cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

العدد ٣
مايو/أيار ٢٠١٢

«التروجان» السياسي!

تقارير عن استهداف أجهزة حاسوبٍ تعمل بنظام «ماك»

مقابلة مع رونا سانفيك احد مطوري برنامج تور

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

أخرج المجلة:
MGSA
لصالح شركة:
tm

للإتصال بنا:
magazine@cyber-arabs.com

تابعنا على:

مقدمة

سوزان فيشر

إنّ التمتّع بالحماية أثناء استعمال الإنترنت هو عملية مستمرّة، فليس بمقدوركم مثلاً أن تعتبروا أنّكم آمنون لمجرد القيام بإجراءٍ معيّن، إذ لا تنفكّ التحدّيات والمخاطر الجديدة تظهر كلّ يوم. تكشف القصة التي تتصدّر غلاف هذا العدد عن واحدٍ من هذه التحدّيات، وهو هجومٌ إلكترونيٌ موجّه قامت به جهات سوريّة.

يصف أعضاء فريق «سايبر آرابز» في هذا المقال كيف فحصوا جهاز حاسوب مصاب ببرمجيةٍ خبيثةٍ، كان مصدرها عنوان بروتوكول إنترنت سورياً. فكانت صاحبة الجهاز قد فتحت مستنداً تلقّته عبر «سكايب»، ظانّةً أنّ مرسله هو أحد النشطاء الذين تعرفهم، بينما من كان يجلس إلى جهاز الحاسوب في الطرف الآخر لم يكن سوى عناصر أمنٍ سوريّين وقع هذا الناشط في قبضتهم، فاستعملوا جهازه للإتصال برفاقه، منتحلين شخصيّته.

سمح هذا التروجين (Trojan) لمرسليه التحكم الكامل بجهاز الحاسوب المصاب، فاستطاعوا رؤية كل ما كانت تقوم هذه الناشطة بطباعته على لوحة المفاتيح، والنفاذ إلى كل كلمات السر الخاصة بها، والولوج إلى حسابات «الفيسبوك» والبريد الإلكتروني التي تملكها، وحتى تشغيل «الويبكام» في جهازها عن بعد.

وليست هذه البرمجية الخبيثة هي الوحيدة التي تستهدف الناشطين. فهذه الحادثة ودرجة التعقيد التي ميّزتها تبيّن أهميّة الحفاظ على الحد الأدنى من تدابير الأمن الأساسيّة؛ فالبقاء بمأمنٍ في العالم الرقمي هو تحدٍ مستمرٌ.

لذا، فقد كان فريق «سايبر آرابز» منهمكاً في الأشهر الأخيرة، ليس بالتحقيق في هجماتٍ عبر البرمجيّات الخبيثة فحسب، بل أيضاً بالإجابة عن سؤالٍ لا يقلّ صعوبةً عن هذه المهمة: كيف يمكننا البقاء آمنين لدى استخدام الهاتف المحمول؟ فغالباً ما يعتمد الصحافيون والناشطون في عملهم على الهاتف المحمول، إذ يقومون باستعماله لتخزين البيانات الحسّاسة والأسماء المرفقة بأرقام الهواتف، واضعين بذلك شبكات كاملة من الناشطين في دائرة الخطر، إذا ما وقعت هواتفهم في الأيدي الخاطئة.

فقد اطّلع فريق أمن الهواتف المحمولة في «سايبر آرابز» على المنتديات الخاصة بهذه الهواتف، للوقوف عند ما تقدّمه – أو لا تقدّمه – من حلول. فمعظم النصائح التي نقدّمها مرتبطةٌ بالهواتف التي تعمل بنظام التشغيل «أندرويْد»، الذي، وبرأينا، يقدّم أفضل سبل الحماية حتى الآن، لا سيّما نسخة «أندرويد ٤» من هذا النظام.

لذا، وابتداءً من هذا العدد، لن تقوم مجلة «سايبر آرابز» بتقديم آخر ما يتعلّق بالأمن الرقمي فحسب، بل ستقوم أيضاً بعرض آخر المعلومات حول أمن الهواتف المحمولة. وكالعادة، إذا كانت لديكم أسئلة حول أيّ من الموضوعين، تفضّلوا بطرحها لأنّنا سنكون مسرورين بمساعدتكم. أرسلوا أسئلتكم إما عبر منتدانا على الإنترت، أو عبر صفحة «سايبر آرابز» على «الفيسبوك» (وبالطبع، سنكون في غاية السعادة إذا قمتم بإبداء إعجابكم بالصفحة).

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

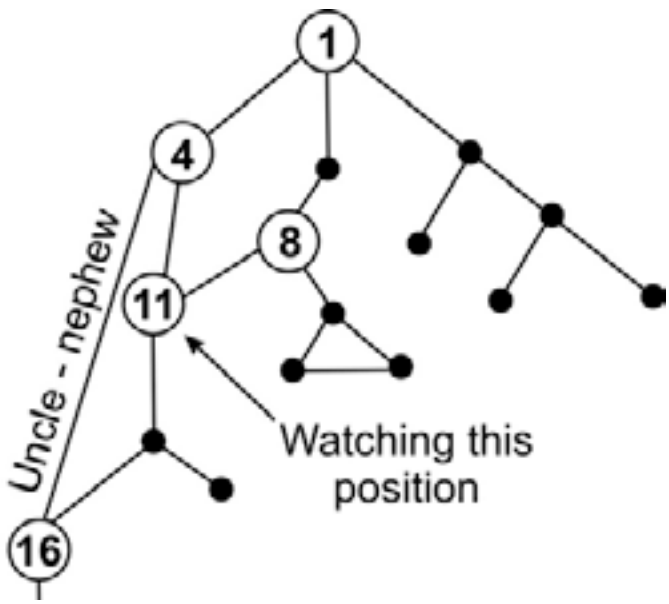
الشبكات الاجتماعية وجبة دسمة لأنظمة الإستخبارات

مقدمة:

ظهر الرئيس العراقي السابق صدام حسين بعد سقوط حكمه في منطقة الأعظمية في بغداد، فكانت آخر لقطة له برفقة رجل سمين كان يُعتبر مرافقه الأساسي آنذاك. كان المرافق يقوم بحماية صدام حسين من المؤيّدين الملتفين حوله، ومن ثم صعد برفقته الى السيارة؛ غاب صدام حسين بعد ذاك اليوم.

