cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

العدد ٥
أبريل/نيسان ٢٠١٣

- ماهي الرقابة على الإنترنت؟
- إلى أي مدى استعمال سكايب آمن؟
- تحسينات على إعدادات الخصوصية على فيس بوك
- محركات بحث بديلة
- حذف الملفات نهائياً

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

للإتصال بنا:

magazine@cyber-arabs.com

تابعنا على:

مقدمة

سوزان فيشر

يشكّل الأمن الرقمي هماً كبيراً بالنسبة إلى كل من يستعمل جهاز حاسوب عادي أو حاسوب لوحي «تابلِت» أو هاتف ذكي، وبالطبع، يشكل هماً أيضاً لكل من يستعمل الإنترنت. إذا كنتم خائفين من أن حكومتكم قد تكون تتجسس عليكم، يصبح عندها الهمّ أكبر.

لذا، فمن غير المفاجئ أن يزداد عدد متابعي موقع «سايبر آرابز» بهدف الوقوف على آخر التهديدات الأمنية والتطورات في المجال الرقمي. تحظى صفحتنا التفاعلية على موقع فيس بوك بأكثر من ١١,٠٠٠ معجب عبر العالم العربي، أي ١١,٠٠٠ شخص يبحثون عن النصيحة حول إبقاء بياناتهم واتصالاتهم بأمان.

نقدم في صفحتنا على موقع فيس بوك دعماً لكل شخص على حِدة، فدعونا نعلم بشأن أي سؤال أو يخطر على بالكم أو أي شيء يقلقكم، يمكنكم التواصل معنا بواسطة رسالة على موقعنا أو على فيس بوك، وسنحاول أن نساعدكم في أسرع وقت ممكن. ستجدون على صفحتنا في فيس بوك آخر الأخبار بشأن الهجمات الخبيثة والثغرات الأمنية وتحذيرات بشأن تصيد المعلومات عبر الإنترنت، بالإضافة إلى مخاطر أخرى.

المخاطر كثيرة، فنحن نعرف أن الحكومات القمعية تسعى إلى إيجاد سبل ليس لكي تسيطر على عقول الناس فحسب، بل أيضاً لتسيطر على اتصالاتهم ونفاذهم إلى المعلومات. ولا تنسوا أن ذلك لا ينطبق على جهاز الحاسوب الخاص بكم فحسب، بل أحياناً يمتد أيضاً ليشمل هاتفكم الجوال.

هذا الخطر يدفع العدد الخامس من مجلة «سايبر آرابز» إلى طرح ما يلي: إلى أي درجة تعد الهواتف الجوالة آمنة؟ إلى أي درجة يمكن اعتبار التشفير في هواتف «أندرويد» آمناً، لا سيما وأن استعمال هذا النوع من الهواتف في العالم العربي يزداد بشكل مستمر؟ في هذا العدد، سنتحقق أيضاً من درجة الأمان التي تتمتع بها إحدى أكثر أدوات الاتصال عبر الانترنت استعمالاً، وهي سكايب؛ هل هي حقاً أداة آمنة؟ وبالطبع، لا يمكن لأي عدد من مجلة «سايبر آرابز» أن يتجاهل أهمية فيس بوك بالنسبة إلى النشطاء في العالم العربي، والتي لا تنفك تزداد. سننظر هذه المرة في موضوع التعرف إلى الوجوه والمزايا الأمنية الجديدة التي تتمتع بها هذه الشبكة الكبيرة للتواصل الاجتماعي.

نأمل أن تساعدكم قراءة هذا العدد من «سايبر آرابز» على البقاء آمنين، وكالعادة، ننتظر ردكم وتعليقاتكم.

سوزان فيشر
مديرة برنامج الشرق الأوسط
«معهد صحافة الحرب والسلام»
(IWPR)

التشفير بواسطة AES Crypt

يمتلك الجميع ملفات يفضلون عدم مشاركتها مع الآخرين ويفضلون حمايتها بطريقة آمنة، وقد يتضمن ذلك صور ومقاطع فيديو، أونصوص أو أنواع أخرى من الملفات.

للحرص على عدم وقوع هذه الملفات في الأيدي الخطأ، يمكنكم أن تشفّروا هذه الملفات، ويعني ذلك أن محتواها يصبح غير مقروء لأي شخص لا يملك كلمة السر لفتح الملف.

شرحنا في مقالات سابقة كيفية تشفير الملفات باستخدام برنامج TrueCrypt (الرابط). يعتبر TrueCrypt مفيداً بشكل خاص في حال أردتم أن تنشئوا سواقة افتراضية تحفظ كل ملفاتكم السرية. إلا أن في بعض الأحيان قد تريدون أن تشفروا ملفاً واحداً فقط، على سبيل المثال إذا أردتم أن ترسلوا ملفاً عبر البريد الإلكتروني بشكل آمن.

لبلوغ هذه الغاية يمكنكم أن تستخدموا تطبيقاً اسمه AES Crypt، ويعني الاسم «معيار التشفير المتقدم». هذا التطبيق سهل الاستخدام ويمكن تشغيله من سطح المكتب في الحاسوب لأنه يصبح جزءاً من القائمة التي تظهر عند النقر على الملف بالزر الأيمن من الفأرة، من دون الحاجة إلى إطلاقه كبقية التطبيقات التقليدية.

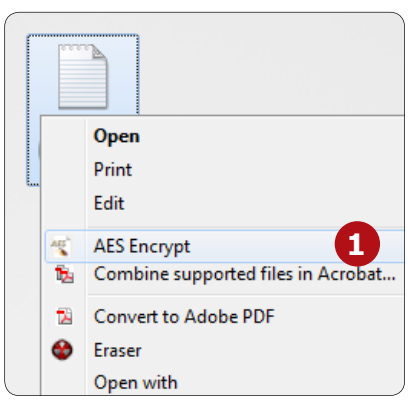
بعد تحميل AES Crypt هنا، افتحوا الملف المضغوط وشغّلوا ملف التهيئة (setup.exe) ستبدأ عندها عملية التنصيب، وهي عملية سهلة وسريعة.
ليس من الضروري أن تكونوا خبراء لكي تستعملوا AES Crypt في ويندوز. كل ما تحتاجون إلى فعله هو النقر بالزر الأيمن على الملف، ثم النقر على خيار «AES Encrypt» ومن ثم إدخال كلمة السر التي تختارونها.

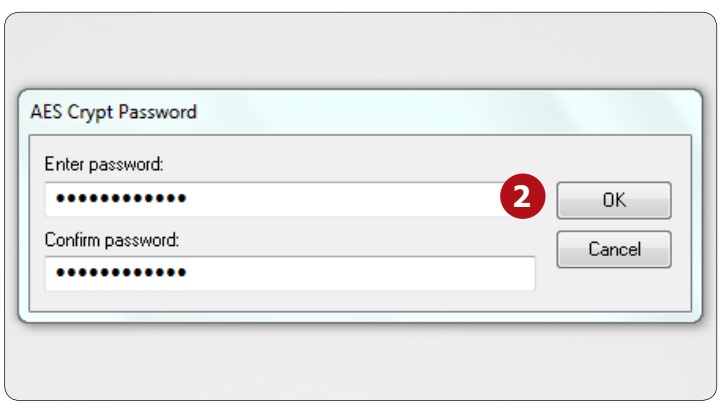
يمكنكم أن تقرؤوا هنا كيف تختارون أفضل كلمة سر ممكنة.

سينتج AES Crypt ملفاً لا يتمكن أي شخص من قراءته إذا لم يكن يعرف كلمة السر. إذا أردتم أن تحصلوا على عدة ملفات مشفرة ومضغوطة في آن واحد، يمكنكم استخدام أحد برامج ضغط الملفات وتضغطوا عدة ملفات لتحصلوا على ملف له لاحقة مثل ZIP. أو 7Z. أو RAR. ومن ثم تقومون بتشفيره. إذا أردتم أن تستعملوا AES Crypt لكي تستبدلوا ملفاتكم بأخرى مشفرة، عليكم أن تعلموا أن التشفير بهذا البرنامج لا يستبدل الملفات الأصلية بأخرى مشفرة، لذلك عليكم حذف الملفات الاصلية يدوياً بعد التشفير. لاتباع الطريقة المثلى لكي تزيلوا الملفات بأمان، إقرؤوا هذا المقال هنا.

فك تشفير الملفات هو بسهولة عملية التشفير نفسها؛ ما عليكم سوى النقر بالزر الأيمن من الفأرة على الملف المشفّر واختيار «AES Decrypt» وإدخال كلمة السر بعد ذلك.

لزيادة درجة الأمان، يمكنكم أن تغيروا إسم الملف إلى اسم لا يوحي بأنه مشفر، وذلك عبر إضافة لواحق مثل mpg. أو jpg. ولكن، يجب أن تعرفوا أنه من الضروري إعادة اللاحقة aes. لكي يتمكن تطبيق AES Crypt من التعرف إلى الملف وفك تشفيره.





محركات بحث بديلة

أصبحت محركات البحث الأدوات الأكثر أهمية في مجال الانترنت، فدون محرك جوجل (Google) أو محرك بينغ من مايكروسوفت (Microsoft's Bing) تغدو الانترنت مجرد مجموعة من الصفحات دون فهرس. إلا أن معظم محركات البحث تقوم أيضاً بجمع معلومات خاصة عن مستخدميها، مثل سلوكهم البحثي، وأماكن تواجدهم، وعناوين بروتوكولات الانترنت (IP address) التي يستخدمونها، إضافة إلى تفاعلهم مع مواقع التواصل الاجتماعي، وذلك بهدف تحسين نتائج البحث التي يحصل عليها هؤلاء المستخدمون. تستخدم محركات البحث هذه المعلومات لجعل نتائج البحث التي تحصلون عليها تتناسب والمعلومات التي تم جمعها عنكم، ولهذا السبب يحصل كل شخص على مجموعة مختلفة من نتائج البحث.

جرّبوا بأنفسكم!

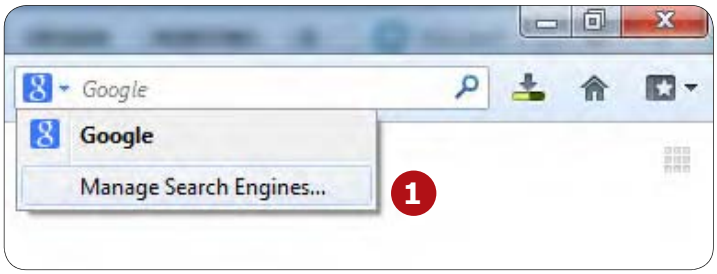
ورغم أن المعلومات التي تجمعها عنكم محركات البحث قد لا تكون حساسة إلا أن الأمر يثير مخاوف أمنية حقيقية، لأنّ تخزين بعض هذه البيانات يتم على حواسيبكم على شكل سجلات تتبع (أو كوكيز Cookies) من السهل الوصول إليها، كما تقوم هذه المواقع بمشاركة بيانات أخرى مع أطراف ثالثة غير معروفة لمستخدمي محركات البحث.

ولهذا السبب، ينصحكم موقع سايبر آرابز باستخدام محركات البحث التي لا تتعقب معلوماتكم أو تشاركها أو تقوم ببيعها. وأحد المحركات هذه هو دك دك جو www.duckduckgo.com الذي يضع الخصوصية أولاً، ولذا فهو لا يقوم بتخزين عناوين بروتوكولات الانترنت المستخدمة أو تسجيل معلومات المستخدم ولا يلجأ إلى استخدام الكوكيز إلا عند الضرورة. كما ننصحكم بمحرك بحث آخر هو ستارت بيج www.startpage.com الذي يستخدم محرك جوجل للبحث لكن دون جمع بياناتكم الخاصة أو مشاركتها مع أطراف ثالثة.

