تكون في الطبيعي مؤمنة.

التحايل: زيارة مواقع محجوبة



عدد كبير من دول المنطقة تعمل على حجب الكثير من المواقع والمدونات، ومن ثم فمن المنطقي الشك إن هذا الحجب ينم عن قدر كبير من الرقابة كذلك، على الرغم من إن مستوى الرقابة يختلف من دولة لأخرى. تستطيع استخدام أدوات التحايل لكي تزور هذه المواقع المُغلقة وتُحمِّل أي مقاطع إعلامية عليها. مهم أن تلحظ الفرق بين التشفير والخصوصية/إخفاء الهوية: تشفر أدوات التحايل الجيدة حركة المرور بين المستخدم ومانح التحايل، لكنها لا تستطيع تشفير حركة المرور بين مانح التحايل والموقع قيد الزيارة. لذلك يعد هامًا أن تستخدم التصفح الآمن HTTPS كلما أمكن ذلك، لأنه يمنح تشفير على طول الطريق من البداية حتى النهاية. لكن استخدام التصفح الآمن HTTPS وحده لن يساعدك على الولوج لموقع مُغلق ولهذا نلجأ لأدوات التحايل ونعدها مهمة. الخدمة البعيدة دائمًا تحفظ عنوان بروتوكول الإنترنت خاصتك فقط عن طريق بروكسي "proxy" مجهول (مثل تور "Tor") حيث يكون عنوان بروتوكول الإنترنت خاصتك مخبأ بالفعل بأمان. تكشف خدمات كثيرة عن آخر تسجيل دخول لك ومن ثم إذا إختُرِقَ حسابك ستنكشف أماكن تواجدك السابقة.

تجاوز جدار النار:

يسمح البروكسي للمستخدمين الوصول إلى المواقع المُغلقة عبر صفحات ويب. يزور المستخدم موقع البروكسي ويُدخل عنوان الموقع الذي يريد زيارته ويجلبه له البروكسي ويعرض الصفحة. يمرر HTTP/SOCKS proxies حركة مرور الشبكة خلال بروتوكولات تسمح بالمرور عبر الحوائط النارية «firewalls». تُدخَل عناوين بروتوكولات الإنترنت وأرقام المنافذ الموجودة على دليل مواقع البروكسي العام في تكوينات المتصفح.

على الرغم من إن البروكسيات العادية وبروكسيات HTTP/SOCKS تستخدم عادة للتحايل على الحجب، فإنها لا توفر إخفاء الهوية (استخدامك للبروكسي يمكن معرفته/ رصده) ونادرًا ما يعرف من يمنحها. هناك عدد من المخاطر المرتبطة بها ولذا فإنه يُنصَح باستخدام نظام مثل Tor، يستطيع توفير التحايل وإخفاء الهوية.

حلًا آخر يعتمد على البروكسي هو Psiphon. يأتي Psiphon بإعدادات متعددة. هو بروكسي على الويب خفيف الحجم ويعمل على أجهزة الكمبيوتر التي تعمل بنظامي تشغيل مايكروسوفت ويندوز وLinux. عادة لا تكون عُقَد Psiphon (أو ما يسمى بـ«psiphonodes») بروكسيات عامة مفتوحة. بدلًا من ذلك، فالهدف هو أن يستطيع المستخدم متوسط الخبرة بدون عدة كمبيوتر متخصصة، منح إمكانية تحايل معتمدة على بروكسي إلى مجموعة صغيرة من الأصدقاء، مقيمين في دولة أخرى تحجب المواقع. يُعرف هذا باسم نموذج شبكة الثقة «web-of-trust»؛ إذ أن «الصديق» الذي يمنح بروكسي Psiphon سيستطيع الدخول على أي حركة تمر عبر عقد Psiphonodes الخاصة بهم، ولذا يجب أن توجد ثقة بين الشخص المانح Psiphonodes وهؤلاء المستخدمين لها. يحفظ Psiphon بيانات المستخدمين، ولكنه يبقي على عناوين بروتوكولات الإنترنت (IP) مجهولة الهوية. يعد الإصدار ٢ Psiphon حلًا مركزيًا يعتمد نظام السحابية (cloud-based) وتديرها Psiphon Inc.، وتتكون من بروكسيات تعيد كتابة الروابط. يجد الإصداران ١ و ٢ من Psiphon صعوبة في التعامل مع التصفح الآمن HTTPS ومواقع Web ٢,٠. لكن عالجت النسخة الجديدة PsiphonX ذلك القصور.