إعتبرت الإستخبارات الأميريكيّة أنّ العقيد محمد إبراهيم المسلط -- أو «الرجل السّمين» كما يسمّونه -- سيكون المفتاح الأساسي للوصول إلى صدام حسين، وعلى هذا الأساس قامت بجلب خبراء في تحليل الروابط الاجتماعية من أجل الوصول إليه.

بدأت الحكاية عندما قام خبراء الشبكات الإجتماعية برسم شجرة العائلة الخاصة بمرافق صدام حسين (الرجل السمين) ومحاولة تحديد أكثر العناصر قرباً إليه. وبالفعل، بدأت الإعتقالات بحسب الشبكة وبحسب المستويات الأقرب إليه، بدءاً من أولاد أخيه ووصولاً إلى أخيه الأصغر. ضمّت قائمة المطلوبين آنذاك ٢٠ إسماً من الأشخاص الذين درسوا تحركاتهم أيضاً، واكتشفوا أنّ أغلبهم كانوا يقدّمون الدّعم لصدام حسين. تراوح هذا الدعم ما بين التنسيق المالي وتنسيق حركته لتغيير مكانه وتأمين المواد الغذائية... إلخ. جميع التحليلات السابقة، وخلال أقل من ٢٤ ساعة بعد أول اعتقال، أوصلت الإستخبارات الأميريكية إلى «الرجل السمين»، والذي بدوره، وتحت تأثير التعذيب، قام بتوجيه القوات الأميريكية إلى مكان اختباء صدام حسين في مزرعة، فتمّ العثور عليه متخفّياً في نفق تحت الأرض.



الشبكات الإجتماعية:

تختلف الروابط الاجتماعية بأنواعها وبحسب الأسس القائمة عليها؛ فيوجد منها العائلية، الصداقة، روابط العمل، التوجه السّياسي... إلخ. كما تختلف قوّة هذه الروابط بحسب المناطق الجغرافية المتواجدة فيها؛ ففي مجتمعنا الشرقي على سبيل المثال، تعتبر الروابط العائلية من أكثر الروابط قوّةً وهي المفتاح الأساسي للوصول إلى أيّ شخص. وتعتبر الروابط الإجتماعية القائمة على العمل واحدة من المفاتيح الرئيسيّة أيضاً للوصول إلى أماكن تواجد الأشخاص واهتماماتهم المختلفة.

عمل أجهزة الإستخبارات على التحليل:

تقوم الأجهزة الإستخباراتية، إذا رغبت بالوصول إلى شخص معيّن، بدراسة روابطه الإجتماعية وطبيعتها ولاسيّما الطبقات العليا منها والتي تحيط به مباشرة. لذا، وبهذه الخطوات التحليلية، يتمّ رسم الشكل الكامل للعلاقات الإجتماعيّة التي يقيمها ومدى قوتها، ممّا يؤدي في النهاية إلى تحديد التواجد الجغرافي للشخص المعني.

على سبيل المثال، إن كان الشخص المعيّن يقوم باستخدام أداة اتّصال غير مسجلة باسمه الحقيقي ولكن في المقابل يتواصل مع أقربائه الذين يحملون أدوات اتصال تحمل أسماءهم الحقيقية أو حتى تلك التي تُحدَّد بأماكن تواجدهم الجغرافي، سيكون كشف مكانه بسيطاً جداً.

الشبكات الإجتماعية الإلكترونية:

قامت العديد من الشركات بتطوير تطبيقات ويب (مواقع إنترنت) تقوم على إنشاء ملف شخصي للأشخاص المسجّلين والذين بدورهم يقومون بتزويد ملفاتهم بمعلومات شخصية على صعيد العمل والدراسة والعائلة والاصدقاء والآراء السياسية والدينية، بالإضافة إلى التواجد الجغرافي والإهتمامات، وصولاً إلى أدقّ التفاصيل، كتوقيت حضور فيلم معين في السينما على سبيل المثال.

تلك المعلومات ليست عبثية ولا يمكن تزويرها بسهولة، فهي عبارة عن دوائر اجتماعية يتمّ بناؤها طوال فترة تواجدكم على شبكات التواصل الاجتماعي. فكلّ جملة تتمّ كتابتها أو صورة يتمّ وضعها تشكل جزءاً يبني هذه الدائرة التي من الممكن استثمارها في المستقبل.

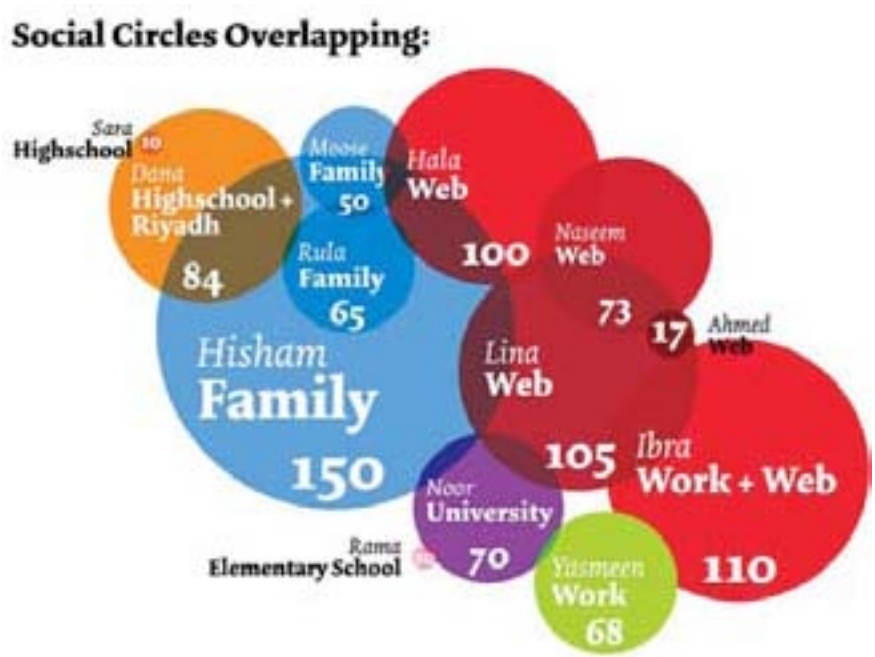
عبّر الرئيس الأمريكي باراك أوباما في أحد لقاءاته مع بعض الطلاب عن خوفه من انتهاك الخصوصيّة على شبكات التواصل الإجتماعي، مما قد يؤثر على مستقبل مستخدمي هذه الشبكات. فالكثير