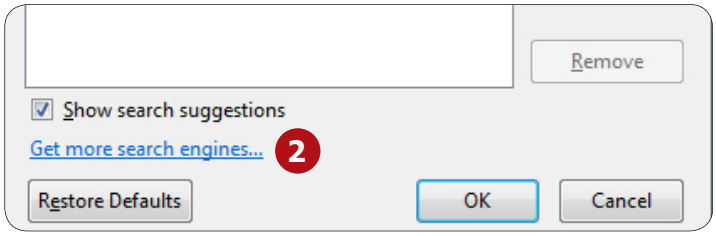
لإضافة أحد محركي البحث إلى متصفحك وجعله الافتراضي قم بالخطوات التالية:

متصفح فايرفوكس:

١- قم بالضغط على السهم الموجود بجانب مربع البحث في الأعلى ثم الضغط على Manage Search Engines

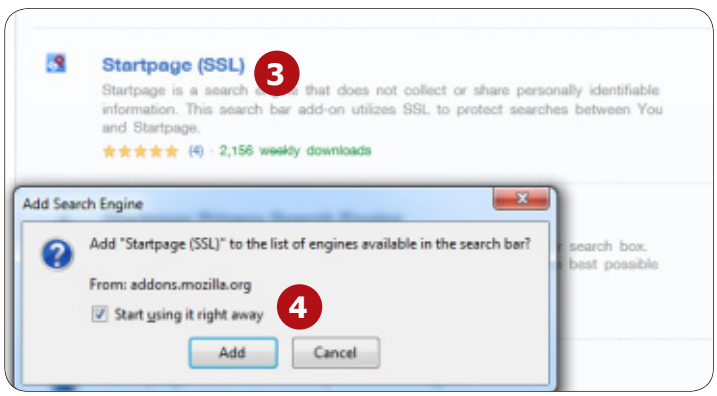


٢- قم بالضغط على Get more search engines



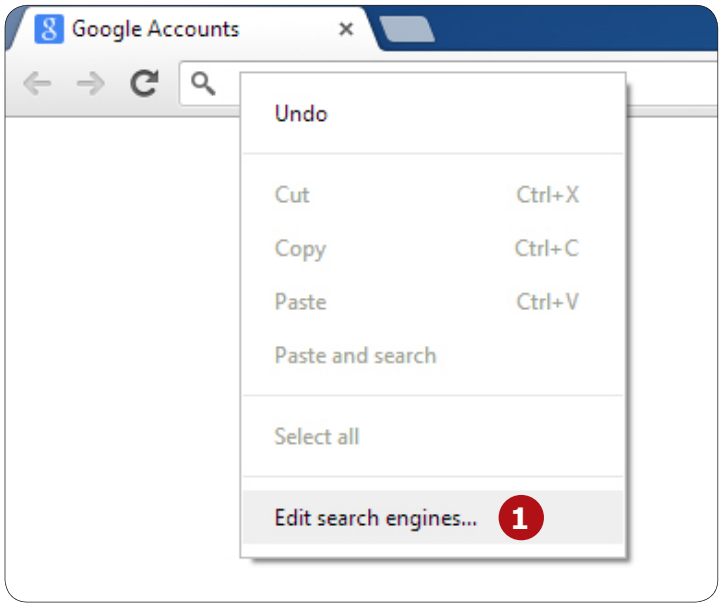
٣- قم بالبحث عن DuckDuckGo (HTTPS / SSL) أو Startpage (SSL) ثم قم بالضغط على Add to firefox

٤- سيظهر لك مربع للتأكيد على إضافة محرك البحث، قم بوضع إشارة صح على Start using it right away لجعله محرك البحث الإفتراضي لديك ثم الضغط على Add.



متصفح كروم:

١- قم بالضغط بالزر اليمين على شريط العنوان وقم باختيار Edit search engines



٢- في خانة Add new search engine قم بإدخال اسم محرك البحث (مثلاً: Startpage)

٣- في خانة Keyword قم بإدخال اسم محرك البحث أيضاً

٤- في خانة URL with %s in place of query قم بوضع الرابط التالي:

أ- Startpage:

https://startpage.com/do/search?cmd=process_search&cat=web&query=%s

ب- Duckduckgo:

https://duckduckgo.com/?q=%s

٥- بعد وضع محرك البحث المراد استخدامه قم بالضغط على Done

٦- قم بإعادة الخطوة رقم (١) والضغط على زر Make default الظاهر بجانب محرك البحث الذي قمت بإضافته

التعرف إلى الوجوه في فيس بوك

أعلن موقع فيس بوك أنه بصدد اعتماد خدمة جديدة تقوم باقتراح وسم الصور (Photo Tags) بشكل تلقائي، وذلك من خلال البرمجية المتقدمة التي يستخدمه الموقع والتي تتيح التعرف إلى الوجوه. ستدخل هذه الخدمة في حيز الاستعمال خلال الأشهر القليلة المقبلة. ونتيجةً لذلك، سيكون أمام المستخدمين اقتراحات لوسم الأشخاص الذين يظهرون في الصور.

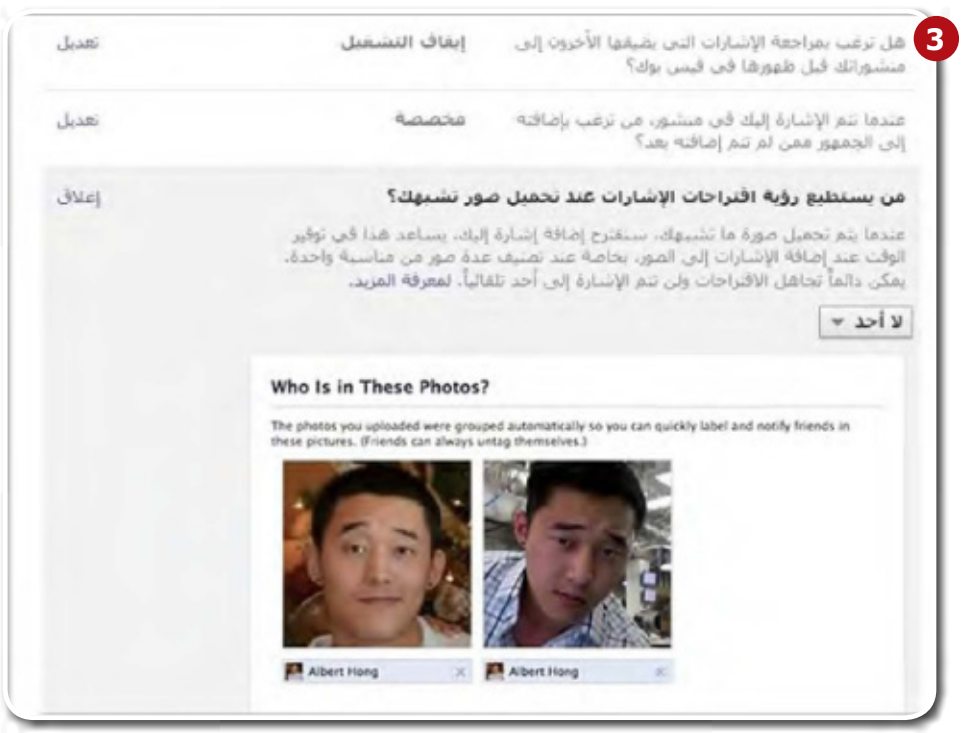
هذه الخدمة لا تقوم بشيء لا تستطعيون القيام به بأنفسكم، فهي تقترح الإسم وتنتظر موافقتكم. سيخبركم فيس بوك أنه تمّت الإشارة إليكم لكي تتسنى لكم فرصة إزالتها، إلا أنه لن يدعكم الاختيار في بادئ الأمر، مع أنه يدّعي معرفة هويتكم.

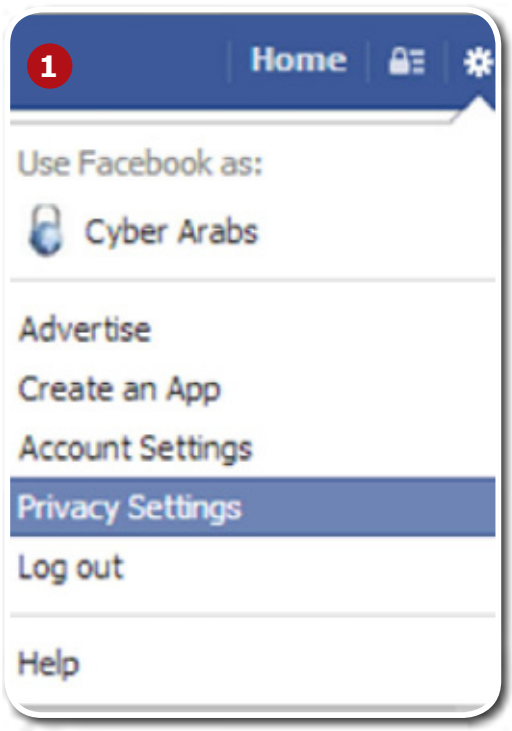
بالإضافة إلى ذلك، في حال كنتم صحافيين أو ناشطين تعيشون في دولة سلطوية، سيعرّضكم التعرف إلى وجوهكم بشكل تلقائي لظروف غير مرغوبة. فقد يستخدم الأشخاص ذوو الغايات الخبيثة هذه الأداة للتعرف إلى هويتكم في صور التقطت في مظاهرات أو نشاطات أخرى مشابهة. لهذه الأسباب، ينصحكم فريق سايبر آرابز أن تعطلوا هذه الميزة في حساب فيس بوك الخاص بكم.

١- لتتمكنوا من فعل ذلك، أنقروا على الأيقونة التي تحمل رمز الدولاب ومن ثم اختاروا «إعدادات الخصوصية» من القائمة.

٢- توجهوا بعدها إلى القائمة على الجهة اليمنى (إذا كنتم تستخدمون فيس بوك باللغة الانجليزية ستكون هذه القائمة على الجهة اليسرى) وانقروا على «اليوميات والإشارة».

٣- والآن راجعوا إعداداتكم، بما في ذلك خيار «كيف يمكنني إدارة الإشارات التي يضيفها الأشخاص واقتراحات الإشارات؟» تحت هذا الخيار راجعوا الإعدادات الخاصة بـ «من يستطيع رؤية اقتراحات الإشارة عند تحميل صور تشبهك؟» غيّروا هذا الإعداد من «الأصدقاء» إلى «لا أحد». تمت العمليّة!





تحسينات على إعدادات الخصوصية على فيس بوك

لطالما كانت خصوصية مستخدمي فيس بوك من المواضيع المهمة في سايبر آرابز (Cyber Arabs)، فمن المعروف أن إعدادت الخصوصية على فيس بوك مخبأة، إضافة إلى صعوبة التعامل معها، مما يؤدي في كثير من الأحيان إلى حالات لا يرغبها مستخدمو الموقع. غير أنّ فيس بوك قد استمع، على ما يبدو، إلى الشكاوى الكثيرة، وبدأ خلال الشهر الماضي بالقيام بسلسلة من التحسينات لجعل التعامل مع إعدادت الخصوصية أسهل.

وتشمل هذه التحسينات اختصارات الخصوصية التي يمكن الوصول إليها من القائمة المنسدلة في الصفحة الرئيسية، وبعضَ التغييرات الطفيفة على تصميم سجل النشاطات، وأداة جديدة لطلب إلغاء الإشارة إليكم في مجموعة من الصور. كما أضاف فيس بوك ملاحظات تعليمية جديدة تسهل عليكم فهم آلية التحكم بما تشاركونه؛ فعلى سبيل المثال، سيُذكّر فيس بوك مستخدميه أنه ما زال من الممكن أن تظهر المواد المخفية في يومياتهم في آخر الأخبار، والبحث، وأماكن أخرى.

إلا أنّ التغيير الأوضح للعيان هو اختصارات الخصوصية، فقد وضع فيس بوك أيقونة جديدة على شكل قفل إلى جانب أيقونة الصفحة الرئيسية في الزاوية العليا اليسرى من القائمة المنسدلة. ومن خلال هذا الخيار الجديد، أصبح بالإمكان الوصول بسرعة إلى الإعدادت التالية: «من يستطيع رؤية محتواي؟»، «من يستطيع الاتصال بي؟»، و«كيف أمنع أحد من مضايقتي؟»

حتى هذه اللحظة، كان تعديل إعدادات الخصوصية والتحكم باليوميات يتطلب من المستخدمين التنقل بين مجموعة من الصفحات المنفصلة، ولكن، ومع قائمة إعدادات الخصوصية الجديدة، أصبحت الآن الإعدادت الأكثر أهمية بمتناول اليد، كما أنه ما زال يمكن الإطلاع على الصفحة القديمة للتعرف على تفاصيل التغييرات في الإعدادات. هذا وتجدون المزيد من المعلومات حول هذه الموضوع في كتيب فيس بوك على موقع سايبر آرابز (يمكن الوصول إلى الكتيب من خلال رابط على الموقع).

ومن الخيارات الجديدة التي تم طرحها مؤخراً شريط «صور لك» الذي يُمكّنكم من اختيار عدد من الصور والطلب من أصدقائكم أن يزيلوا الصور التي لاتريدون أن يُشار إليكم فيها. ويمكن العثور على هذا الخيار تحت «الصور» في الجانب الأيمن من الشاشة بعد النقر على «سجل النشاطات» في صفحتكم الخاصة، وسيكون بإمكانكم إرفاق رسالة حول أهمية طلبكم هذا. غير أنه يجب أن نُبقي نصب أعيننا حقيقة أنه ما زال من الممكن للصور التي لم يشر إلينا فيها وبالتالي لا تظهر في يومياتنا، أن تظهر في أماكن أخرى على فيس بوك مثل «البحث»، «آخر الأخبار»، أو «يوميات» الأصدقاء.