TOR: إخفاء الهوية على الإنترنت

يعد Tor أداة ممتازة ومتطورة للتحايل على حجب الإنترنت ويساعدك على الحفاظ على هويتك مجهولة على الإنترنت. لكن عيبها الرئيسي أنها قد تكون أبطأ من حلول التصفح الأخرى. تتولى حزمة متصفح تورTor Browser Bundle كل الإعدادات وقد يساعد استخدام جسر تور Tor bridge في الوصول إلى المواقع المحجوبة في بيئة مكثفة الرقابة.

هناك عدة طرق لاستخدام تور *Tor*:

- أحد الطرق هي استخدام إضافة فايرفوكس Torbutton، والتي تمكنك من تشغيل Tor وأيقافه من داخل نافذة متصفح فايرفوكس. يجب عليك تثبيت Tor وتشغيله لكي يقوم بهذا. يمكنك تنزيله من هنا أو هنا ثم تعيد تشغيل فايرفوكس لتبدأ استخدامه. (ملحوظة: قد لا تعمل بعض المحتويات النشطة مثل جافاسكريبت وفلاش بصورة افتراضية لتقليل مكامن الضعف الأمنية التي قد يشتملون عليها. لمعرفة المزيد عن كيفية مخاطبة مثل تلك الجوانب، أرجو الذهاب إلى الأسئلة المتداولة عن TOR)

- يمكنك كذلك تنزيل باقة تصفح Tor، والتي تمكنك من استخدام Tor على ويندوز أو Mac OSX أو لينوكس دون الحاجة إلى تركيب أي برنامج. ممكن أن يعمل من على ذاكرة فلاش «USB flash drive» كما إنه ينزل مع متصفح شبكة مُكون مسبقًا ومستقل. للحصول على باقات التصفح المشتملة على الرسائل الفورية الآمنة أو بدونها بلغات عدة (بما في ذلك العربي والفارسية) أرجو زيارة موقع تحميل Tor

لسوء الحظ، موقع Tor الرئيسي المرتبط بالمواقع المذكورة أعلى مُغلق في أغلب دول المنطقة. لكنك تستطيع الوصول للبرنامج عن طريق:

- زيارة موقع Tor باستخدام التصفح الآمن HTTPS - https://www.torproject.org/projects/projects

- العثور في جوجل على مرآة لموقع torproject.org عبر البحث عن «tor mirror». كما يمكنك الذهاب إلى خابية جوجل "Google cache" لمعاينة القائمة الرسمية لمرايا الموقع بالبحث عن: «site:torproject.org mirrors»، ومشاهدة نتائج الخبايا لصفحة: "Tor Project: Mirrors"

- أو يمكنك طلب باقة عن طريق إرسال رسالة إلكترونية إلى «gettor» الآلي على gettor@torproject.org. ملحوظة: للحصول على أفضل آمان وأحسن نتائج، يفضل استخدام حساب جيميل محمي بواسطة التصفح الآمن، لإرسال رسالة إلكترونية إلى gettor@torproject.org. اختر أحد أسماء الحزم التالية وضعه في أي مكان داخل رسالتك الإلكترونية:

الأجهزة المحمولة

تم تتبع العديد من النشطاء عبر تليفوناتهم المحمولة. وبعض الدول تجري مراقبة بشكل أوسع عن غيرها. عانى النشطاء المصريون مراقبة عالية على كافة المستويات، واستخدمت السلطات المصرية نوع من التكنولوجيا يمكنهم من تحويل التليفونات إلى أجهزة استماع في محيطهم عن بعد، حتى لو كانوا مغلقين في ذلك الوقت. عليك أن تُقَيِّم خطورة نشاطك مع الوضع في الاعتبار ممارسات بلدك ومدى أهمية عملك، وما تعرض له الآخرون في مجموعتك. تمتلك شركات التليفون المحمول القدرة على تتبع استخدامك للتليفون المحمول وجمع المعلومات عنه، بما في ذلك معلومات عن مكانك، ومن المحتمل إشراك الحكومة في هذه المعلومات لو طُلِب منها ذلك.