من السّاعين إلى الحصول على وظيفةٍ لم يتم قبولهم في سوق العمل بسبب أفعالٍ طائشةٍ قاموا بالإعلان عنها في وقت سابق على شبكات التواصل الإجتماعية.

ما يلي مثال على ذلك: ناشطٌ في مجالٍ معيّن تحاول السلطات الوصول إليه واعتقاله، يقوم بالدخول إلى حساب «الفيسبوك» الخاص به وإجراء نشاطات فيه. يظهر من خلال التعليقات أنّه على تواصلٍ قويٍّ مع الشخص س١، وقد تحدّثا عن جلسة عشاءٍ معيّنة حضراها سويةً. لذا، لقد أصبح من المعروف أنّ الناشط المعني يلتقي بالشخص س١ بشكل شخصي، وسيتحول مجرى البحث كاملاً من الناشط الى س١، رغم أنّ الأخير غير مطلوب.

سيتم عندها محاولة مراقبة الإتصالات أو تحليل ملف الشخص س١ فيما يتعلّق بعمله وأصدقائه وأقربائه، إلى أن يتمّ الوصول إليه واعتقاله، وبالطبع، سيكون اعتقاله أسهل بكثير من اعتقال الناشط.

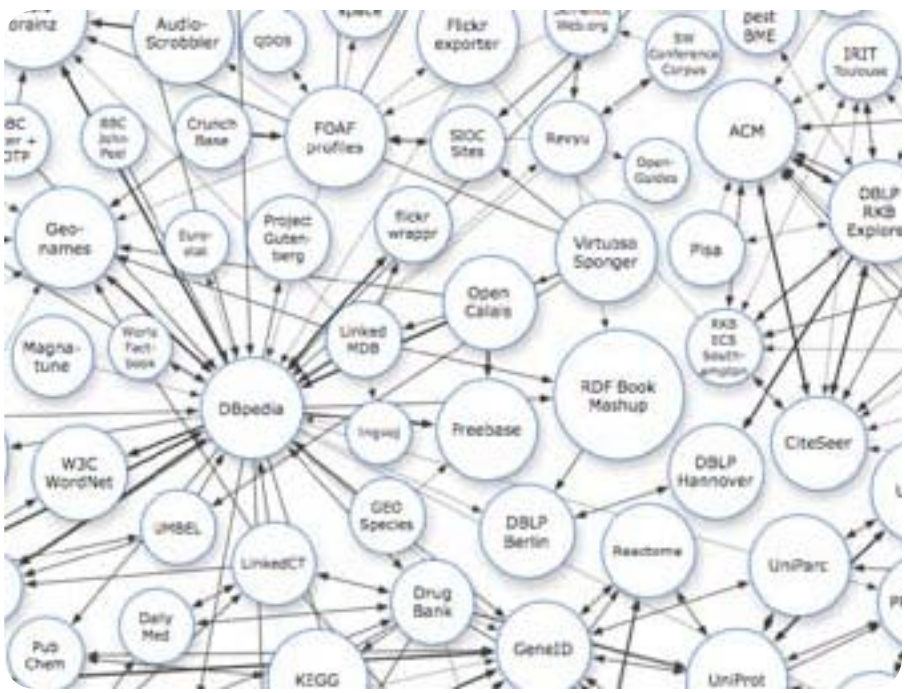
عندها يصبح من الممكن، لا بل من السهل، الضغط عليه تحت الإعتقال ومعرفة مكان إقامة الناشط المطلوب والقيام باعتقاله.



البيانات المبعثرة:

قد نحاول قدر المستطاع إخفاء صورٍ لنا كانت قد أُخذت في ظروفٍ معينةٍ من على صفحات «الفيسبوك» من أجل زيادة درجة الخصوصيّة والحماية اللّتين نتمتّع بهما، ولكن في حال كنّا من المدوّنين والنّاشطين الإلكترونيين ولدينا تاريخٌ على شبكة الإنترت يسبق ظهورنا على «الفيسبوك»، سيكون من السّهل البحث عن صورة شخص معين بواسطة محرّك البحث «غوغل» والتي قد تكون قد نُشرت بواسطة مدونات أو مواقع معينة نشرت مقالات لنا، فسيتم من خلالها كشف صورنا الشخصية بالإضافة إلى عناويننا الإلكترونية وبعض توجّهاتنا الفكرية.

حتى عناوين البريد الإلكتروني الخاصة بكم قد تكون مدخلاً لكشف هويتكم؛ قد يكون شخصٌ ما كتب عنوان بريدكم الإلكتروني على صفحةٍ معيّنةٍ مرفقاً بإسمكم. يصبح عندها من السهل الحصول عليه ومحاولة اختراقه من قبل «الهاكرز» الذين سيقومون بدورهم بالوصول إلى عدّة حساباتٍ خاصةٍ تملكونها في عدة مواقع إلكترونية، كمواقع التواصل الإجتماعي، على سبيل المثال، التي تعتمد على هذا البريد الإلكتروني.