استعمال الانترنت عبر شبكات الواي فاي العامة وفي مقاهي الانترنت

كثيراً ما يتواصل معنا أشخاص عانوا من مشاكل أمنية بعد استخدامهم حاسوباً عاماً في أحد مقاهي الانترنت، ولدى موقع سايبر آرابز نصيحة واحدة بسيطة بهذا الشأن، وهي ألا تستخدموا الحواسيب العامة في مقاهي الانترنت على الإطلاق، إذ قد تحتوي هذه الحواسيب على برمجيات خبيثة منصّبة مسبقاً ولن تستطيعوا تفادي خطرها بما أنه ليست لديكم أية سيطرة على الحاسوب الذي تستخدمونه. لقد صادفنا الكثير من الحواسيب العامة التي تحتوي على برامج لتسجيل ضربات المفاتيح Keylogger (وهي برامج تسجل كل ضربة مفتاح تقومون بها بما في ذلك كلمات المرور الخاصة بكم)، وبرامج لمراقبة حركة تبادل المعلومات عبر الانترنت، وأخرى تقوم تلقائياً بأخذ لقطات للشاشة.

في بعض الدول مثل سوريا، على سبيل المثال، يطلب موظفو الحكومة من أصحاب مقاهي الانترنت أن يقوموا بتنصيب برامج خبيثة للتجسس على المستخدمين وتقديم تقارير حول أنشطتهم، وقد أظهر بحثٌ قمنا به في دمشق انصياعَ العديد من المقاهي لهذه الأوامر.

في حال كنتم ممن يستخدمون خدمات مقاهي الانترنت، استخدموا حاسوبكم الخاص أو حاسوباً تثقون بمالكه.

وتظهر مشكلة مماثلة عند استخدام الإنترنت عبر شبكات واي فاي عامة. تقدم عدة مؤسسات سياحية مثل الفنادق والمطاعم والمقاهي خدمة الإنترنت المجانية، وهي خدمة يستعملها العديد من قراء موقع سايبر آرابز. إلا أن استعمال الإنترنت في الأماكن العامة ليس آمناً تماماً، إذ يمكن للقائمين على الشبكة أو أي شخص يستطيع النفاذ إليها أن يراقب المعلومات غير المشفرة التي تتبادلونها مع مواقع الإنترنت، مثل الرسائل الإلكترونية والتحديثات على مواقع التواصل الاجتماعي. ومن المعروف أنّ السلطات في بعض البلدان تقوم بشكل نشط بمراقبة النقاط العمومية التي تؤمن الإنترنت.

لذا، فإنه من المهم أن تتخذوا بعض التدابير لتحموا أنفسكم خلال استخدام نقطة إنترنت عامة. تذكروا أن المواقع التي تبدأ عناوينها بـ https يخضع محتواها للتشفير وهي بالتالي تتمتع بالأمان، بعكس المواقع التي تبدأ عناوينها بـhttp ؛ المعلومات التي يتم تبادلها مع المواقع التي تبدأ عناوينها بـhttps لا يمكن لأي طرف ثالث أن يقرأها.

عند دخول مواقع لا تتمتع بخدمة https، لا سيما مواقع البريد الإلكتروني والتواصل الإجتماعي، وخصوصاً عند استخدام شبكات واي فاي العامة، عليكم حماية أنفسكم من خلال استعمال إحدى التطبيقات الخاصة بالأمان مثل Tor أو Psiphon أو VPN/SSH. كما ننصحكم باستعمال هذه التطبيقات أيضاً في مقاهي الإنترنت. إلا أنه في حال استخدام اجهزة الخاصة بمقاهي الإنترنت لا شيء يمكنه أن يحميكم إذا كان منصب عليها برنامج لتسجيل ضربات المفاتيح Keylogger.

ستؤمن لكم هذه التطبيقات تشفير كل نشاطكم عبر الإنترنت، مما يجعل من المستحيل على أي شخص آخر الإطلاع على بياناتكم. ويبقى الخيار الأكثر أمناً أن تؤدوا النشاطات الحساسة في البيت وليس في مكان عام.

إلى أي مدى الهواتف الجوالة آمنة؟

تعد الهواتف الجوالة الوسيلة الأولى للتواصل في الشرق الأوسط. كما أن هناك عدداً متزايداً من الأشخاص الذين بدؤوا بالنفاذ إلى الإنترنت من خلال هواتفهم. على موقع سايبر آرابز، نقوم بشكل دوري بمناقشة تطبيقات أمن الإنترنت الخاصة بهواتف أندرويد وآيفون. لكن، وعلى رغم الطفرة في استعمال الإنترنت التي ظهرت في العامين الأخيرين، يبقى الإتصال وإرسال الرسائل النصية القصيرة أكثر الخدمات استعمالاً في الهاتف. إلى أي حد يعد هذا الإستعمال آمناً؟

هناك جواب بسيط؛ استعمال الهاتف الجوال لا يمكن أن يكون آمناً. إن تكنولوجيا GSM التي تسيّر الهواتف الجوالة اليوم لم يتم تطويرها لمراعاة خصوصيتكم وأمنكم، وبالتالي، فإنه من المستحيل جعل استعمال هاتفكم الجوال آمن بشكل كامل.

ليس فقط من السهل على مزودي الخدمة والحكومات أن يتنصتوا على محادثاتكم، ولكن يمكنهم أيضاً أن يعرفوا موقعكم، والأماكن التي زرتموها، وهويتكم، بالإضافة إلى الأشخاص الذين اتصلتم بهم. والأسوأ هو أنكم لا تستطيعون فعل أي شيء حيال ذلك! عندما تشغّلون هاتفكم، تتم مشاركة بياناتكم مع السلطات ومشغلي خدمة الخليوي. لذا، من المهم ألا تستعملوا هاتفكم في أي اتصالات حساسة أو أوضاع لا تريدون فيها الكشف عن موقعكم. تخيّلوا أنّ الحكومة قامت بكشف مجموعة هواتف تعود إلى ناشطين معارضين يجلسون في الغرفة نفسها، ماذا ستفعلون لو كنتم من بينهم؟

في السنوات الأخيرة أصبح من الواضح أنه يمكن تشغيل الميكرفون في الهاتف دون أن يلاحظ ذلك المستخدم. لذا ننصح بأن تطفئوا هاتفكم اثناء تواجدكم في اجتماعات حساسة.

لاحظ فريق سايبر آرابز أيضاً أن هناك اعتقاداً سائداً بأن تغيير الشريحة الهاتفية سيجعل من المستحيل على السلطات أن تحدد هويتكم. لسوء الحظ ذلك غير صحيح. عندما تقومون باستعمال الشريحة مع هاتف ما، فذلك يعني أن هاتفكم قد "أصيب"، أي تم ربطه بهويتكم وتغيير الشريحة الهاتفية لن يغير أي شيء. الشرائح المجهولة والأجنبية لا توفر أي حل هي الأخرى، إذ يجب استخدامها بهاتف جديد كي لا يتم ربطها بهويتكم. فالحكومات التي تراقب استعمال الهاتف تقوم بتجميع ملفات ضد أشخاص عبر مراقبة الأرقام التي يتصل بها هاتفهم.

الهواتف الجوالة هي أدوات ممتازة للتواصل، ولكن من المفيد التذكر أنها أيضاً أدوات ممتازة لأجهزة الإستخبارات التابعة لحكومتكم.

تشفير أندرويد ٤

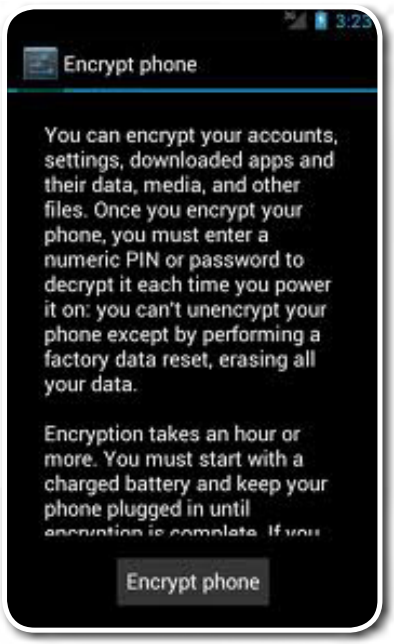
يمنحكم تشفير هواتفكم المزيد من الحماية في حال تمت سرقة الهاتف أو مصادرته من قبل الأجهزة الأمنية، إذ لا يمكن الوصول إلى المعلومات المخزنة في الهواتف الذكية المشفرة دون امتلاك كلمة السر، وبالتالي تكون معلوماتكم الشخصية وصوركم ودفتر الأرقام بأمان، على نقيض الهواتف العادية التي لا يمكن تشفيرها. ولذلك ينصحكم موقع سايبر آرابز بأن تقوموا بتشفير هواتفكم الذكية ذات برنامج أندرويد ٤ (أو أحدث) في حال كنتم تخزنون فيها معلومات حساسة أمنياً.

قبل البدء بعملية التشفير، تأكدوا من أنكم قد وضعتم رمزاً سرياً لقفل الشاشة، وأن بطارية الهاتف مشحونة والهاتف موصول بمأخذ كهربائي. سيستغرق التشفير ساعة على الأقل ولن يكون بإمكانكم مقاطعة العملية خلال هذا الوقت دون أن تخسروا بعضاً من بياناتكم أو جميعها لذا نرجو أن تتوخوا الحذر!

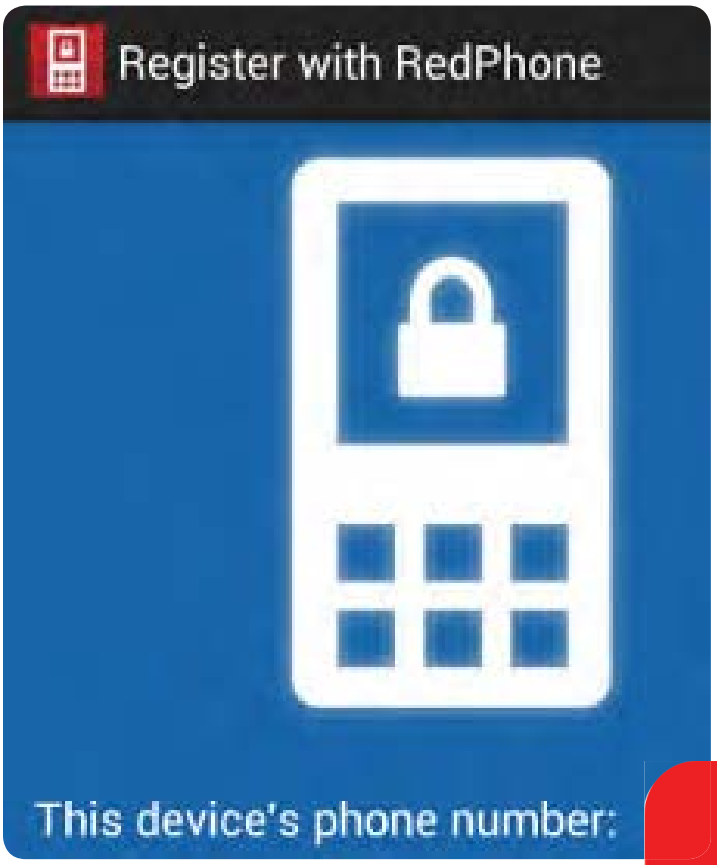
عندما تصبحون جاهزين لبدء عملية التشفير، قوموا بفتح أيقونة "الإعدادات" (Settings) من خلال الشاشة الرئيسية (Home) أو شاشة "جميع التطبيقات" (All Apps)، ومن ثم افتحوا التالي: شخصي (Personal) > الحماية (Security)> التشفير (Encryption)> تشفير الهاتف (Encrypt phone)، وقوموا بقراءة المعلومات المتعلقة بالتشفير بتمعن.

سيبهت لون أيقونة التشفير في حال لم تكن البطارية مشحونة أو لم يكن الهاتف موصولاً بمأخذ كهربائي، وفي حال لم تعودوا ترغبون بتشفير الهاتف، بإمكانكم لمس أيقونة "تراجع" (Back). اختاروا "تشفيرالهاتف" (Encrypt phone) لمتابعة العملية وسيطلب منكم إدخال الرمز السري لفك قفل الشاشة . إختاروا "متابعة" (Continue) ثم "تشفير الهاتف" (Encrypt phone) مرة أخرى.

سيتم إعلامكم بتقدم عملية التشفير، وقد تستغرق العملية ساعة أو أكثر وقد تتم إعادة تشغيل هاتفكم عدة مرات خلال هذه المدة. عند انتهاء عملية التشفير، سيطلب منكم إدخال الرمز السري، كما سيكون عليكم إدخال هذا الرمز كلما قمتم بتشغيل الهاتف بعد ذلك حتى تتمكنوا من فك تشفير بياناتكم.



ريدفون: (Red Phone) خيار آمن لإجراء مكالمات عبر الإنترنت



كثيرا ما يصلنا إلى موقع سايبر آرابز السؤال التالي: "كيف يمكنني ألا أدع أحداً يتنصت على مكالماتي؟"

كما ناقشنا في مرات سابقة، فهنالك العديد من التطبيقات المختلفة التي تشفّر مكالماتكم الهاتفية عن طريق الاتصال بالانترنت، وأشهرها برنامج سكايب. إلا أنّ سكايب يصبح بطيئاً جداً عند استخدامه عن طريق الهواتف الذكية، فهو لايتمتع بالمواصفات نفسها التي تتمتع بها برامج الاتصال المرافقة لهذه الهواتف.

