دليل الأمان في الفضاء الإلكتروني

تصدره الجمعية الدولية للصحف وناشري الأخبار

للمنتدى العربي للصحافة الحرة AFPF

نوفمبر 2013

بقلم آلان بيرس

إن أرادت الجهات التنفيذية أو أجهزة المخابرات مراقبة نشاط شخص ما على الانترنت– قراءة بريده الإلكتروني وملصقاته على مواقع التواصل الاجتماعي، أو السطو على قوائم اتصالاته، أو معرفة عن ماذا يبحث وماذا يُحمّل، والتنصت على مكالماته الهاتفية– فهم يستطيعون، بغض النظر عن تفاصيل أوامر المحكمة وأذن النيابة. ما يعني أن كل شيء طرّاً تحت الرقابة.

بصفة عامة، يمكنهم الدخول على أجهزة الكمبيوتر والهواتف الذكية بما يسمى "الهندسة الاجتماعية". فن جذب المستخدمين لمواقع كيدية حيث يتم خداعهم بجعلهم يفصحون عن معلومات سرية أو بزرع برمجيات ضارة في أنظمتهم وعلى بريدهم الالكتروني تُعرف بـ "تحميل حادثة طريق– drive-by download".

احذر من مراسلات التواصل الاجتماعي والرسائل الإلكترونية التي تتضمن وصلات قد تكون ملفتة، حيث يتم اختصار الكثير منها أحياناً لئلا تعرف إلى أين تتجه. يمكن تكبير الوصلة المختصرة على longurl.org (موقع يمكن من التعرف على أصل الوصلة المختصرة ويتجنب الفيروسات والبرامج الخبيثة).

أبداً لا تفتح ملف مرفق أو تضغط على وصلة إن لم تكن واثقاً من أصلها. إن كان لابد من فتح ملف مرفق مشتبه فيه، قم بقطع اتصال الانترنت أولاً، ثم اعد تشغيله بنظام حماية sandbox مضاد للفيروسات.

إن كان من عادتك قراءة ملفات حساسة وتشك في كونك تحت رقابة ما. استخدم في قارءة تلك الملفات جهاز كمبيوتر منفصل غير متصل بالانترنت، أسلوب يُعرف بـ "صنع فجوة هوائية– air-gapping".

يجب تأمين شبكتي الانترنت اللاسلكي بالعمل والمنزل بتغيير كلمة سر رجل الإدارة الخاصة بجهاز التوجيه (الراوتر).
من السهل دائما لفت الانتباه بالبحث عن موضوعات شائكة على الانترنت أو إن كنت ببساطة مسجلاً في قائمة اتصالات أحد المشتبه فيهم.

فجأة يغدو التواجد على الانترنت خطر جسيم على الصحفيين. مع ذلك فبالانتباه جيداً للمخاطر واستخدام مجموعة من الأدوات والتقنيات المذكورة أدناه، يمكنك مبدئياً البقاء خلف خط الرادار دون أن تلفت الأنظار.

عند اختيار كلمة السر، اختر جملة يمكنك تذكرها بدلاً من كلمة يمكن البحث عنها في القاموس. مثال: أنا احب خل كثير على السمك والبطاطس، لأنها ستُكتب هكذا: (أناأحبخلكثيرعلىالسمكوالبطاطس). اضف لها بعض الأشكال التي ليست بحروف ولا بأرقام مع شرطات علوية وسفلية، وذلك لجعل كسرها بقوة دخيلة أمراً في غاية الصعوبة.

إن لم يكن ذلك بعد فوات الأوان، لا تدون أية معلومات شخصية على شبكات التواصل الاجتماعي– لا تاريخ ميلاد، ولا قرابات عائلية، ولا محل الإقامة، ولا خطط السفر، ولا صور شخصية، إلى آخره.

بصفة عامة، يُفضّل استخدام البرامج مفتوحة المصدر، المجانية، على تلك التي تشتري على الانترنت، لأنها تخضع لاختبار المطورين ويمكن تحديد أي جهاز تسجيل أو تسلل. يجب التعامل مع جميع البرامج المشفرة الملكية بأعلى درجة من الحرص.