تعتبر البيانات المبعثرة على شبكة الإنترنت من أخطر العوامل التي يجب الحذر منها ومحاولة التخلص منها في أوقاتٍ معينة، إذ يجب التواصل مع من يقوم بنشر تلك المعلومات من أجل حذفها وعدم تعريضكم لعملية تجميع بيانات معينة تخصكم وإعادة هيكليتها لتكشف أموراً قد تعرضكم للخطر مستقبلاً.

إستمرار تدفق البيانات:

إنّ استمرار تدفق البيانات من تلك المصادر نفسها التي تحدثنا عنها يُعتبر أمراً في غاية الخطورة. فعلى سبيل المثال، قد يفيد النشاط الدائم على الشبكات الإجتماعية وكتابة أخبار ونشر صور بتحديد موقعكم الجغرافي أو هوية الأشخاص الذين تتواصلون معهم، بالإضافة إلى شكل هذا التواصل ودوائركم الإجتماعية، مما قد يعرّضكم لما يسمّى بتجميع البيانات وإعادة تحليلها بعد فترة، ويضع الشخص وشبكته المقربة في مأزقٍ حقيقي. لذا، يجب إيقاف مصادر تدفّق المعلومات وتمويه التواصل الإجتماعي وعدم كشفه للعلن ورفع درجة الخصوصية بشكلٍ كبيرٍ، بالإضافة إلى إجراء بحثٍ دوري عن طريق محركات «غوغل» عن المعلومات الشخصيّة الخاصة بكم (صور، بريد الكتروني... إلخ) ومحاولة حذفها.

الحماية

يجب الإلتزام بالخطوات التالية:

١- عدم استخدام الأسماء الكاملة في صفحات التواصل الإجتماعي

٢- محاولة استخدام برامج للتخفي عند الدخول للتصفح كبرنامج Tor

٣- عدم وضع الروابط العائلية أو إظهارها

٤- عدم كتابة أية معلوماتٍ تخص العمل حتى لو كانت قديمة

٥- عدم التواصل مع الأصدقاء الذين تعرفونهم في الواقع بشكلٍ مكشوفٍ على صفحات التواصل الإجتماعي

٦- عدم تحديد موقعكم الجغرافي

٧- عدم التحدث عن ظواهر عامة تحصل (كنزول الأمطار، صوت انفجار، إشتباكات، حركة أمنيّة معينة) فقد تكون مصدراً لمعرفة موقعكم الجغرافي

٨- عدم ربط بريدكم الإلكتروني المعروف بحساباتكم الأخرى كصفحات التواصل الاجتماعي

٩- عدم إظهار أرقام الهاتف الخاصة بكم

١٠- رفع درجة الخصوصية لأعلى مستوى على الصفحات الإجتماعية

١١- عدم كشف صفحاتكم لأشخاص غير موثوقين أو التواصل معهم

١٢- التأكد من حماية أجهزة الحاسوب خاصتكم

«التروجان» السياسي!

«سأقوم بإرسال الخطة الطبيّة إليكِ، قومي بتلقّي الملف ونشره على المجموعة»

تحت غطاء هذه الجملة قام الدكتور (X) الذي كان قد تمّ اعتقاله قبل ساعةٍ بإرسال ملفٍّ يحتوي على برنامجٍ خبيثٍ (تروجان) إلى الناشطة التي كانت تعمل معه بما يخص المساعدات الطبيّة في سوريا.

ففي بداية شهر شباط/فبراير من العام الحالي، إستقبل فريق Cyber-Arabs جهاز حاسوبٍ مصاباً يعود لإحدى الناشطات التي خسرت حساب «الفيسبوك» الخاصّ بها، بالإضافة إلى حساب بريدها الإلكتروني وحساب «السكايب» الخاص بها، وذلك لكونها استقبلت ملف «الخطة الطبيّة» المشار إليه أعلاه.

عند بدء فحص الجهاز، تبيّن أنه مصابٌ ب «تروجان» وهو نسخة مطوّرة من تطبيق «دارك كوميت» (DarkComet) المجاني، والتطبيق صُمّم بالأساس للتحكّم بالأجهزة وإدارتها عن بعد.

يقوم «التروجان» بالسّيطرة الكاملة على الحاسوب عبر زرع ما يسمى الـ Keylogger والذي يقوم بتسجيل جميع ضربات لوحة المفاتيح (Keyboard) في جهازكم، مما يعني أنّ البيانات التي تحتفظون على جهازكم مثل كلمات السر، وعناوين البريد الإلكتروني، وعناوين المواقع الإلكترونية، ونصّ الدردشة، إلخ. يتمّ تسجيلها في ملفٍّ نصي ومن ثم رفعها الى مخدم (Server) عائدٍ لمصمّمي «التروجان».

لا يقتصر عمل هذا «التروجان» على زرع الـ Keylogger فحسب، بل يستطيع البرنامج أيضاً فتح «الويب كام» (Webcam) والتجسّس عليكم، وفتح الميكروفون والتنصّت على الحديث الذي تتبادلونه مع الآخرين، كما أنّ «التروجان» يمتلك القدرة على تغيير شكله وزراعة «تروجان» آخر في حال تم كشفه.

إتضّح أنّ «التروجان» الذي زرعه ملف «الخطة الطبيّة» يقوم بتجميع كل البيانات المسروقة ورفعها لمخدم يحمل الـ IP address التالي: 28.0.6.216. والذي تبيّن فيما بعد أنّه عائدٌ لوزارة الإتّصالات السوريّة.

قام فريق عمل Cyber-Arabs ، وبعد الإنتهاء من تحليل الملف، بالتواصل مع شركة Symantec التي قامت بتصنيف «التروجان» وإيجاد مضاد له.