وقد حاولت شركة أمن المعلومات الأمريكية ويسبر سيستمز (Whisper Systems) أن تحل هذه المشكلة من خلال تطوير تطبيق مفتوح المصدر هو ريدفون (RedPhone)، وهو تطبيق مصمم بحيث يشفّر جميع المكالمات التي تتم من خلاله من بدايتها وحتى النهاية، ويمكن تشغيله بمنتهى السهولة بعد تحميله من Google Play Store . بعد تشغيل التطبيق، سيُطلب منكم فتح حساب ريدفون باستخدام رقم هاتفكم الجوال فقط، ويحتوي التطبيق على لوحة أرقام ودفتر للعناوين خاصَّين به ويعتمدان نمط لوحة الارقام في أندرويد مما يعني أنكم لن تجدوا الكثير من الفروقات عما أنتم معتادون عليه مع نظام أندرويد.

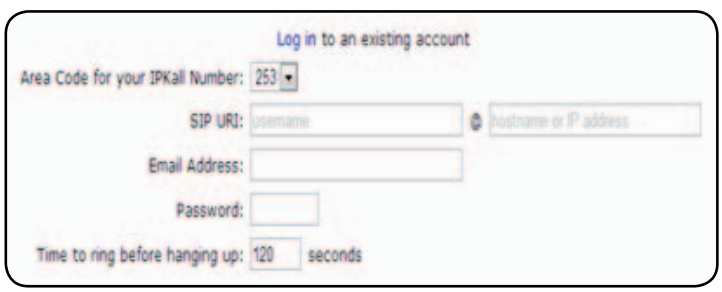
ويوجد أمر آخر مهم، ألا وهو ضرورة أن يستخدم طرفا المكالمة برنامج ريدفون حتى يتمكن هذا الأخير من تشفير المكالمة. وفي حال حاولتم الاتصال بشخص لا يستخدم تطبيق ريد فون، سيتم سؤالكم إن كنتم تودون دعوة هذا الشخص إلى استخدامه. بالطبع سيكون بإمكانكم تجاهل السؤال وإجراء المكالمة، إلا أن هذا يعني أن ريدفون سينتقل تلقائياً إلى استخدام النظام العالمي للاتصالات الجوالة (GSM) الأقل أمناً.

عند تلقيكم مكالمة عن طريق ريدفون، سيرنّ هاتفكم كما لو كان يتلقى مكالمة هاتفية عادية، ولكن تجدر الإشارة إلى أن هذه المكالمة ستكون عن طريق "الصوت عبر الانترنت" (VoIP) وليس النظام العالمي للاتصالات (GSM). هذا وتقوم مراكز خدمات ريدفون (في الولايات المتحدة الأمريكية) بكل ما يتطلبه تشفير المكالمات وبتجنب موجات النظام العالمي للاتصالات الجوالة (GSM) التي تستخدمها شبكتكم المحلية، وفي حال كنتم تستخدمون تقنيات الجيل الثالث (3G) أو نظام الجوالات العالمي المعزز (Edge)، فسيتم احتساب تكلفة المكالمة بناء على اشتراك حزمة البيانات الخاص بكم.

ولا يبدو أن هنالك أية مشاكل في تطبيق ريدفون رغم أنه ما زال، تقنياً، في مرحلته التجريبية الثانية (إصدار ٠.٨)، بل إننا نوصيكم بكل ثقة باستعمال هذا التطبيق إن كنتم تبحثون عن حل سهل وآمن لمهاتفة أصدقائكم وزملائكم.

كيف يمكن الاتصال بي عندما تتعطل خدمات النظام العالمي للاتصالات الجوالة (GSM)؟

توقفت شبكات الاتصالات الهاتفية عن العمل في بعض المناطق التي تشهد نزاعات في الشرق الأوسط، كما هو الحال، على سبيل المثال، في شمال شرقي سوريا. في معظم الحالات، قامت اللجان المحلية في هذه المناطق بتجهيز مراكز لتوفير خدمات الاتصال بالانترنت، مع بقاء القدرة على الاتصال بأحدهم هاتفياً غير ممكنة في معظم الأحيان. ولكن في حال كان بإمكانكم استخدام خدمات الاتصال بالانترنت، فليس من الصعب الحصول على رقم هاتف مسجل في الولايات المتحدة الأمريكية ومجاني ليتمكن الآخرون من الاتصال بكم من خلاله. قد يكون هذا الحل مفيداً جداً خصوصاً لهؤلاء الذين تقيم عائلاتهم خارج منطقة النزاع. ويُكلف الاتصال بهاتف مسجل في الولايات المتحدة الأمريكية من برنامج سكايب آوت (Skype-out) مثلاً أقل من ١,٥ سنتاً أمريكياً في الدقيقة. ويمكنكم طبعاً استخدام هذه الخدمة حتى يصبح بإمكان الآخرين الاتصال بكم على رقم إضافي دولي، ولكن من الجدير بالذكر أن التواصل عبر هذا الخط لن يكون مشفراً إلا في حال كانت خدمات الاتصال بالانترنت التي تستخدمونها مشفرة.



الحصول على حساب SIP (بروتوكول بدء الجلسة) ورقم هاتف

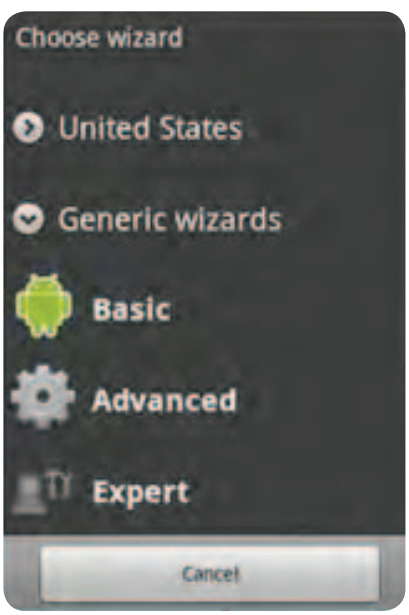
اذهبوا إلى موقع انتيسيب (Antisip) لإنشاء حساب (SIP) مجاني (هنا). لن تحتاجوا إلى تزويد الموقع برقم هاتف في حال لم يكن لديكم رقم، وسيعني إنشاؤكم حساب (SIP) أنكم قمتم بالتسجيل في شركة هواتف افتراضية، والتي ستكون في هذه الحال شركة (Antisip). في حال تم التسجيل بنجاح، احفظوا إسم المستخدم وكلمة المرور الخاصين بكم أو اكتبوهما ثم اذهبوا إلى IPkeall حيث ستجدون استمارة يجب ملؤها بدقة. قوموا بإدخال إسم المستخدم الذي اعتمدتموه للتسجيل في (Anitsip) في الخانة التي تلي «SIP URI» مباشرة، وفي الخانة التالية قوموا بإدخال «sip.antisip.com». كما يجب أن تستخدموا عنوان البريد الالكتروني (email) وكلمة المرور اللذين استخدمتموهما للتسجيل في (Antisip). بعد أن تنتهوا من ملء الاستمارة ومن اختبار «كابتشا» (اختبار تورنج العام والأوتوماتيكي للتمييز بين الحاسب والإنسان Captcha)، أنقروا على (submit) أي تسليم. إن تمت العملية بنجاح، ستصلكم رسالة إلكترونية من (IPkall) يقول سطرها الأول:

Thank you for signing up. Your IPKall phone number is: «XXX-XXX-XXXX»

أي «شكراً لكم لأنكم سجلتم في IPKall. رقم هاتفكم هو: كذا وكذا». وسيكون هذا هو رقم الهاتف المسجل في الولايات المتحدة الذي سيستطيع الآخرون الاتصال بكم من خلاله!

استقبال المكالمات على هاتفكم الذكي بنظام آندرويد

بعد أن قمتم بإنشاء حساب SIP ورقم هاتف والحصول عليهما، يجب أن تقوموا بتفعيل الخدمة على هواتفكم الذكية حتى يستطيع الآخرون الاتصال بكم. للقيام بهذا، عليكم أن تقوموا بتنصيب برنامج من تطبيقات الـ «SIP client». أحد هذه البرامج الجيدة هو برنامج (cSIPsimple)، الذي يمكنكم تحميله من Google play store، وإن لم يكن بإمكانكم الوصول إلى صفحة جوجل، فبإمكانكم تحميل ملف مجموعة تطبيقات آندرويد (APK) من هنا.



قوموا بتشغيل (cSIPsimple) بعد تنصيبه. ستحمل أول شاشة سترونها عبارة «Easy configuration» أي «الترتيب السهل»: لا تعدلوا أي شيء واختاروا «safe» أي

«آمن»، وسيطلب منكم إضافة حساب. إفتحوا قائمة «Add+ account» أي «إضافة حساب»، واختاروا «Basic» أي «أساسي» من آخر قائمة مزودي خدمات الهاتف التي ستظهر لكم لتقوموا باختيار إعدادات حسابكم: أدخلوا أي إسم في خانة «account name» أي «إسم الحساب»، ولكن أدخلوا اسم المستخدم الذي استعملتموه في (Antisip) في خانة «User» أي «المستخدم»، وأدخلوا «sip.antisip.com» في خانة «server» أي «خادم»، وكلمة السر التي اخترتموها في خانة «password» أي «كلمة المرور». عند الانتهاء، اختاروا «safe» أي «آمن» وتصبحون جاهزين لتلقي المكالمات عن طريق رقم هاتفكم الجديد المسجل في الولايات المتحدة الأمريكية.

ملاحظة: قد يحجب بعض مزودو خدمة الانترنت الاتصالات الهاتفية أو الاتصالات الواردة عن طريق الـ(SIP) وهو ما يفعله بشكل خاص مزودو خدمة اتصال الجيل الثالث الـ(3G) في العالم العربي. وللتخلص من مشاكل الحجب، قوموا بالاتصال بالانترنت عن طريق (VPN) شبكة خاصة افتراضية وتجدون في الرابط شبكة خاصة افتراضية مجانية يمكنكم استخدامها والحصول عليها من http://www.vpnbook.com، ألا وهي شبكة الـ(PPTN) أي (شبكة مزود الاتصالات المهنية).

من الجدير بالذكر أن هذه الطريقة ستزودكم برقم هاتف يستقبل المكالمات فقط (إضافة إلى خدمة البريد الصوتي!) دون أن يكون بإمكانكم الاتصال بأحد من هذا الرقم. لإجراء المكالمات، أنتم بحاجة إلى برنامج سكايب أو غيره من برامج الصوت عبر الانترنت لتدفعوا ثمن مكالماتكم وذلك لأن الاتصال هاتفياً بالآخرين له تكلفته.

استقبال المكالمات عبر حاسوبكم

كما يمكنكم استقبال المكالمات الهاتفية عن طريق حاسوبكم بدل هاتف الأندرويد. لتمكين جهازكم من استقبال المكالمات، قوموا بتحميل برنامج مجاني يدعى (X–Lite) من هنا، ومن ثم اذهبوا إلى (Softphone) ومن ثم (Account settings) من القائمة الرئيسية، وستظهر لكم نافذة جديدة لتدخلوا البيانات التي حصلتم عليها من (Antisip) ألا وهي إسم المستخدم والذي يجب ادخاله في خانة «User ID»، وعبارة «sip.antisip.com» التي يجب إدخالها في خانة «Domain». إياكم وأن تنسوا كلمة السر الخاصة بكم!

سيقوم برنامج (X–Lite) بتسجيل حساب الـ(SIP) الخاص بكم، وسيسألكم عن رقم هاتفكم لإكمال هذه العملية. قوموا باختيار «الولايات المتحدة الأمريكية» من القائمة المنسدلة وأدخلوا رقم هاتفكم المسجل في الولايات المتحدة في الخانة المخصصة. تأكدوا من أنكم أضفتم رقم (١) إلى بداية رقم الهاتف (الذي يجب أن يتكون من ١١ رقم)، ورقم (١) هو رمز الهاتف الدولي للولايات المتحدة الأمريكية. بعد ذلك، سيجري (X–Lite) مكالمة تجريبية معكم يزودكم فيها برمز من خمسة أرقام عليكم إدخاله إلى استمارة أخرى تزودون بها. عندما تنتهون من هذا بنجاح، تصبحون جاهزين لاستقبال الاتصالات الهاتفية عبر حاسوبكم.

إلى أي مدى استعمال سكايب آمن؟

سكايب هو إحدى الخدمات الأكثر استخداماً لإجراء الإتصالات في العالم العربي. جميع الإتصالات عبر سكايب مشفرة، ولذلك فقد أصبح هذا البرنامج أداة أساسية للتواصل خلال «الربيع العربي». ولكن توجد بعض الثغرات الأمنية في برنامج سكايب من المهم تذكرها أثناء استعماله.