جميع الوصلات المذكورة في هذا الدليل يمكن فتحها على متصفح الانترنت خاصتك. أما وصلات الموقع العميق Deep Web التي تتضمن هذه العلامة <!> فلا يمكن فتحها إلا بمتصفح تور فيرفكس Tor-Firefox الذي ستتعلم استخدامه من هنا.

اعلم انه لا يوجد نظام أو برنامج واحد آمن أو سليم بنسبة مائة في المائة.

إعدادات الدفاع

يمكن القول أن أكثر برامج التصفح احتراماً لأمان المستخدم هو موزيلا فيرفكس. نسخته العربية متاحة هنا.

لكن قبل استخدامه، يجب أن تقضي عدة دقائق في ضبط *الإعدادات:*

- **اضغط على لوجو فيرفكس واختر من الشريط الأعلى** *أدوات* **ومنها** خيارات
- **في خيار** *الخصوصية* **تحت بند** *التعقب* **ضع علامة على مربع** *اخبر المواقع إنني لا أريدها أن تتعقبني.*. **تحت بند** *التأريخ* **اختر** *يستخدم إعدادات مخصصة للتأريخ*، **ضع علامة على** *استخدم نمط التصفح الخاص دائماً*. **زِل العلامة عن مربع** *اقبل الكعكات من المواقع*. **قد تختار** *لن يتذكر التأريخ أبداً*. **وقد ترغب أيضاً بأن** *تمسح تأريخك الحالي كله*.
- **في خيار** *الأمان*. **اختر** *حذرني عندما يحاول موقع تثبيت إضافات*، **ثم احذف جميع الاستثناءات. ضع علامة على** *احجب مواقع الهجمات المبلغ عنها*، **وعلى** *احجب تزويرات الويب المبلغ عنها*، **وزل العلامة عن** *تذكر كلمات سر المواقع*.
- **في خيار** *متقدم*، **تحت بند** *عام* **اختر** *حذرني عندما تحاول مواقع وب إعادة توجيه أو تحميل الصفحة*. **تحت بند** *الشبكة* **ضع علامة على** *نبهني عندما يطلب موقع تخزين بيانات للاستخدام دون اتصال*، **وعلامة على** *تجاهل الإدارة الآلية للذاكرة الخبيئة* **أو اضبط العداد استعمال مساحة الذاكرة الخبيئة على 0.**

يوجد عدد من إضافات الأمان المجانية لبرنامج فيرفكس. قم بتثبيت الآتي منها:

HTTPS Finder أو HTTP Everywhere
Do Not Track Me
BetterPrivacy
QuickJava
DownThemAll

لا تستخدم محرك البحث جوجل في البحث عن موضوعات شائكة، بدلا منه استخدم Secret Search Labs **أو** iXQuick
لتصفح سريع ومجهول المصدر استخدم AllNetToo **أو** Guardster **أو** Anonymouse.
من الشبكات الافتراضية الخاصة المجانية **VPN:** FreeVPN **و** ProxPN.
امسح آثار تعقبك بـ CCleaner **واحذف البيانات الحساسة تماماً بـ** Heidi Eraser.
ثبت برنامج مضاد للفيروسات مجانا من على AVG **أو** Avast.

استخدام تور

تور شبكة مخبئة للويب العميق حيث يتم تشفير وتقنيع هوية المستخدمين ومواقعهم، مما يوفر تخفي جيداً للغاية. ابدأ بتنزيل حزمة تور فيرفكس Tor/Firefox bundle . النسخة العربية منها متاحة هنا. ويسهل تنزيلها وتثبيتها. فقط اتبع التعليمات الظاهرة على الشاشة وستفتح لك بوابات للويب العميق خلال دقائق ودون أن يتطلب الأمر أية مهارات خاصة.
كذلك، أضف منفذ وصلات HTTPS enforcer مثل HTTPS Everywhere. **وأضف أيضاً** Do Not Track Me.
في الصفحة الافتتاحية حيث يقول "*رقم الآي بي الخاص بك يظهر كالتالي.....*" ثمة عدة أرقام لا يمكن أن يكون لها علاقة بحاسوبك بأي حال من الأحوال. أنت الآن مجهول وبوسعك تصفح تور أو التفرع إلى تصفح الويب بأقل قدر ممكن من مخاطر المراقبة.