تمّت تسمية «التروجان» بـ Backdoor.Breut ومن ثم تمّ تعميم تفاصيل الملف على باقي شركات مكافحة الفايروسات من أجل

حماية أكبر عددٍ ممكنٍ من المستخدمين.

بعد انتشار هذا «التروجان» قام المبرمج الأساسي للأداة DarkComet بتطوير أداة تساعد على كشف «التروجان» في حال كان متواجداً في الجهاز:

لم يقتصر الأمر على ذلك، ففي تاريخ ١٥ آذار/مارس ٢٠١٢ قام الموقع التابع «لمؤسسة الحدود الإلكترونية» (EFF) بنشر تقرير يتحدّث عن موقعٍ إلكتروني، وهو نسخةٌ مزوّرةٌ من موقع يوتيوب، يقوم بتحميل «تروجان» مطابق لذلك الذي سبق الحديث عنه وتبيّن فيما بعد أنه أيضاً يرسل المعلومات إلى خوادم سوريّة.

إنّ استعمال برامج حماية الحاسوب مثل AntiVirus و Firewall وتحديث نظام التشغيل بشكلٍ مستمرٍّ أمرٌ ضروريٌ جداً لبقاء نظام تشغيل الحاسوب آمناً بشكلٍ شبه دائم. وعلاوةً على ذلك، يجب الإمتناع عن استقبال ملفاتٍ من مصادر غير معروفة، كما يجب التنّبه إلى الظروف التي تترافق مع تلقّي رسالة معيّنة، مما قد يساهم في معرفة نوايا المرسل وما إذا كان محتوى الرسالة خبيثا أم لا. إنّه لأمرٌ في غاية الأهميّة أن تبقوا بعيدين عن البرامج الخبيثة التي قد تعرّض خصوصيّتكم -- بالإضافة إلى تعريضكم وأصدقائكم شخصياً -- للخطر.

كيف تحمون أنفسكم من البرمجيّات الخبيثة التي تنشرها الحكومة السوريّة

بدأت تصلنا تقارير منذ بضعة أسابيع عن «تروجان» -- وهو برنامجٌ خبيثٌ يتيح التجسّس على أجهزة الحاسوب والتلاعب بها - يُسمّى «دارك كوميت رات» (DarkComet RAT)، يهاجم أجهزة حاسوب تعود لناشطين سوريّين. ويتيح هذا «التروجان» تسجيل عمل «الويبكام»، ومنع بعض البرامج المضادة للفيروسات من القدرة على تنبيه المستخدمين من إصابة أجهزتهم، وتسجيل الطباعة على لوحة المفاتيح، وسرقة كلمات السرّ، بالإضافة إلى أنشطة أخرى. واتّضح أن هذا «التروجان» يقوم بإرسال المعلومات إلى خادم يحمل عنواناً (IP Address) سورياً. يمكنكم الإطّلاع على التقرير والتوصيات ذات الصلة التي وضعتها شركة «سيمانتك» (Symantec) هنا.

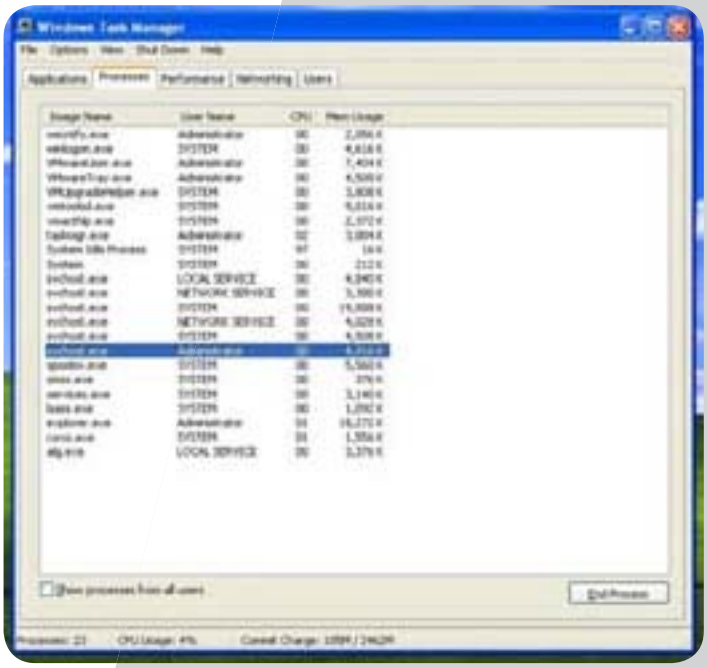
أمّا حالياً، فقد رأينا تقارير عن برنامج خبيث آخر يسمى «إكستريم رات» (Xtreme RAT)، وهو يقوم بإرسال المعلومات إلى الخادم ذي العنوان نفسه في سوريا. كما أنّه يبدو أنّ ظهوره يسبق ظهور «الدارك كوميت رات». تشير التقارير إلى أنّ هذا «التروجان» ينتشر عن طريق البريد الإلكتروني وبرامج الدردشة، وأنه يتمّ استعماله بهدف تسجيل الضربات على لوحة المفاتيح وأخذ صور للشاشة في الحاسوب المصاب، ومن المحتمل أيضاً أن يكون قد تمّ اختراق خدمات أخرى على أجهزة الحاسوب المصابة.

يتوجّب عليكم اتخاذ خطوات معينة من أجل حماية جهازكم من الإصابة، وهي ألا تقوموا بتشغيل أية برمجيّات حصلتم عليها عن طريق البريد الإلكتروني، وألا تقوموا بتنصيب أي برنامج لم تحصلوا عليه عن طريق التصفّح الآمن عبر استخدام (HTTPS)، أو برنامج حصلتم عليه من مصادر غير معروفة، حتى إذا كان قد نُصح باستعماله عبر الدعايات التي تظهر في النوافذ المنبثقة (Pop-up Ads) أو من قبل أحد الأصدقاء. كما وتنصح «مؤسسة الحدود الإلكترونية» (EFF) بتحديث نظام التشغيل في جهاز الحاسوب الخاص بكم بشكل دائم، وذلك عبر تحميل التحديثات الأمنية التي توفّرها الشركة المنتجة لنظام التشغيل. فلا تقوموا باستخدام نظام تشغيل قديم لا توفّر له الشركة المنتجة التحديثات المطلوبة.