الأبواب الخلفية

على رغم أنه من الصعب جداً فك تشفير التواصل عبر سكايب، إلا أن الخبراء يجمعون بشكل كبير على أن هناك أبواباً خلفية في البرنامج. الباب الخلفي هو نقطة يوفرها سكايب، يمكن لطرف ثالث النفاذ منها إلى مجرى اتصالاتكم. ويشتبه بالحكومة الأميركية بشكل خاص بأنها تقوم بالتنصت على محادثات سكايب. بالطبع، لم تعترف أي حكومة ولا القيمون على سكايب بهذا الأمر، ولكن من المهم أن تكونوا حذرين بعض الشيء عند القيام باتصال عبر هذا البرنامج إذا كنتم تعيشون في بلد على علاقة جيدة بالولايات المتحدة. بينما استعمال سكايب آمن في سوريا، الحال ليس كذلك في البحرين أو السعودية أو قطر.

تاريخ الدردشة

يستعمل العديد من الناس خدمة الدردشة (Chat) في سكايب، ومع دمج سكايب وإم إس إن مسينجر من مايكروسوفت، فمن المتوقع أن تزداد هذه الخدمة شعبيةً، إلا أن سجل الدردشة يتم حفظه على خادم سكايب، وكلما سجلتم دخولكم في سكايب، يقوم التطبيق بتحميل تاريخ دردشاتكم بشكل كامل. قد لا يشكل ذلك مشكلة إذا كنتم تستعملون حاسوبكم الخاص، إلا أن هذا السجل يتم تحميله أيضاً على أجهزة الحاسوب العامة. خلال مسح أحد أجهزة الحاسوب في مقهى إنترنت في دمشق، وجد فريق سايبر آرابز التاريخ الكامل لدردشات ٣٦ شخصاً! لذا، فإنه من المهم أن تستعملوا سكايب فقط في أجهزة تثقون بها. كما يمكنكم أن تهيّئوا سكايب لكي لا يحفظ تاريخ دردشتكم، وذلك من خلال القيام بالخطوات التالية:

الضغط على (أدوات) Tools› (خيارات) Options › (خصوصية) Privacy› (إبقاء التاريخ) Keep History.
واختيار (بلا محفوظات) no history. ومن ثم الضغط على (مسح المحفوظات) Clear history ومن ثم حفظ الاعدادات بالضغط على (حفظ) save.

ربط سكايب بالإنترنت بطريقة آمنة

يستعمل العديد من الناس سكايب مع أدوات لتخطي الرقابة أو أدوات لتشفير بيانات الإنترنت الخاصة بهم. إذا اخترتم برنامجاً مناسباً مثل Tor أو VPN أوSSH فإن التواصل عبر سكايب يمكن أن يكون آمناً جداً. إلا أن سكايب تم تصميمه بحيث إنه يقوم بالإتصال بالإنترنت من دون احترام إعدادات الأمان الخاصة بكم. يقوم البرنامج دائماً بالبحث عن الطريقة الأفضل للإتصال بالإنترنت، وهي ليست دائماً عبر خدمات الأمان التي قمتم بإعدادها. لذا، تأكدوا جيداً أن سكايب يقوم فعلاً باستعمال طريقة الربط بالإنترنت التي قمتم باختيارها. على عكس الإعتقاد السائد، فإن تغيير إعدادات «البروكسي» الخاصة بسكايب لن يغيّر ذلك، إذ سيبقى الإتصال الذي تستعملونه غير آمن.

لن يمر الإتصال بين سكايب والانترنت عبر قناة آمنة إلا عبر إجبار البرنامج على استعمال أداة لتخطي الرقابة. قام فريق سايبر آرابز بإنشاء «سكريبت» (Script) سهل الاستخدام يغيّر إعدادات الأمن في ويندوز من أجل بلوغ هذه الغاية. لاستعمال هذا «السكريبت» أنتم بحاجة إلى استعمال ويندوز ٧ أو نسخة أكثر حداثة مع تشغيل جدار الحماية (Windows Firewall) حسب الإعدادت القياسيّة (Standard).

هناك ملفان تحتاجون إلى تحميلهما لكل نسخة من ويندوز. إذا كنتم تستعملون النسخة ٣٢ بِت من ويندوز، حمّلوا «السكريبت» من أجل تفعيل استعمال سكايب بشكل آمن و«السكريبت» الخاص بإزالة التفعيل من هنا. لمستخدمي ويندوز ٦٤ بِت، حمّلوا «سكريبت» التفعيل والخاص بإزالة التفعيل من هنا. للتحقق من نسخة ويندوز التي تستخدمونها، إفتحوا قائمة البداية (Start Menu) ثم انقروا بالزر الأيمن على أيقونة «My Computer»، بعد ذلك، اختاروا «الخصائص» (Properties). ستفتح نافذة جديدة تظهر لكم أي نسخة من ويندوز قمتم بتنصيبها.

بعد تحميل ملف «السكريبت» المناسب عليكم أن تفعّلوه بنمط «مسؤول نظام التشغيل» عبر اختيار «Run as administrator».

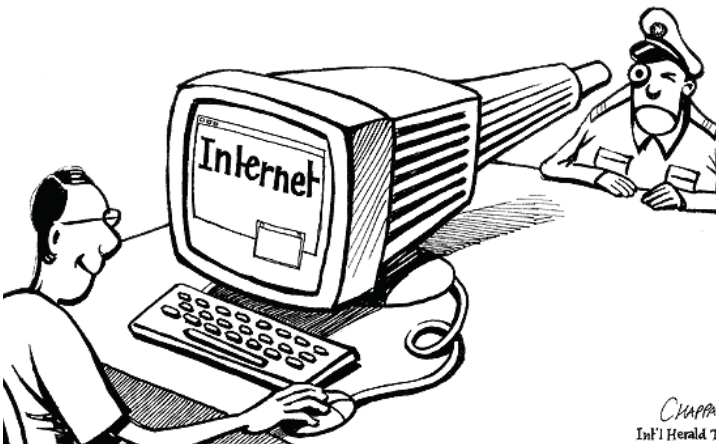
ستظهر نافذة منبثقة تحمل سؤال عن موافقتكم – أنقروا على «Yes» لإبداء الموافقة، سترون عندها نافذة سوداء ستختفي بشكل سريع. أنتم الآن جاهزون لاستخدام سكايب عبر تور (Tor) أو سايفون (Psiphon) أو الشبكة الإفتراضية الخاصة بكم .(VPN) عليكم التنبه إلى أن هذا «السكريبت» جرى إعداده للعمل مع الإعدادت القياسية فقط (Standard). للتأكد مما إذا كان السكريت يعمل، قوموا بإعادة تشغيل سكايب ومن ثم توجّهوا قسم الإتصالات الهاتفية (Call Phones) إذا كان العلم فوق لوحة المفاتيح الرقمية مختلف عن علم الدولة التي تتواجدون فيها، فذلك يعني أنكم تتصلون بالإنترنت عبر قناة آمنة.

ما هي الرقابة على الانترنت؟

تقوم الحكومات ومزودو خدمة الانترنت (ISPs) في العديد من دول الشرق الأوسط بحجب مواقع تحتوي على معلومات لا يتفقون معها، إما لأنّ السلطات لا تسمح بانتشار وجهة نظر الموقع المحجوب أو ببساطة لأن الصفحة المحجوبة تحتوي على كلمات من قائمة الكلمات المحظورة لدى هذه السلطات. كما هو الحال،على سبيل المثال، مع المواقع التي تحتوي على كلمة "إسرائيل"، والتي تعتبر من المواقع الأكثر حجباً في الشرق الأوسط.

من النشاطات الرئيسية التي يقوم بها موقع سايبر آرابز تقديم النصائح حول كيفية التحايل على الرقابة على الانترنت باستخدام برامج خاصة، حيث نكتب العديد من المقالات حول هذا الموضوع بالإضافة إلى تزويد القراء بنصائح فردية من خلال صفحتنا على موقع فيس بوك. ومع هذا فقد لاحظنا أنّ قلة فقط من الاشخاص تعرف ما هي الرقابة على الانترنت، وما هي آلية عملها، ومن هم المسؤولون عنها.

باختصار، هنالك نوعان رئيسيان من الرقابة: أولهما الرقابة النشطة وهي التي تقوم فيها السلطات بالتدخل فعلياً لمنع وصول منشورات معينة إلى الناس. ويحتاج هذا النوع من الرقابة إلى الاستعانة بأدوات تقنية وماسحات ومراقبين يتابعون ما تنشره مواقع الانترنت.



والنوع الآخر هو الرقابة الذاتية. ولعل هذا النوع من الرقابة هو الأكثر إشكالية لأن نجاحه يعتمد على خوف القائمين على المواقع من إغضاب السلطات فيمتنعون عن نشر مواد إشكالية لتجنب المواجهات القانونية، وبالتالي فمن الصعب اكتشاف هذا النوع من الرقابة أو التحايل عليه. ولا توجد قواعد ناظمة لهذا النوع من الرقابة. ومع أن الرقابة الذاتية في وسائل الإعلام عبر الانترنت شائعة جداً في الشرق الأوسط، إلا أننا في سايبر آرابز معنيون على نحو رئيسي بالنوع الأول من الرقابة على الانترنت، والذي سيشكل بدوره المحور الرئيسي لهذه المقالة.

ما هي آلية عمل الانترنت؟

لنتمكن من فهم آلية عمل الرقابة على الانترنت وكيفية التحايل على هذه المشكلة، لا بد لنا من أن نبدأ بفهم آلية عمل الانترنت ذاتها. عندما تتصفحون الانترنت في المنزل أو مقهى عام، فأنتم تتصلون بالشبكة العنكبوتية بواسطة أحد مزودي خدمة الانترنت (Internet Service Provider ISP) الذي يقوم بإعطاء الحاسوب الذي تستخدمونه عنواناً (عنوان آي بي أو عنوان بروتوكول الانترنت IP Address) يشبه إلى حد ما العناوين البريدية في أنه يستخدم لتعريفكم وتبادل المعلومات معكم، ويكون بإمكان أي شخص يعرف عنوان بروتوكول الانترنت الخاص بكم أن يتوصل إلى مكانكم الجغرافي (بإمكانكم معرفة عنوان برتوكول الانترنت الخاص بكم هنا).

والأمر سيان بالنسبة إلى مواقع الانترنت، فهي أيضاً لها عناوين آي بي؛ وفي واقع الامر، فأنتم تقومون بطلب المعلومات من عنوان آي بي معين في كل مرة تستعرضون فيها صفحة ما على حاسوبكم. وبسبب صعوبة تذكر هذه العناوين، فإن نظام مخدمات أسماء النطاقات

(Domain Name Servers DNS) يعطيها أسماء يمكن لنا قراءتها وتذكرها هي "أسماء النطاقات"، مثل (www.cyber-arabs.com)، أي أن نظام أسماء النطاقات يعمل وكأنه دليل هاتف ضخم يربط بين الأسماء وأرقامها.

ويعني هذا أنّ سلسة من الأشياء تحدث عندما تطلبون من متصفحكم فتح موقع مثل (www.cyber-arabs.com)، إذ يقوم حاسوبكم بطلب عنوان الآي بي الخاص بهذه الصفحة من أحد مخدمات أسماء النطاقات الكثيرة، وعادة ما يكون هذا المخدم تحت إدارة مزود خدمة الانترنت، ويطلب متصفحكم من مزود الخدمة هذا أن يتصل بعنوان الآي بي المطلوب. بعد ذلك، يمر الطلب عبر للسلة من الموجهات (Routers) وهي نقاط اتصال (Conne – tion Points) يرسل كل منها نسخة من الطلب إلى الموجه التالي الأقرب للهدف، حتى يصل الطلب إلى موجه متصل بالحاسوب الذي يحوي على الموقع الذي تريدون فتحه. في نهاية المطاف، يتم إرسال الموقع المطلوب إليكم وعرضه على شاشتكم. طبعاً لا تستغرق جميع هذه الخطوات أكثر من أجزاء من الثانية.

ليكون بمقدور مزودي خدمة الانترنت إرسال حزمة من المعلومات من حاسوب إلى موجه ومن ثم إلى حاسوب آخر، لا بد لهذه المزودات من أن تتبع قوانين دولية معينة. تسمح هذه القوانين، والتي تعرف أيضاً بالبروتوكولات، بمشاركة البيانات والموارد على نحو منظم. فعلى سبيل المثال، تستخدم الانترنت منافذ مرقّمة لتوزيع الاتصالات على مجموعات مختلفة من الطلبات، فيتم تصفح شبكة الانترنت المعتاد عبر المنفذ رقم ٨٠ في حين يجري إرسال الملفات عبر المنفذ رقم ٢١، ويستخدم البريد الإلكتروني المنافذ ٢٥ أو ٥٣ أو ١٤٣، وتستخدم الاتصالات الهاتفية المنفذ رقم ٥٠٦٠، وذلك لأن الشبكة جزء فقط من الانترنت. هذا وتستخدم أدوات التحايل على الرقابة المنافذ المرقمة ااتها، فيستخدم بروتوكول القشرة الآمنة (The Secure Shell Pr – tocol SHH) المنفذ رقم ٢٢ وتستخدم الشبكة الافتراضية الخاصة (Virtual Private Network – VPN) القياسية المنفذ رقم ١٧٢٣.