نقاط الدخول للويب العميق

- **الويكي المخبأة**

<!> http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page

- **فهرس تور**

<!> dppmfxaacucguzpc.onion

- روابط تور

<!> torlinkbgs6aabns.onion

- منتدى مساعدة تور

<!> http://zntpwh6qmsbvek6p.onion/forum/

إذا واجهتك صعوبة في الدخول على أحد المواقع في الويب العميق، عاود المحاولة بعد وقت وقد يفتح. يمكن التحقق من إتاحة موقع ما في الويب العميق بواسطة ***Is it up?*** من هذا الرابط:

<!> http://zw3crggtadila2sg.onion/downornot/

للأمان الفائق، ادخل على شبكة تور من محرك USP، أو كارت SD، أو سي دي، أو دي في دي، أو قرص صلب محمول، يمكن استخدام أي من هذه الأدوات على أي حاسوب متصل بالانترنت. قم بثبيت شبكة تور/فيرفكس والبرامج المفيدة الأخرى على الأداة مباشرة.

اقتراحات بتطبيقات مجانية قابلة للنقل

- PortableApps.com – مجموعة متنوعة من البرامج مفتوحة المصدر للأجهزة الناقلة
- KeePass Portable
- Notepad Portable Text Editor
- VLC Media Player Portable
- IrfanView Portable
- GIMP Portable
- Sumatra PDF Portable
- Eraser Portable
- Zip Portable-7

وسائل اتصالات آمنة

البريد الالكتروني: استمر في استخدام بريدك الالكتروني المعروف في الاستخدامات العامة ليكون لدى أجهزة الرقابة شيء ما لتراقبه ولئلا تثير الشكوك باختفاءك. للمراسلات الحساسة استخدم شبكة تور أو شبكة افتراضية خاصة **VPN** وسجل باسم مستعار في أي من مواقع البريد الإلكتروني المجانية (تجنب شركات مثل الهوت ميل أو الجي ميل، وما شابه). حاول أن تستخدم كمبيوتر منفصل لعمل هذه الإجراءات. كذلك يمكن تشفير البريد الالكتروني داخل الرسالة، وأن يرفق بها أي ملف، لكن ذلك في حد ذاته قد يلفت الانتباه. اوقف أيضاً خاصية صفحة *HTML* من إعدادات بريدك الالكتروني واضبطه على صفحة خالية *plaintext*

المراسلات السرية:

- PrivNote رسائل مجانية تدمر نفسها ذاتياً.
- SpamMimic تحول الرسائل البسيطة إلى نصوص غير مرغوب فيها spamtext.
- PasteOnion يلصق ويشارك النصوص والصور وما إلى ذلك على الموقع العميق.

<!> http://xqz3u5drneuzhaeo.onion/users/boi/

المراسلات الخاصة:

- Tor*PM* <!> http://4eiruntyxxbgfv7o.onion/pm/.
- Simple*PM* <!> http://4v6veu7nsxklglnu.onion/SimplePM.php

الدردشة على الموقع العميق:

- تور شات

<!> http://lotjbov3gzzf23hc.onion/index.php/group/torchat

- برنامج دردشة فوري نِدّ لِندّ EFG Chat

<!> http://xqz3u5drneuzhaeo.onion/users/efgchat/index.php?chat=lobby

التواصل الاجتماعي على الموقع العميق:

- تور ستيتوس نت

<!> http://lotjbov3gzzf23hc.onion/

- تور كتب

<!> http://ay5kwknh6znfmcbb.onion/torbook/

- تور سكوير

<!> http://ay5kwknh6znfmcbb.onion/torsquare/

الهواتف الذكية والمحمول

أبداً لا تترك هاتفك الذكي أو أي جهاز رقمي آخر خاصتك بعيداً عن عينيك. إن أراد مسئول أو أي شخص آخر فحصه، لا تتركهم وحدهم وهم يفعلون ذلك. وبنفس القدر من الحرص انتبه جيداً أين تعيد شحن هاتفك لأن الأمر لا يستغرق سوى ثواني قليلة لإدخال برنامج تجسس لهذه الأجهزة.