إن إيجاد أيٍّ من الملفات أو الإجراءات التالية في جهاز الحاسوب الخاص بكم يظهر أنّه معرّض للتهديد من التروجان المذكور، «إكستريم رات»، وأيّة علامات إضافية هي دليل أقوى على وجود هذا التهديد.

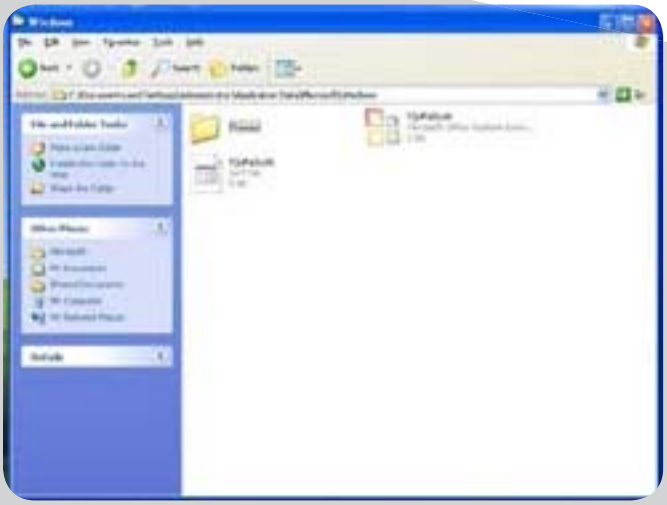
كيف تكتشفون عمل «إكستريم رات» لدى استخدامكم نظام «ماكروسوفت ويندوز» (Windows) Microsoft:

١. توجّهوا إلى «منظم المهمات في الويندوز» (Windows Task Manager) عبر الضغط على Ctrl+Shift+Esc، ثم أنقروا على زر «الإجراءات» (Processes).
إبحثوا عن إجراء إسمه svchost.exe وهو يعمل تحت إسم المستخدم الخاص بكم. في المثال التالي، يُشار إلى المستخدم باسم Administrator.



٢. إفتحوا «مستندات» (Documents) ومن ثم مجلّد «الإعدادات» (Settings)؛ أنقروا على إسم المستخدم الخاص بكم في المثال الحالي الإسم هو («Administrator») ؛ أنقروا على «جميع البرامج» (All Programs)؛ أنقروا على «الإقلاع» (Startup). إبحثوا عن رابط مشار إليه بكلمة «Empty»، وهي العلامة أنّ الجهاز الخاص بكم مصابٌ بهذا «التروجان».

٣. إفتحوا مجلد «مستندات وإعدادات» (Documents and Settings) أنقروا على إسم المستخدم الخاص بكم («Administrator» في هذا المثال)؛ إفتحوا مجلّد «الإعدادات المحلية» (Local Settings)، ثم مجلد «الملفات المؤقتة» (Temp)؛ إبحثوا عن الملفين: _$SdKdwi.bin و System.exe. إذا كان خيار «إظهار تذييل الملفات» (Display File Extension) مشغّلاً، سيظهرالملف تحت إسم System.exe، أما إذا كان الخيار معطّلاً، فسيظهر الإسم كالتالي System Project Up-date DMW.



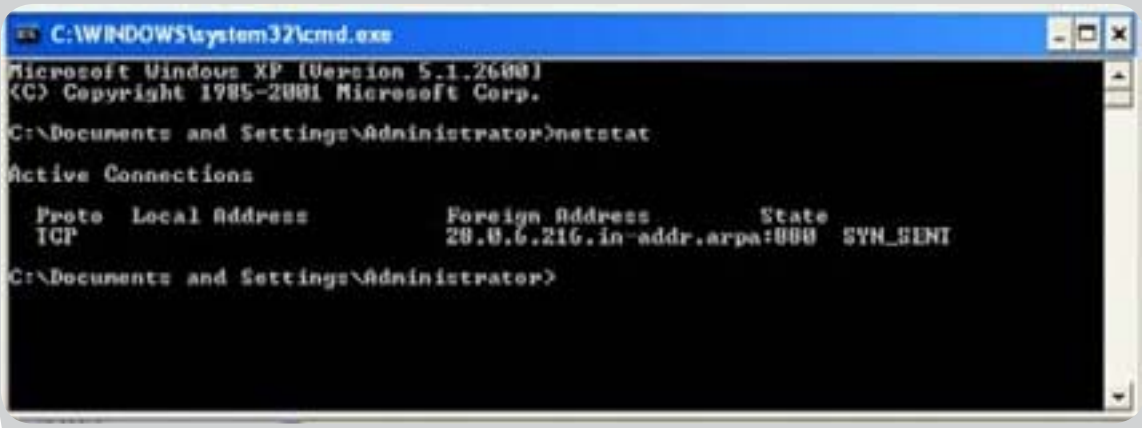
٤. إفتحوا مجلد «مستندات وإعدادات» (Documents and Settings) ثم أنقروا على إسم المستخدم الخاص بكم («Administrator» في هذا المثال)؛ إفتحوا مجلد «الإعدادت المحلية» (Local Settings)، إفتحوا مجلّد «بيانات التطبيقات» (Application Data) ؛ إفتحوا مجلد «مايكروسوفت» (Microsoft)؛ إفتحوا مجلد «ويندوز» (Windows)؛ إبحثوا عن الملفين: fQoFaScoN.dat و. fQoFaScoN.cfg.

٥. أنقروا على زر «البداية» (Start)؛أنقروا على «تشغيل» (Run) ثم إطبعوا كلمة «cmd» لفتح نافذة التحكم، ثم إطبعوا كلمة «netstat». إبحثوا في لائحة الإتصالات الفاعلة (Active Connections) عن إتصالٍ خارجٍ باتجاه ال IP Address التالي: 216.6.0.28.