وبناء على هذه القوانين، تتصل السلطات المسؤولة عن الانترنت في بلدكم ببقية العالم من خلال موجهات ضخمة، ويمكن أن تصبح هذه الاتصالات مع العالم الخارجي نقاطاً يمكن من خلالها مراقبة حركة انتقال المعلومات عبر الانترنت أو السيطرة عليها على مستوى الدولة.

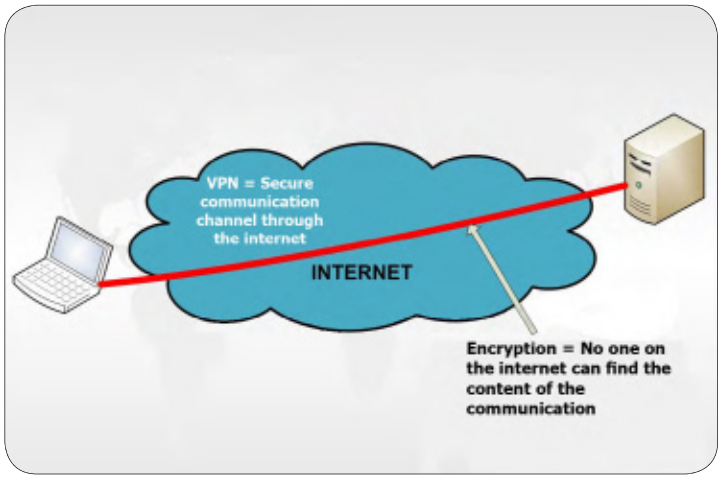
لنتمكن من فهم آلية حجب المعلومات الموجودة على الانترنت، لابد لنا من الخوض في التفاصيل، وذلك لأنه من الممكن لحجب المعلومات أن يحدث في أي مستوى من مستويات نظام الانترنت. وهذا هو، مثلاً، حال مخدمات أسماء النطاقات (DNS) التي صممت لتكون دليل هاتف الانترنت الذي يصل بين عناوين الآي بي (IP addresses) وعناوين الانترنت (URLs)، إلا أنه من الممكن أيضاً استخدامها لحجب المعلومات. فكما يمكن تمزيق صفحات معينة من دليل الهاتف، يمكن تغيير مرجعية مخدمات أسماء النطاقات هذه.

الرقابة على الانترنت

يمكن أن تحدث الرقابة في نقاط مختلفة في نظام الانترنت، ابتداءً من مكتبكم الخاص وانتهاءً بالاتصال الذي تجريه الدولة التي تقيمون فيها مع الشبكة العنكبوتية. كما يمكن أن تتم الرقابة على الانترنت من خلال أكثر من طريقة وباستخدام أدوات تقنية مختلفة. ولذلك فإنّ الطريقة الوحيدة للتحايل على الرقابة بفعالية هي تحديد التقنية المستخدمة في الرقابة، وهو مجال ينشط فيه موقع سايبر آرابز.

تتم الرقابة الاحترافية على مستوى الحكومات ومزودي خدمة الانترنت من خلال أجهزة متطورة تكنولوجياً يمكنها أن تمسح عناوين الأي بي (IP addresses) أو عناوين المواقع (URLs) بسرعة هائلة. ورغم أن الرقابة على الانترنت شائعة في دول الشرق الاوسط، فعادة ما تأتي تكنولوجيا الرقابة من الدول الغربية الليبرالية. ومن الشركات الأشهر في مجال إنتاج الأجهزة والبرامج التي تستخدم في الرقابة على الانترنت: Cisco، و Websense، و McAfee، وتتمتع هذه الشركة الأخيرة بشهرة إضافية كونها الشركة التي طورت برنامج مكافحة الفيروسات المعروف.

كما ظهرت شركة Blue Coat systems، وهي أيضاً شركة تنتج معدات تستخدم في الرقابة على الانترنت ويقع مركزها في كاليفورنيا، في عناوين الأخبار مؤخراً بعد أن اتضح أن السلطات السورية تستخدم منتجات هذه الشركة لحجب كلمات مثل "إسرائيل" أو "وكيل: proxy" (رابط)، ورغم أن الشركة ادعت أنها لم تتعامل مع النظام السوري قط، إلا أنه من المرجح أن الشركة كانت تعلم أن أجهزتها تستخدم في سوريا بالإضافة إلى دول أخرى تحكمها أنظمة سلطوية. ويعمل



فريق سايبر آرابز مع شركائه على نشر الوعي حول هذه الممارسات بهدف إيقاف الدعم الذي تقدمه الشركات الغربية للرقابة.

وتجدون أدناه قائمة بأساليب الرقابة الأكثر انتشاراً:

• إلغاء تسجيل بنود من مخدمات أسماء النطاقات (DNS):

وهو ما يحدث عندما تقوم السلطات في الدول التي تسيطر فيها حكوماتها على مخدمات أسماء النطاقات بـ"إلغاء تسجيل" المواقع المحظورة. ويشبه هذا الإجراء حذف إسم شخص ما من دليل الهاتف أو كتابة رقم غير صحيح إلى جانب الإسم.

• حجب عناوين الآي بي (IP addresses):

وهو ما يحدث عندما تكون نقاط الاتصال (الموجهات) التي يستخدمها مزود خدمة الانترنت تحت سيطرة السلطات. ببساطة، تقوم هذه السلطات ببرمجة نقاط الاتصال بحيث تحجب عناوين الآي بي لمجموعة معينة من المواقع والمحتويات التي ترغب السلطات بحجبها، فيقطع مزود خدمة الانترنت الاتصال إن حاولتم الوصول إلى أحد هذه المواقع المحظورة ويظهر لكم متصفحكم رسالة تقول بوقوع خلل ما.

• الحجب على أساس كلمات البحث:

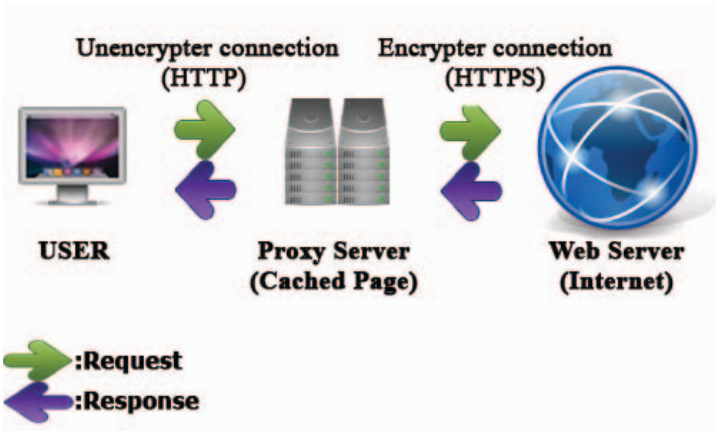
وهو ما يحدث عندما تريد السلطات حجب محتوى معين مثل المواقع التي تحتوي على كلمة "إسرائيل" أو "معارضة"، وذلك لأن حجب عناوين الآي بي وإلغاء تسجيل بنود من مخدمات أسماء النطاقات لا يحجبان إلا المواقع الموجودة بالأصل على قائمة الحظر. وهناك الكثير من الطرق لمسح محتوى موقع ما بغرض الرقابة، إلا أن ارتفاع تكلفة مسح كل موقع بعينه، وحجم الوقت الذي يتطلبه مثل هذا العمل، يجعل معظم مزودي خدمة الانترنت يلجؤون إلى مسح عناوين المواقع (URL) عوضاً عن مسح المواقع ذاتها. وتقوم هذه التقنية بمسح العناوين بحثاً عن كلمات معينة (على سبيل المثال: www.cnn.com/مقالة-إسرائيلية)، فإن احتوى عنوان الصفحة على كلمات محظورة (مثل "إسرائيل")، يتم قطع الاتصال ومن ثم إعادتها مما يجعل متصفحكم يظهر لكم رسالة خلل أو صفحة بيضاء.

• تصفية الحُزم (Packet Filtering):

تعدّ تصفية الحزم أكثر طرق حجب المعلومات تطوراً (وتعرف أيضاً بفحص الحُزم أو المسح الدقيق للحزم). وللقيام بهذا، يحتاج مزود خدمة الانترنت إلى تنصيب معدات خاصة تقرأ وتفتح جميع البيانات التي يرسلها أو يستقبلها مستخدم ما. وتدعى هذه الطريقة بتصفية الحزم لأن تبادل البيانات عبر الانترنت يتم من خلال ما يسمى بـ"الحزم". وإحدى الطرق الشائعة لمنع مزود خدمة الانترنت الذي تتعاملون معه من مسح بياناتكم هو تشفيرها، إذ لا يستطيع المزود تفحص ما داخل الحزم التي ترسلونها أو تستقبلونها بعد أن يتم تشفيرها. ولكن ولسوء الحظ، فإن بعض مزودي خدمة الانترنت أصبحوا الآن يحجبون الحزم المشفرة.

• حجب المنافذ:

يعد حجب منافذ معينة طريقة أخرى شائعة لحجب المعلومات. فكما ناقشنا سابقاً، تستخدم الانترنت منافذ معينة محجوزة مسبقاً لأنشطة بعينها، وبالتالي فإن حجب منفذ معين يؤدي بسهولة إلى منع حركة المعلومات عبر الاتصالات الهاتفية، منع عمل بعض أدوات التحايل على الرقابة، أو منع خدمات إرسال الملفات أو البريد الإلكتروني. بإمكانكم معرفة المنافذ المحجوبة في خدمة الانترنت التي تستخدمونها من هذا الموقع.



الصورة ١ : تحذير أن الانترنت مراقبة في دولة الإمارات

• حذف نتائج البحث:

عادة ما تتعاون المنظمات التي تبدو وكأنها تعارض الرقابة، مثل جوجل، وياهو، وبلاك بيري، وآبل، ومايكروسوفت مع الحكومات لحجب البيانات عن مستخدمي الانترنت أو مراقبتها أو تسجيلها. وفي حين يدعي موقع جوجل الشفافية حول هذا التعاون، لكونه ينشر تقريراً سنوياً عن الشفافية يصرح فيه عمّا يحجبه (رابط)، فلا تتمتع جميع المواقع بهذا المستوى من الشفافية. كما يجب أن يدرك مستخدمو الانترنت أنّه عادة ما تتعاون كبرى شركات تكنولوجيا المعلومات مع حكوماتها.

• حجب (أجزاء من) الانترنت:

يعد حجب جميع أشكال الاتصال بالانترنت شكل متطرف من الرقابة. ولكن، وبما أنّ الحكومات تملك البنية التحتية للانترنت أو تتحكم بها في معظم دول الشرق الأوسط، فبإمكان هذه الحكومات إغلاق الانترنت عندما ترى لذلك ضرورة. فعلى سبيل المثال، تم إغلاق الانترنت لمدة أسبوع خلال الانتفاضة الشعبية في مصر وقامت الحكومة السورية بشيء من هذا القبيل مؤخراً. ومع ذلك يبقى من غير الوارد حدوث هذا النوع من الرقابة كثيراً وذلك بسبب الآثار المالية الهائلة التي تنتج عن إغلاق الانترنت.

• وسائل أخرى للرقابة:

توجد وسائل أخرى عديدة لممارسة الرقابة على محتوى الانترنت، وعادة ما يكون لشركات الانترنت سياساتها الخاصة لمراقبة المحتوى، كما هو الحال، على سبيل المثال، في موقع فيس بوك، الذي يفرض رقابة نشطة على مستخدميه فيما يتعلق بالعري، والعبارات العدائية والعنصرية، والتمييز (رابط). وطبعاً يكمن الخطر هنا في أن فيس بوك نفسه هو من يقرر طبيعة المواد التي تقع ضمن هذه الفئات الممنوعة.

ولأن الحجب يبدوعادة وكأنه خلل تقني أو مشكلة في الاتصال، فمن الصعب معرفة ما إن كنتم تتعرضون بالفعل للرقابة وتحديد التقنية المستخدمة لمراقبة نشاطكم. كما أنه لا يكون من الواضح عادةً من هو المسؤول عن هذه الرقابة: الحكومة، أم مزود خدمة الانترنت، أم المخدم المحلي مثل مدرستكم أو مقهى الانترنت الذي تستخدمونه، مما يجعل من الصعب التحايل على هذه الرقابة دون إجراء بحث دقيق وتفصيلي لتحديد المشكلة والحل المطلوب لمواجهتها، وعلاوة على ذلك، لا توجد حلول عامة تنفع في جميع الحالات. رغم هذا فقد كان لفريق سايبر آرابز، منذ بداية الربيع العربي، دوره في اكتشاف بعض حالات الرقابة وتقديم النصح لمستخدمي الانترنت حول كيفية التحايل عليها.