لمستخدمي الأندرويد ثمة خيار جيد ومجاني لحمايته من البرامج الخبيثة وبرامج الجاسوسية وهو AVG Mobilation كذلك يحمي برنامج Lookout نظم التشغيل الشخصية iOS، أو الأندرويد، من شبكات الانترنت اللاسلكي غير الآمنة، والتطبيقات الخبيثة والوصلات المخادعة، وما شابه.

تساعد الشبكات الافتراضية الخاصة المحمولة على إخفاءك وسط العامة. يقوم برنامج Hotspot Shield بتشفير الحركة المرورية للهواتف الذكية من خلال شبكة افتراضية خاصة ليخفي هويتك ويمنع التعقب، وكذلك يتيح لك مشاهدة المحتوى المحجوب والدخول على موقعي تويتر والفيسبوك بواسطة المحمول في حال منعهما محلياً.

- ضع كود تأمين على هاتفك الذكي بالإضافة لكود الشريحة وشغل خاصية الإقفال التلقائي
- أوقف اتصال الشبكة واغلق الاتصالات العابرة، ولا تنشر اسمك على خاصية البلوتوث واوقف الاتصال التلقائي بالانترنت اللاسلكي.
- من *إعدادات* الهاتف، أوقف خاصيتي تحديد الموقع والـ GPS.
- حيثما أمكن، يفضل الدخول على شبكات 3G ،2G، أو 4G بدلاً من الشبكات اللاسلكية المجانية.
- عند تغطية المظاهرات، أو ما شابه، بدّل كارت الذاكرة الخاص بالموبايل بآخر احتياطي لا يحوي أية بيانات أو اتصالات شخصية في حال إذا ما تم القبض عليك. كذلك شغل هاتفك على وضع الطيران لتجنب تعقبك.
- تجنب توصيل أجهزة شخصية لشبكة أو حاسوب المكتب.
- قم بتحديث النظم بانتظام ليبقي نظام التشغيل ملاحقاً للتجديدات التأمينية.
- انزع البطارية أو اترك هاتفك حين تكون مع آخرين أو مع المسجلين في قائمة اتصالاتك أو ماشابه.

تطبيقات الأمان

بإمكانك أخذ هاتفك الذكي إلى شبكة تور وإبعاد كل ما به عن مؤشر الرادار باستخدام تطبيقات خاصة بكل من أندرويد و نظم التشغيل الشخصية iOS لها إمكانية الدخول على كل من الويب العميق والويب السطحي، بالإضافة للرسائل الخاصة PM والبريد الإلكتروني دون أن تتم مراقبتك أو حجبك.

- **برنامج رسائل سري–** Heml.is **تطبيق يؤمن نظام الرسائل للآي فون والأندرويد.** تطبيق رسائل قصيرة سرية لنظم التشغيل الشخصية iOS **يقوم بتشفير الرسائل بين المستخدمين وإخفاءها.**
- **كاميرات سرية–** مسجل فيديو سري للمحترفين لأندرويد **و** نظم التشغيل الشخصية iOS. كاميرا سرية لنظم التشغيل الشخصية iOS **و** كاميرا خفية لأندرويد.
- **مسجل سري–** مسجل صوت سري لأندرويد ومسجل جاسوس لنظم التشغيل الشخصية iOS.
- **مسجل مكالمات–** مسجل مكالمات فائق السرية لأندرويد ومسجل مكالمات محترف لنظم التشغيل الشخصية iOS.
- **خزانة سرية–** مجلدات سرية لأندرويد ونظم التشغيل الشخصية iOS.
- **محو الدليل–** توجد آليات تمزيق لأندرويد ونظم التشغيل الشخصية iOS.

إخفاء وتداول البيانات السرية

- Onion File Hosting: <!> http://f4om2jzqkad5zpxv.onion/hosting/login
- Anonyshares <!> http://4eiruntyxxbgfv7o.onion/anonyshares.html
- Onion File Sharing - <!> http://f3ew3p7s6lbftqm5.onion/
- TORage - <!> http://utovvyhaflle76gh.onion/
- QicPic <!> http://xqz3u5drneuzhaeo.onion/users/qicpic/
- OneSwarm
- Pastebin

برامج مجانية مقترحة

- Comodo Personal Firewall
- Lavasoft's Ad-Aware
- Spybot Search and Destroy
- Anti-Trojans
- Crap Cleaner
- Avast Free Antivirus
- AVG Anti-Virus Free Edition