هناك كذلك احتمالية تركيب برنامج مراقبة على التليفون ويعمل في الخلفية دون ملاحظة المستخدم لذلك البرنامج. يوجد خطورة لحدوث ذلك لو كان جهازك بعيدًا عن يدك فعليًا لفترة من الوقت.

عندما يعمل تليفونك، فإنه دائما يتواصل بالمعلومات الآتية مع الأبراج القريبة:

- رقم هوية المعدات المنقولة دوليًا (IMEI)- رقم يُعَين تليفونك بصورة فريدة.
- رقم هوية مشترك التليفون دوليًا (IMSI)- رقم يُعَين بطاقة SIM بصورة فريدة - رقم تليفونك موصول بهذا الرقم
- رقم هوية مشترك التليفون المؤقتة، وهو رقم مؤقت يُعاد تحديده بصفة دورية وفقًا لتغيرات الموقع أو الشبكة لكن يمكن تتبعه باستخدام أنظمة التجسس المتوفرة تجاريًا.
- خلية الشبكة الموجود بها التليفون في الوقت الحالي. يمكن للخلايا أن تغطي أية منطقة في مدى يتراوح من عدة مترات وحتى عدة كيلومترات مع وجود خلايا أصغر في الحضر وأصغر في المباني التي تستخدم إرسال مُكرر لتحسين الإشارة داخل المبنى.
- يُحَدَد موقع المشترك داخل هذه الخلية عن طريق تثليث الإشارة من سواري قريبة. مرة أخرى، دقة الموقع تعتمد على حجم الخلية - كلما زادت السواري في المنطقة، كلما أصبح تحديد الموقع أكثر دقة.

فبسبب ذلك، عندما يكون تليفونك مفتوحًا ويتواصل مع أبراج الشبكة، فيمكن استخدامه بمثابة جهاز مراقبة بواسطة الذين يدخلون على المعلومات التي تجمعها شركات الاتصالات، وذلك يشمل الآتي:

- مكالماتك التي استقبلتها وأرسلتها
- رسائلك القصيرة التي استقبلتها وأرسلتها، بما في ذلك بيانات المُرسلين والمُتلقين

- tor-im-browser-bundle for Windows (Tor & instant messaging)
- tor-browserbundle for Windows OR Intel Mac OS X OR Linux (Tor browser)
- torbutton (For Firefox add-on only)

بعد إرسال رسالتك الإلكترونية بفترة وجيزة، ستتسلم رسالة إلكترونية من «Gettor» الآلي تشتمل على البرنامج المطلوب في هيئة ملف مضغوط. لمزيد من المساعدة بخصوص Tor، ارسل رسالة إلكترونية إلى tor-assistants@torproject.org.

خيار آخر للتحايل يشفر تبادل المعلومات ويوفر إخفاء الهوية هو شبكة VPN. يمكنك قراءة المزيد عن كيفية إعداد واحدة هنا، أو تنزيل النسخة المجانية من Hotspot Shield VPN من هنا أو عن طريق إرسال رسالة إلكترونية إلى hss-sesawe@anchorfree.com (يجب أن يحتوي سطر موضوع رسالتك على الأقل على واحدة من الكلمات التالية «hss»، «sesawe»، «shield»، «hotspot»)

أدوات تحايل أخرى مستخدمة على نطاق واسع تشتمل على Ultrasurf و Freegate. تعد الأدوات الثلاث من VPN تلك أدوات جيدة للدخول على المواقع المُغلقة، لكن يجب أن تعرف أنهم مثل شبكات proxies البسيطة أو HTTP/SOCKS proxies ، فهم لا يخفون الهوية (أي إنهم لا يخفون هويتك عندما تستخدمهم.) بالإضافة إلى ذلك، معروف عن هذه الخدمات إنها تحجب وتُغلق المواقع التي لا يدعمها أو لا يشجعها مُشغلهم. كما إنه معروف عن هذه المواقع أنها تسجل بيانات دخول كل المستخدمين. فهي شركات تجارية تدر ربحها عن طريق توجيه الإعلانات لك على أساس بياناتك الشخصية (المواقع الإلكترونية التي تشاهدها، كلمات البحث التي تستخدمها، إلخ) - هذا موضوع حساس للساعين إلى إخفاء هويتهم أو ببساطة خصوصيتهم في استخدامهم لبرامج التحايل.