ما الذي يتوجب عليكم فعله إذا كان حاسوبكم مصاباً بهذا «التروجان»:

إذا كان حاسوبكم مصاباً فإنّ إزالة الملفات المذكورة أو استعمال برامج مضادة للفيروسات لإزالة هذا «التروجان» لا يضمن أنّ جهازكم أصبح في مأمن. إذ يمكن هذا «التروجان» الجهة المهاجمة من تنفيذ نص برمجة إعتباطي في الجهاز المصاب. فلا توجد ضمانةٌ بأنّ الجهة المهاجمة لم تقم بتنصيبٍ برمجيّات خبيثة إضافيّة أثناء سيطرتها على الجهاز.

توجد حالياً شركةٌ واحدةٌ تبيع برنامجاً مضاداً للفيروسات يستطيع أن يتعرّف على هذا «التروجان». يمكنكم أن تقوموا بتحديث البرنامج المضاد للفيروسات الذي تستخدمونه، وأن تشغّلوه لإزالة هذا «التروجان» إذا ما ظهر. ولكنّ الإجراء الأكثر أماناً هو بالتأكيد إعادة تنصيب نظام التشغيل على جهاز الحاسوب الخاص بكم.



برمجيات خبيثة تسلل إلى الهواتف عبر «الروتنغ»

يزداد تعرض الهواتف الذكية للهجوم من قبل برمجيّاتٍ خبيثةٍ معقّدةٍ، إذ اكتشف العاملون لدى مزود البرمجيات المضادة للفيروسات «إن كيو موبايل» NQ Mobile نسخةً جديدةً من DroidKungFu، وهو «تروجان» يستهدف نظام التشغيل «أندرويْد» يسمّى DKFBootKit. ويستهدف الأخير المستخدمين الذين يعمدون إلى الـ«روتنغ» Rooting)، وهو تخطي بعض القيود التي تضعها الشركة المصنّعة على إمكانية تنصيب بعض البرامج. وتتسلّل هذه البرمجية عبر التطبيقات التي يتطلب تنصيبها القيام بالـ«روتنغ». فإذا ما قَبِل المستخدم بتنصيب التطبيق المصاب، ستقوم هذه البرمجية الخبيثة بإدخال نفسها في عملية الإقلاع (Boot) الخاصة بالهاتف الذكي. وبحسب الباحثين في أمن المعلوماتية، فإنه من الصعب كشف وجود هذه البرمجية لأنها لا تستغلّ أية ثغرةٍ أمنيةٍ.

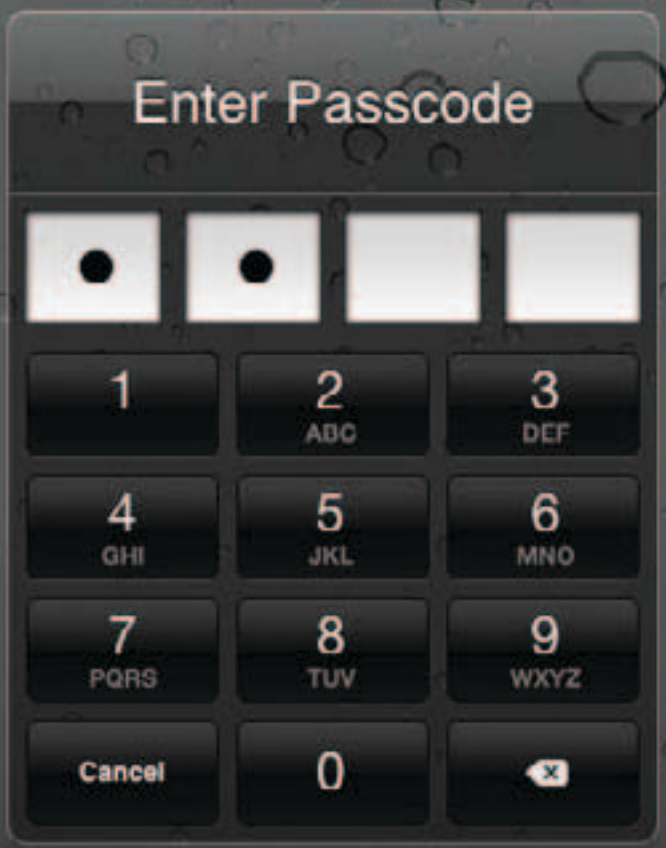
وكمثال على هذه التطبيقات التي تنقل الـ DKFBootKit، ذكرت شركة «إن كيو» الأداة التي تحوّل تطبيق ROM Manager إلى النسخة المدفوعة ذات الدرجة الأولى (Premium Edition)، بالإضافة إلى أدواتٍ أخرى تتيح فكّ الأقفال في الألعاب والتطبيقات الخاصة بتنظيم التطبيقات الأخرى ونسخها.

وتطلق هذه البرمجية برنامجاً بمقدوره العمل بشكلٍ مستقلٍ، أو «بُت» (Bot) ، يمكنه الإتّصال بمراكز تحكمٍ مختلفةٍ. لم تفصح «إن كيو» عن الغرض من وراء عمل هذا «البُت»، إلا أنه من المرجح أنّه يتيح التحكم بجميع وظائف الهاتف عن بعد، بما يتضمن عمل الميكروفون، والكاميرا، ونظام الـ «جي بي إس» (GPS) وحتى البيانات المُخزّنة. فيتحوّل هاتفكم بذلك إلى جهاز تجسس في غاية الفعالية، أو أداةٍ لمهاجمة أجهزة حاسوبٍ أو هواتف أخرى، من دون أن تتمكّنوا من كشفه. ولقد شهد مزوّدو البرامج المضادة للفيروسات حتى الآن أكثر من مئة ملفٍّ مصابٍ بالـ DKFBootKit.