التحايل على الرقابة

لابد أن نعرف كيف تتم الرقابة حتى نتمكن من إيجاد طريقة للتحايل عليها. وبما أن الانترنت أُنشئت أساساً لتكون شبكة مفتوحة غير محكومة بحدود الدول، فإن ذلك يمنحنا القدرةَ في جميع الأحيان تقريباً على تجهيز نقاط نفاذ آمنة وغير مراقبة، ويبقى الاستثناء الوحيد الذي يستحيل فيه التحايل على الرقابة هو عند حدوث حجب كامل لإمكانية الاتصال، أي عندما يتم إغلاق الانترنت بأكملها. وتعدّ سرعة الاتصال، للأسف، إحدى التنازلات الرئيسية التي يجب علينا تقبلها لنتمكن من التحايل على الرقابة.

ومن الطرق الأكثر استخداماً للتخلص من الرقابة، الاتصالُ بالانترنت عن طريق حاسوب أو مزود ما يدعى بـ "الوكيل" (Proxy) ويكون موجوداً خارج بلدكم (رابط). فبدل أن تقوموا بطلب الدخول إلى موقع معين (محجوب) مباشرة، فإنكم تطلبون من ذاك الحاسوب غير المراقب، والموجود في منطقة لاتوجد فيها رقابة على الانترنت، أن يعثر على عنوان الموقع بالنيابة عنكم. ويقوم هذا الحاسوب بعد ذلك بإعادة توجيه الموقع أو أية بيانات أخرى كنتم قد طلبتموها منه إليكم. تعني هذه العملية أنكم قمتم بالتحايل على الرقابة بفعالية.

وتوجد الكثير من الطرق لاستخدام هذا النموذج من التحايل على الرقابة، ولكن لعل الأدوات التقنية الأكثر استخداماً لهذا الغرض هي الوكيل غير المشفر (مثل Glype proxies)، والشبكات الافتراضية الخاصة (VPN)، وبروتوكول SSH، وبرنامج ToR. وعلاوة على قيام البرامج الثلاثة الأخيرة بإعادة توجيه الموقع المطلوب من الوكيل، فإنها تقوم أيضاً بتشفير البيانات. ويعني هذا أنكم تعتمون على جميع الاتصالات التي جرت بين حاسوبكم والحاسب الوكيل مما يجعل من المستحيل على ماسحات المحتوى أن توقف تبادل المعلومات الذي تقومون به أو أن تعترض طريقه.

كما تمكنكم البرامج المذكورة أعلاه من استخدام المنافذ المحجوبة في بلدكم. فإن كان المنفذ الخاص بالهواتف الرقمية (٥٠٦٠)، على سبيل المثال، محجوباً في بلدكم، بإمكانكم إجراء الاتصالات عبر المنفذ (٥٠٦٠) ذاته ولكن باستخدام الحاسب الوكيل. والبرامج التالية أمثلة على برامج التحايل على الرقابة التي تستخدم هذه الطريقة: SecurityKiss، Psiphon، TOR browser، وHotspot Shield والعديد غيرهم.

كما يقوم برنامج تور (ToR) بزيادة درجة تعقيد التشفير من خلال إنشاء شبكة من الحواسيب المجهولة الهوية التي تتعاقب على طلب المواقع والبيانات التي تريدونها باستخدام برامج تشفير متطورة. ويعني هذا أن برنامج تور لا يمنحكم القدرة على الوصول إلى جميع أجزاء الانترنت فقط، بل يقوم أيضاً بتشفير حركة تبادل المعلومات في وجه السلطات بالإضافة إلى مالكي الحاسب الوكيل، بحيث لا يمكن لأيّ كان أن يعلم ماذا تفعلون أو أن يربط بين نشاطكم على الانترنت وهويتكم. إلا أن استخدام برنامج تور يؤدي إلى إبطاء سرعة الاتصال على نحو ملحوظ، وذلك لأنّ تور يستخدم شبكة من الحواسيب عوضاً عن حاسوب واحد ليصلكم بالانترنت، على عكس خدمة VPN و SSH).

وباعتبار أن معظم الحكومات السلطوية لا تقوم بفرض الرقابة على الانترنت فقط ، بل تستخدمها للتجسس أو للتنصت على تواصل الأشخاص مع بعضهم البعض، فإن موقع سابير آرابز ينصحكم باستخدام أحد البرامج المشفرة مثل SSH، أوVPN ، أو ToR فقط. فعلى الرغم من أن البرامج الأخرى قد تبدو وكأنها تعمل على نحو جيد، فهي لن تمنحكم مستوى الأمان نفسه.

وفي حال كانت الرقابة المفروضة على اتصالكم بالانترنت من نوع الرقابة على حزم البيانات المتطور، يصبح من الممكن للسلطات المسؤولة عن الانترنت ملاحظة حركة تبادل المعلومات المشفرة عن طريق SSH أو VPN أو ToR. ولكن لحسن الحظ توجد حلول للتحايل على هذا النوع من الرقابة أيضاً، فبدل التواصل مع حاسوب وكيل باستخدام أسلوب التشفير المعتاد، تقوم بعض برامج التحايل على الرقابة بتشفير معلوماتكم بطريقة تجعلها تبدو وكأنها قانونية أي وكأنها بريد الكتروني عادي أو تصفح لموقع عادي، على سبيل المثال. يدعو برنامج تور هذا النوع من التكنولوجيا بـ ObfsProxy.

وتتضمن وسائل التحايل على الرقابة الأقل تطوراً استخدام أنظمة أسماء نطاقات أجنبية (مثل نظام أسماء نطاقات جوجل Google's DNS server) وهي أنظمة لا تغير عناوينها أو تشفر البيانات. ويعتبر تشفير عناوين الانترنت (كما هو الحال في برنامج Glype proxies) طريقة أخرى شائعة لتجنب الحجب بناء على كلمات معينة، إلا أن البرامج التي تستخدم هذه التقنية لا تخفي هويتكم أو تغيّر المسلك الذي تتبعونه للاتصال بالانترنت، فهي تقوم بالتحايل على الرقابة فقط دون تشفير بياناتكم أو إخفاء هويتكم.

الصورة٢ : آلات بلوكوت للرقابة؛ تم التقاط هذه الصورة بشكل غير قانوني في مراكز مزود خدمة الانترنت تراسل في سورية

الطرق الأمثل لاختيار كلمة السر

عادة ما نتلقى تقارير عن أشخاص تم اختراق بريدهم الإلكتروني أو حاسوبهم، دون أن يكون لدى المخترق، في معظم الأحيان، القدرة على الوصول إلى معدات متطورة تكنولوجياً أو أجهزة تجسس أو برامج خاصة بالقرصنة. بدلاً من ذلك، تُعزى معظم الاختراقات إلى مجرد تخمين كلمة السر الخاصة بالضحية.

أظهر استبيان أجري مؤخراً حول استخدام كلمة السر أنه ليس من الصعوبة بمكان اختراق معظم الحواسيب، فكلمة السر الأكثر استخداماً هي عبارة "كلمة سر" متبوعةً بـ "12345678". وتتضمن كلمات السر الأخرى التي يسهل اختراقها أرقام هواتف، أسماء، تواريخ ميلاد، أسماء مستعارة أو خليطاً من هذه المعلومات. أي أنّ تخمين الكثير من كلمات السر يصبح ممكناً باستخدام بعض البرمجيات الخاصة والقليل من المعلومات الشخصية التي عادة ما يتم الحصول عليها من مواقع التواصل الاجتماعي.

ولذا، ينصح موقع سايبر آرابز (Cyber Arabs) باستخدام كلمات سر لا تحتوي على معلومات شخصية وتتألف من مجموعة من الأرقام، الأحرف والرموز الخاصة (مثل %#^)؛ وكلما كان ترتيب مكونات كلمة السر عشوائياً أكثر، كلما أصبح من الأصعب تخمينه أو اختراقه. كما يجب أن تتكون كلمة السر من أربعة عشر رمزاً على الأقل حتى تكون آمنة.

يستخدم قراصنة الانترنت برامج خاصة تقوم بتجريب آلاف كلمات السر في الثانية، وبالتالي فإنكم تزيدون من صعوبة "تخمين" كلمة السر الخاصة بكم من قبل هذه البرامج كلما زدتم عدد رموزها. على سبيل التجربة، بإمكانكم الولوج إلى موقع http://howsecureismypassword.net لتكتشفوا بنفسكم كم من الوقت يلزم لاختراق كلمة سر ما باستخدام البرامج الخاصة.

بالطبع، نرجو أن لاتزودوا الموقع بكلمة السر الحقيقية الخاصة بكم.

ويُعد استخدام عبارة سرية أفضل بكثير من استخدام كلمة سر، ونعني بالعبارة السرية جملةً تتألف من كلمات عشوائية. ويفضل أن تتضمن بعض الرموز الخاصة. وعادة ما يكون من الأسهل تذكر العبارات السرية، كما يعني حجم هذه العبارات أن اختراقها يتطلب المزيد من الوقت. إلا أنه من المهم أن تستعملوا جملة غير منطقية كعبارة سرية، مثل:

bluebirdsaresittingnearthebalconystaircase!*!. جملة مثل هذه قد يستغرق فكها بواسطة حاسوب سريع عدة ملايين من السنوات. عندها، لن تمانعوا أن يقرأ أحد من أحفادكم البعيدين الرسائل الالكترونية الخاصة بكم.

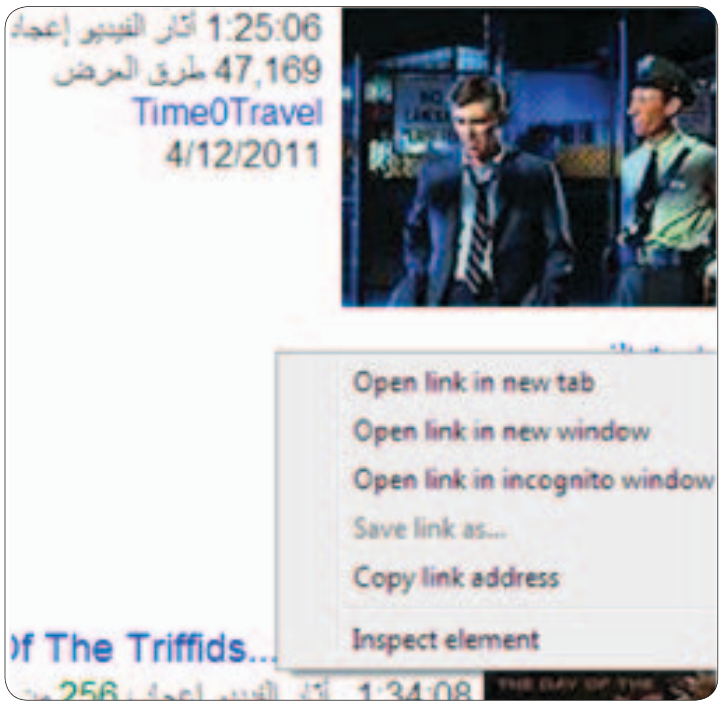
ولا يجب أن تُطلعوا الآخرين على كلمات السر الخاصة بكم أو أن تستخدموا كلمة سر واحدة في أكثر من تطبيق أو موقع؛ فأنتم حتماً لا تريدون أن يستطيع قرصان الانترنت، في حال تمكنه من الدخول إلى حسابكم للبريد الالكتروني، أن يدخل أيضاً إلى حسابكم على فيس بوك.

يوتيوب وخدمات الاتصال البطيئة

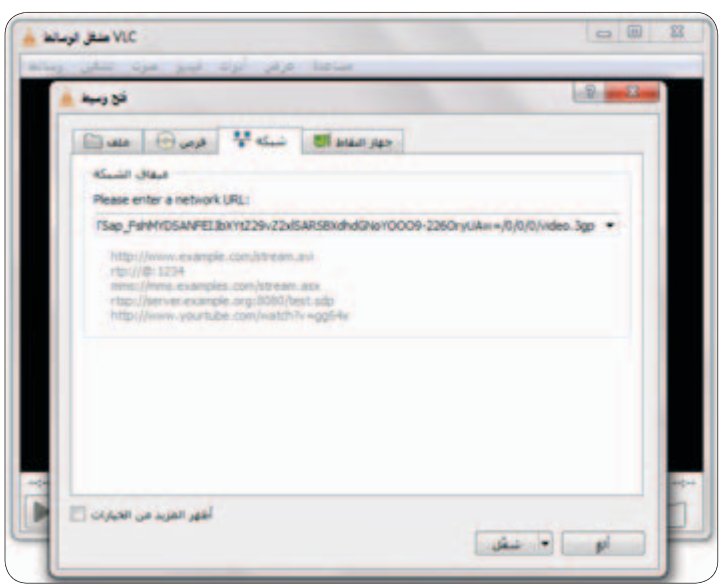
غيّر موقع يوتيوب YouTube وجه الإنترنت في السنوات الأخيرة. ويوتيوب هو الموقع الذي يستخدمه الملايين لمشاهدة الفيديوهات، والذي أصبح في دول "الربيع العربي" وسيلةً لمعرفة الأحداث الهامة. إلا أنّ يوتيوب يتطلب اتصال إنترنت سريع، وهو الأمر الذي لا يكون متوفراً دائماً، حتماً ليس في دول مثل سوريا، حيث انخفضت سرعة الإنترنت خلال السنة الماضية مع كون البعض ما زال يعتمد على خدمات الاتصال الهاتفي لاستخدام الإنترنت.