ملحوظة هامة: عندما تمتلك الحكومة القدرة على التحكم في خدمات الإنترنت في دولتها، يمكنهم استخدام عدة استراتيجيات أخرى للتسوية بين أمنك وسريتك عن طريق كود وحقن شهادات الأمان للتعامل مع هذا. فعليك استخدام الأدوات والطرق المذكورة أعلاه وحاول تتبع الأخبار والإنذارات من النشطاء الآخرين على الإنترنت في بلدك الذين قد يعرفون تلك الأشياء ويمنحون إنذارات مبكرة.

مزيد من الموارد: برامج تعليمية مسجلة بالفيديو عن كيفية استخدام أدوات التحايل المختلفة باللغتين الإنجليزية والعربية

(12 pm Tutorials)

الأجهزة المحمولة (تابع)

- أية خدمات بيانات تستخدمها (على سبيل المثال نشاطات متصفح الشبكة ما إذا كان يستخدم التصفح الآمن HTTPS، الدردشة الغير المؤمنة) بالإضافة إلى حجم البيانات المنقولة (على سبيل المثال «إن كنت قد حَمَّلت فيديو على يوتيوب»)
- مكانك التقريبي (في مدى يتراوح بين عدة مترات إلى عدة كيلومترات بناء على كثافة الأبراج)

من المهم ملاحظة إنك لو اعتقدت إنك مُتتبع، فلا يكفي دائمًا استبدال بطاقة SIM، إذ إنه من الممكن أن تكون مُتتبعا عن طريق هوية المعدات المنقولة دوليًا لتليفونك المحمول وحده (IMEI)

يوجد كذلك الكثير من المعلومات على تليفونك التي يمكن أن تُستخدم ضدك في حالة مصادرة التليفون أو أخذه منك. لدي كل أجهزة التليفون المحمول مساحة تخزين صغيرة على بطاقة SIM وكذلك على ذاكرة التليفون الداخلية. (بالإضافة إلى ذلك، تشتمل بعض التليفونات على كارت تخزين SD أو (micro-SD) للملفات الوسائط المتعددة (multimedia files) بوجه عام، تخزين بيانات على بطاقة SIM وكارت SD (إذا كان متاحاً) أفضل من التخزين داخليًا على التليفون، لأنك تستطيع مسح البيانات من على SIM أو ذاكرة SD وإتلافها بشكل أيسر.

تشتمل البيانات المحفوظة على بطاقة SIM، وذاكرة التليفون الداخلية، وذاكرة SD (إذا كان متاحاً) على الآتي:

- دليل تليفونك - سجل اتصالاتك وأرقام التليفونات
- تاريخ مكالماتك - بمن اتصلت، من اتصل بك، ومتى أُجريت المكالمة
- الرسائل القصيرة التي أرسلتها أو استلمتها
- بيانات من أي برنامج تستخدمه، مثل النتيجة أو قائمة المهام
- صور رقمية أو فيديو التقطه بواسطة كاميرا التليفون، لو كان تليفونك يحتوي على واحدة. أغلب التليفونات تسجل وقت أخذ الصورة وقد تحوي كذلك معلومات عن المكان.

بخصوص التليفونات التي تتيح تصفح الشبكة، يجب أن تراعي كذلك تاريخ تصفحك المحفوظ على تليفونك. لو أمكن، فلا تحتفظ بتاريخ تصفحك. فالبريد الإلكتروني خطر آخر محتمل إذا حصل المهاجم على مدخل إلى بطاقة SIM أو إلى ذاكرة التليفون.

مثل القرص الصلب في الكمبيوتر، تحفظ ذاكرة SIM في تليفونك أية بيانات عليها حتى تمتلئ ثم تبدأ البيانات الجديدة بحل محل القديمة. هذا يعني إن حتى الرسائل القصيرة وسجل المكالمات والاتصالات المسوحين يمكن استعادتهم من SIM. (يوجد برنامج مجاني لفعل هذا باستخدام قارئ البطاقة الذكية.) ينطبق نفس الشئ على التليفونات التي لديها ذاكرة إضافية، سواء كانت مدمجة في التليفون أو باستخدام كارت ذاكرة. تقول القاعدة، كلما زادت مساحة التخزين على التليفون، كلما أمكن استعادة البيانات الممسوحة منذ وقت أطول.

فماذا يعني هذا لك؟

يمكن أن تكون التليفونات المحمولة أدوات قوية للنشطاء، لكنها يمكن كذلك أن تكون عبء هائل لو كانت الحكومة أو قوات الأمن تعمل بفعالية مع شركات الاتصالات لتتبعك. لو كنت في دولة تستخدم التليفون المحمول بكثافة لمراقبة النشاطات الهامة، خاصة لو كنت تعتقد إنك مراقب عن قرب، فيُفَضل ألا تستخدم التليفونات المحمولة للتواصل، بل الأفضل أن تجري المقابلات وجهًا لوجه.

في النهاية المخاطر التي تتخذها ترجع لك: لو كنت لا تعتقد إنك مستهدف كناشط مهم أو جزء من حملة مراقبة كبرى وتريد استخدام تليفونك للتواصل مع النشطاء الآخرين، أو التقاط الصور وتسجيل الفيديو، أو تمرير المعلومات، فيمكنك استخدام النهج الآتي:

- ابتكار واستخدام نظام كلمات مشفرة للتواصل مع النشطاء الآخرين.
- استخدام «الرنة» بمثابة نظام للتواصل مع النشطاء الآخرين (الاتصال مرة أو مرتين ثم انهاء الاتصال لتخبر الشخص إنك وصلت لمكانك، أو إنك آمن، إلخ.)
- لا تستخدم الأسماء الحقيقية للنشطاء الآخرين في سجل الأسماء على تليفونك؛ اعطهم أرقام أو أسماء مستعارة. وبهذه الطريقة إذا أُخذ تليفونك أو بطاقة SIM بواسطة قوات الأمن، فلن يحصلوا على كل شبكة النشطاء الآخرين المسجلة عندك.
- احضر معك إلى المظاهرات أكثر

الأجهزة المحمولة (تابع)

من بطاقة SIM احتياطية لو تعلم إنهم يُصادرونهم ومهم أن يكون معك تليفون محمول يعمل أثناء الحدث. لوكنت مضطرًا للتخلص من بطاقة SIM، حاول إتلافها هي نفسها وليس المعلومات الموجودة عليها.

- اغلق تليفونك بكلمة سر لو كان ممكنًا فعل ذلك. ويمكن أن تكون هي رقم PIN الخاص ببطاقة SIM: تأتي بطاقة SIM برقم PIN افتراضي؛ لو أمكنك غيَّر رقم PIN الافتراضي وفَعِّل قفل PIN على بطاقة SIM. سيُطلب منك بعد ذلك إدخال كلمة سر (رقم PIN خاصتك) كل مرة تستخدم فيها تليفونك.

- لو كنت تعتقد إن المظاهرات ستُقابَل بصور قمعية متزايدة، قد تريد وضع التليفون على نمط الطيران أثناء الحدث؛ وبذلك لن تستطيع استقبال أو إرسال مكالمات، لكن مازلت تستطيع التسجيل بالفيديو والتقاط الصور وتحميلهم على مواقع الإنترنت لاحقًا. هذا النهج مفيد كذلك لو كنت تعتقد إن قوات الأمن تطارد كل من يحمل تليفونًا محمولًا أثناء الحدث. يمكن للحكومة لاحقًا طلب سجل المكالمات أو الرسائل القصيرة أو البيانات لكل الأفراد الذين تواجدوا في مكان معين من أجل القبض الجماعي.

- اغلق خاصية تتبع الموقع وتحديد الموقع الجغرافي المتاحة في برامج متعددة إلا إذا كنت تستخدم هذه الخاصية جزءًا من مشروع مستهدف لوضع علامة جغرافية على المادة الإعلامية في حدث ما بمثابة جزءًا من النشاط. لو كنت تستخدم التليفون المحمول لعرض الفيديو ، اغلق GPS أو خيار تحديد الموقع الجغرافي (إرشادات من أجل Bambuser)

- لو كان تليفونك يعمل بنظام تشغيل أندرويد (Android Operating System)، يمكنك استخدام عدة أدوات لتشفير تصفح الشبكة، والرسائل الفورية، والرسائل القصيرة، والمكالمات الصوتية عبر الأدوات المبتكرة بواسطة Guardian Project وWhispersys

- عند استخدامك تليفونك المحمول لتصفح الشبكة، استخدم التصفح الآمن HTTPS كلما أمكنك ذلك.