ولكن من حسن حظ مستخدمي خدمات اتصال الإنترنت البطيئة أن هناك حل لهذه المشكلة، إذ يقوم يوتيوب حالياً بتجريب خدمة جديدة تدعى يوتيوب فيذر(YouTube Feather) (للبدء باستخدام هذه الميزة توجهوا إلى http://www.youtube.com/feather_beta). وتقوم هذه الميزة بتعديل سرعة الفيديو وجودته تلقائياً لتتناسب مع سرعة خدمة الاتصال الموجودة فيصبح من الممكن مشاهدة هذا الفيديو رغم غياب اتصال سريع بالانترنت (وهو ما يعرف أيضاً باتصال الحزم العريضة Broadband Connection). للأسف لا يمكن استعمال هذه الميزة مع جميع الفيديوهات على موقع يوتيوب حالياً لأنها لا تتطابق معها، إلا أن يوتيوب كان قد وعد بتحسين قدرة هذه الميزة على تغطية عدد أكبر من الفيديوهات قريباً.

ففي حال بقي من الصعب عليكم أن تستخدموا خدمة Yo – Tube Feather بسبب البطء الشديد في خدمة الإنترنت لديكم، فهنالك طريقة أخرى لمشاهدة الفيديوهات، حتى باستخدام أبطأ خدمات الاتصال؛ قوموا بتنصيب برنامج مشغل الوسائط VLC Free Multimedia Player من الرابط:
http://www.videolan.org/vlc/index.html ومن ثم توجهوا إلى موقع يوتيوب للهاتف الجوال http://m.youtube.com. سيتم تشغيل أي فيديو تختارونه من خلال برنامج مشغل الوسائط VLC الذي يتطابق مع خدمات الاتصال البطيئة.
بعض متصفحات الإنترنت لا تفتح برنامج (VLC Player) تلقائياً. فإن حدث هذا، ما عليكم إلا النقر بالزر الأيمن على "مشاهدة الفيديو" (Play video link) واختيار (Copy link address) (أي نسخ عنوان الرابط). بعدها، قوموا بتشغيل برنامج VLC ومن ثم فتح قائمة



"وسائط" واختيار "افتح دفق الشبكة" (Open network stream)، وقوموا بلصق الرابط الذي نسختموه للتو في الحقل الذي سيظهر لكم (ctrl+v) ويصبح بإمكانكم مشاهدة الفيديو بمجرد النقر على زر التشغيل.



تخلصوا من البيانات الوصفية (Metadata) غير المرغوبة

عادة ما نرى حالات يعاني فيها البعض من المشاكل بسبب معلومات تسربت من البيانات الوصفية (Metadata) لملف ما من ملفاتهم، وهذه البيانات هي المعلومات الشخصية الموجودة في جميع الملفات التي تنتجونها. وكنا قد نشرنا مؤخراً تقريراً حول هذه المشكلة فيما يتعلق بالصور المأخوذة بواسطة الكاميرات الرقمية أو الهواتف الذكية (رابط).

ولكن الصور ليست وحدها عرضةً لهذه المشكلة، إذ تحمل تقريباً جميع الملفات التي تنشؤونها على حواسيبكم علامات تدل على هويتكم، وعادة ما تُكون هذه البيانات الوصفية نسخة عن المعلومات التي زودتم بها نظام التشغيل في حاسوبكم. ولذلك ينصحكم موقع سايبر آرابز بتجنب تزويد نظام التشغيل في حاسوبكم بمعلومات دقيقة (على سبيل المثال عدم تزويد النظام بأسمائكم الحقيقية).

لتغيير إعداداتكم الشخصية في ويندوز (Windows)، افتحوا قائمة "إبدأ" (Start menu) وانقروا بالزر الأيمن على أيقونة "جهاز الكومبيوتر" (My Computer)، ثم اختاروا "خصائص" (Properties) وستظهر نافذة جديدة تجدون فيها جميع المعلومات المعروفة عن جهازكم. في حال كنتم بحاجة إلى تغيير إسم جهازكم بحيث لا يشير بوضوح إليكم، بإمكانكم تغيير الإسم من خلال الرابط "تغيير الإعدادات" (Change Settings). هذا وتجمع البرامج الشائعة الاستخدام مثل مايكروسوفت وورد (Microsoft Word) معلومات شخصية عنكم وترفقها بملفاتكم. بإمكانكم تغيير هذه الإعدادات في برنامج وورد (Word) من خلال النقر على "ملف" (File) ومن ثم "خيارات" (Options).

تُعد أفضل طريقة لمنع تسرب المعلومات عن طريق البيانات الوصفية (Metadata) لملف ما أن تقوموا ببساطة بتجريد الملفات من هذه البيانات.

اوذلك بالنقر بالزر الأيمن على الملف المراد ازالة البيانات الوصفية (Metadata) منه ومن ثم النقر على "خصائص" (Options).

ثم "التفاصيل" (Details)، وبعدها على "إزالة الخصائص والمعلومات الشخصية" Remove Properties and Personal Information وختاروا "إزالة الخصائص التالية من هذا الملف" (Remove the following properties from this file)، ومن ثم انقروا على "تحديد الكل" (Select All)، وبعدها على "موافق" (Ok).

وبذلك تكون تمت إزالة معظم البيانات الوصفية من الملف. ولكن هذه الطريقة قد لا تعمل مع بعض انواع الملفات مثل ملفات الـ pdf وبعض انواع الصور.

كذلك يمكنكم استخدام برامج خاصة تدعى "Scrubbers". برنامج "Doc Scrubber"، على سبيل المثال، خاص بملفات مايكروسوفت وورد وهو مجاني وسهل الاستخدام، وبإمكانكم تحميله من هنا. يُمَكّنكم هذا البرنامج من اختيار ملف وورد (أو مجموعة من الملفات) وتجريده من بياناته الوصفية بنقرة واحدة دون أن يطرأ أي تعديل على الملف الأصلي. ولكن للأسف لايوجد في السوق حالياً أية أدوات آمنة وسهلة الاستخدام لتجريد ملفات الـ PDF من بياناتها الوصفية، إلا أنه بإمكانكم، في حال كان لديكم برنامج Adobe Acrobat في جهازكم، استخدام أداة "فحص المستند" "Examine Document" التي ستبحث عن أية معلومات مخفية في المستند.

وفيما يتعلق بالصور، من المفيد أن تفكروا بإيقاف خاصية تحديد الموقع في هواتفكم الذكية أو كاميرتكم الرقمية حتى لا تحمل أيٌّ من صوركم هذه المعلومات. هناك الكثير من الأدوات السهلة الاستخدام التي تمكنكم من تجريد صوركم من البيانات الوصفية (Metadata) (التي يشار إليها أيضا بـ"إكسيف داتا" EXIF Data وهي تعني "صيغة ملف صوري متبادل"). بإمكانكم العثور على ثلاثة من البرامج التي اختبرناها هنا، وهنا، وهنا.

أهمية برامج مسح الفيروسات

برامج مسح الفيروسات هي أدوات في غاية الأهمية لضمان أمن مراسلاتكم عبر الإنترنت. إلا أن فريق سايبر آرابز قد لاحظ أن العديد من القراء لم يقوموا بتنصيب هذه البرامج، أو لم يقوموا قطّ بتحميل أي تحديثات للبرامج التي يملكونها، وهي تحديثات أساسية لضمان حسن عمل البرنامج.

في الأشهر القليلة الماضية، وقع العديد من الناس في العالم العربي، لا سيما في سوريا، ضحية هجمات إلكترونية نفذتها مجموعات مناصرة للحكومة. في بعض الحالات، تم تنصيب برمجيات خبيثة على أنظمة تشغيل أجهزة الحواسيب المصابة، وهذه البرمجيات قادرة على القيام بعمليات تجسس. ولأن الهجمات نادراً ما تتم ملاحظتها، فإن نسبة كبيرة من قراء سايبر آرابز تتم حالياً مراقبة حواسيبهم بواسطة برمجيات خبيثة.

إذا أردتم أن تتمتعوا بالأمان، إحرصوا على تنصيب برنامج لمسح الفيروسات. من المهم أن يكون مصدر هذا البرنامج موثوقاً. في بعض البلدان، يتم بيع نسخ مقرصنة من هذه البرامج في الشارع أو يتم تنصيبها في المتاجر التي تبيع أجهزة الحواسيب. يجب العلم أن هذه المصادر غير آمنة، لأن هناك طرفاً ثالثً من الممكن أن يكون قد غير محتوى البرنامج لخدمة غاياته الخبيثة.

أحد برامج مسح الفيروسات الذي نوصي به هو أفيرا Avira. يمكن تحميل نسخة مجانية منه على الإنترنت، كما يمكن النفاذ إلى الموقع وتحديثات البرنامج في البلدان التي تخضع لحظر تصدير من قبل الدول الغربية. يمكن تحميل النسخة المجانية من برنامج Avira هنا:

http://www.avira.com/en/avira-free-antivirus

حذف الملفات نهائياً

يبدو التخلص من البيانات الموجودة على حاسوبكم عملية بسيطة، تتطلب النقر على الملف الذي تريدون التخلص منه واختيار "حذف" (Delete) ومن ثم إفراغ سلة المحذوفات. على الأقل، هذا ما يجعلنا نظام التشغيل نعتقده، وقلة من الأشخاص فقط تدرك أنّ الملفات المحذوفة تبقى موجودةً على القرص الصلب حتى بعد إفراغ سلة المحذوفات، بحيث يمكن لأي شخص يمتلك الأدوات المناسبة استعادة معظم هذه الملفات بسهولة شديدة وخلال ثوان قليلة.

ويعود هذا إلى الطريقة التي يتعامل بها نظام التشغيل مع الملفات، فهو لا يحذف الملف، بل يحذف الإشارة إليه فقط مبقياً على الملف كما هو إلى أن تتم الكتابة فوقه.

كما هو الحال، على سبيل المثال، عند حذف فصل من فهرس كتاب ما دون أن يؤدي ذلك إلى حذف الفصل من الكتاب نفسه.

لتتمكنوا من حذف الملفات نهائياً دون أن يتمكن أحد من استعادتها، أنتم بحاجة إلى برامج خاصة تقوم بحذف الملف غير المرئي الموجود على القرص الصلب، مثل برنامج Eraser العملي والمتوفر مجاناً ومفتوح المصدر. يمكن تحميله من هذا الرابط:

http://eraser.heidi.ie/download.php.

بعد أن تقوموا بتنصيب البرنامج، قوموا بتشغيله كـ"Administrator mode" أي "نمط المسؤول" وذلك من خلال النقر على الزر الأيمن على أيقونة البرنامج واختيار "Run as administrator".

بعد التشغيل، قوموا بالنقر على السهم المتجه إلى الأسفل والملاصق لعبارة "Erase Schedule" والتي تعني "جدول الحذف".

اختاروا من القائمة التي ستظهر لكم "New Task" أي "مهمة جديدة"، وسيؤدي هذا إلى فتح نافذة جديدة تختارون منها "Run manually" أي "التشغيل يدوياً". بعدها أنقروا على "Add data" أي "إضافة بيانات"، وستظهر لكم نافذة جديدة.

ستسألكم هذه النافذة الأخيرة عن المكان الذي تريدون حذف الملفات منه. في حال كانت هذه أول مرة تقومون فيها بتشغيل برنامج Eraser، فأفضل ما يمكنكم القيام به هو النقر على "Unused disk space" أي "المساحة غير المستخدمة في القرص"، وسيقوم هذا الخيار بتدمير جميع الملفات التي قمتم بحذفها وإفراغها من سلة المحذوفات سابقاً. كما يمكنكم اختيار ملف معين أو جميع الملفات التي ما زالت موجودة في سلة المحذوفات.

الرجاء الانتباه إلى أنّ استخدام هذه الطريقة لحذف ملفات مايكروسوفت أوفيس لن يغنيكم عن تشغيل خيار "Unused disk space" لاحقاً وذلك لأن برنامج أوفيس يترك نسخاً مخبأة من الملفات على السواقات.

بعد اختيار المكان أو الملفات، استمروا بالنقر على "OK" حتى تعودوا إلى النافذة الأولى، حيث سترون مهمة الحذف "Erase Task" التي أوجدتموها للتو.

أنقروا على المهمة بالزر الأيمن واختاروا "Run Now" أي "التشغيل الآن" وسيقوم برنامج Eraser بتدمير ملفاتكم المحذوفة أو تلك التي اخترتموها تدميراً نهائياً.

http://www.youtube.com/watch?v=WBYiD_D2bHM