ملاحظة لمستخدمي Blackberry:

تمنح الشركة المصنعة لهواتف Blackberry وهي (Research In Motion(RIM نوعين من الاشتراكات بنظامي تشفير مختلفين. بالنسبة للمستهلكين الفرادى، لم يوجد قبل ذلك تشفير حقيقي بين طرفي الاتصال عبر Blackberry - حيث تستطيع شركة RIM أو شركة خدمة المحمول اعتراض المكالمات، ورسائل البريد الإلكتروني، والرسائل القصيرة، وتصفح الإنترنت، إلخ. وعلى النقيض، يحصل مستخدمو خدمة الشركات لـBlackberry على ميزة التشفير الكامل على حساب شركتهم الذي يستخدم نظامBlackBerry Enterprise (BES Server)، حيث سيصبح الإتصال عبر البريد الالكتروني، وعبر خدمة الرسائل الفورية (BBM) وعبر الويب مشفراً بالكامل. ولكن لو كنت مستخدم خدمة الشركات، خذ في اعتبارك أن المشرف على خادم شركتك، أي المشرف على قسم تكنولوجيا المعلومات في شركتك، بإمكانه فك تشفير كل اتصالاتك. كما يمكن للحكومة استخدام وسائل قانونية (وشبه قانونية) للحصول على اتصالاتك غير المشفرة.

وقد حاولت دولة الإمارات العربية، مؤخرًا، إجبار شركة RIM على إعطائها آلية فك شفرة كل مراسلات البلاك بيري، لكن شركة RIM رفضت أن تذعن لهم. ينبغي على مستخدمين البلاك بيري متابعة أخبار المفاوضات بين حكوماتهم وشركة RIM في هذا الصدد. ينبغي عليهم كذلك التنبه لأية محاولات أخرى لاعتراض اتصالات البلاك بيري المشفرة. وفي ٢٠٠٩ أرسلت شركة اتصالات في دولة الإمارات "تحديثًا" غير رسميًا مكَّن شركة الاتصالات من تسلم نسخًا من كل رسائل المستخدمين. لكن سرعان ما أرسلت شركة "رم" تحديثًا إلى المستخدمين أزال البرنامج الاحتيالي؛ لكن ينبغي على مستخدمي البلاك بيري أن يكونوا على دراية بأية تحديثات برمجية مريبة لا تأتي مباشرة من شركة "رم".

مزيد من الموارد:

Mobiles in a box Tactical Tech's (باللغة الإنجليزية)

دليل MobileActive التمهيدي لمخاطر الاتصال الخلوي الأمنية (باللغة الإنجليزية)

أخرى:

المدونات:

لو كان لديك مدونة أو تريد عمل مدونة، يوجد عدة مصادر لعمل المدونات. يجب أن يكون اهتمامك الرئيسي هو الحفاظ على هويتك آمنة والتأكد من أن الناس تستطيع قراءة مدونتك في حالة أن الحكومة حجبتها. ستجد في الآتي مزيدًا من الموارد عن إعداد موقعك وعمل مرآة له في حالة أصبح عنوانه الأصلي محجوبًا:

Anonymous blogging with wordpress and Tor (Global Voices)

Mirroring a censored wordpress blog (Global Voices)

Tips on how to blog safely (EFF)

Handbook for Bloggers (Reporters Without Borders)

تسجيل الفيديو

كتاب: فيديو للتغيير بالعربية وفيديو: كيف تبتكر فيديو للتغيير بالترجمة العربية (شاهد)

مزيد من الموارد عن الأمن والنشاط الرقمي:

Tactical Tech & FrontLine - Security in a Box: عربي إنجليزي

مؤسسة الجبهة الإلكترونية- دليل مُفصل: الدفاع عن النفس ضد المراقبة وموجز

الطبعة الدولية للدفاع عن النفس ضد المراقبة (كلاهما باللغة الإنجليزية.)