عليكم إذن التفكير مليّاً فيما إذا كنتم فعلاً بحاجة إلى إجراء الـ«روتنغ» في هواتفكم، إذ إنّ هذه العملية غير ضرورية في معظم المهام اليومية، وهي تعرّض أمن هاتفكم برمّته للخطر. وعليكم أيضاً ألا تعمدوا إلى تنزيل التطبيقات المُقرصنة. فبشكل عام، لا يمكنكم الثقة سوى بالتطبيقات التي يطلقها المزوّدون الرسميّون (مثل «أي تيونز» و«غوغل بلاي ماركت»).

وبالإضافة إلى ذلك، إن "بمقدور التطبيقات التي لا تتيح الـ «الروتنغ» لمستخدميها أيضاً التجسّس عليكم بشكل خفيّ. لذا، عليكم أن تتأكدّوا من الإذن الضروري الذي يطلب منكم لدى تنصيب التطبيقات قبل القيام بهذه العملية، وألا تدعوا أشخاصاً آخرين ينصّبون البرامج في هواتفكم. للمزيد من المعلومات عن هذا «التروجان»، يمكنكم النقر هنا، كما يمكنكم القراءة عن النسخة السابقة منه عبر هذا الرابط .

عشرة أخطاء شائعة يرتكبها النشطاء والصحافيون أثناء استعمالهم الهواتف النقّالة



عشرة أخطاء شائعة يرتكبها النشطاء والصحافيون أثناء استعمالهم الهواتف النقّالة

لم يعد من الصعب على الأجهزة الأمنية في أنحاء العالم التجسّس على الأفراد من خلال الهواتف المحمولة التي يستعملونها. فهذه الهواتف، وبقدر ما تسهّل حركة الصحافيّين أو ناشطي المجتمع المدني في بيئةٍ أمنيّةٍ حسّاسةٍ، هي مصدر خطرٍ أمنيٍّ لا يستهان به، لاسيّما وأنّ السلطات الأمنيّة في غير بلدٍ باتت تُولي الجانب التقني والمعلوماتيّ من عملها أهميةً خاصة. فالمعلومات التي يتبادلها الأفراد إمّا عبر المكالمات الهاتفية وإمّا عبر الرسائل النصيّة ليست بمأمنٍ من عيون أجهزة الأمن وآذانها الحريصة على الإحاطة بكل شاردةٍ وواردةٍ تتعلّق بأنشطةٍ قد تراها مصدر قلق. وأمّا الخطر الأكبر، فيتمثّل في تحوّل الهاتف إلى أداة للتعقّب، حيث تكون حركة المستخدم مكشوفةً تماماً أينما توجّه. لا بدّ إذن من التذكّير أنّ أيّة هفوةٍ تقنيّةٍ قد تتسبّب بتعرّض مرتكبها، كما الأشخاص الآخرين المرتبطين به، للإعتقال أو حتى القتل.

فيما يلي عرض لعشرة أخطاءٍ على النشطاء تجنّبها أثناء استعمالهم الهواتف النقّالة:

١) إستعمال الهاتف النقال بشكلٍ عامٍ

يكمن الخطأ الأول في استعمال الهاتف المحمول بهدف إيصال رسالة ما، إذ إنّ الهاتف وسيلةٌ غير آمنةٍ. فمن المهم أن تعلم أنّ كل ما تقوله أثناء المكالمات الهاتفية أو تتبادله في الرسائل النصيّة القصيرة يخضع للتسجيل وقد يتم استعماله ضدّك في المستقبل، وأنّ موقعك سيكون دوماً مكشوفاً طالما أنّ هاتفك ليس مقفلاً (راجع رقم ٤ أدناه). لذا، عليك أن تسأل نفسك إذا ما كان من الضروري أن تستعمل هاتفك النقال. فكّر في استعمال وسائل اتصالٍ أخرى، خصوصاً وأنّه من الممكن، وببساطة، أن تعمد الشركة المشغّلة إلى إقفال الشبكة ممّا قد يضعك في عزلةٍ في حال كان اعتمادك الأول على الهاتف كوسيلة تواصل.

٢) التحدّث بصوتٍ مرتفعٍ عندما يكون الخطّ الهاتفي أو صوت الميكروفون رديئاً

لا يدرك الكثير من الناس إلى أيّ مدى يرفعون أصواتهم عندما يكون الإتصال الهاتفي رديئاً، ممّا يشكّل خطراً لا يتنبّهون إليه. إذ من الممكن أن يسمعك الآخرون من مسافةٍ بعيدةٍ، وهذا العمل لن يساعدك أصلاً على إسماع صوتك للطرف الآخر على الهاتف. فإذا قمت بتحسين نوعيّة الصوت، لن تجد ضرورةً لرفع صوتك أثناء الحديث.

أولاً، حاول أن تنظّف الميكروفون والسماعة إن وجدت أيّاً منهما متسخاً. ثانياً، إن كنت محاطاً بالضجّة، إستعمل السّماعات مع الميكروفون. السّماعات ليست كلها متشابهة ولا تتطابق كلها مع جميع أنواع الهواتف، إذ تختلف نوعية الصوت بين سماعةٍ وأخرى. لذا، يجب أن تستعمل السمّاعات الأصليّة التي أتت مع الهاتف. وأثناء الإتصال الهاتفي، قم بتعديل مستوى صوت المكبّرات ليتلائم مع الضجة المحيطة بك. فإذا كان صوت المكبّرات مرتفعاً جداً، ستقوم تلقائياً بالتحدث بصوتٍ مرتفعٍ.

ثالثاً، إنّ الهواتف الرخيصة، على عكس تلك المتطوّرة، لا تتمتّع بنوعية صوتٍ جيدة، كما أنّ الميكروفونات ذات الجودة العالية وتلك التي تتمتّع بخاصيّة إزالة الضجة الزائدة ليست زهيدة الثمن. لذا، قم بمقارنة عدة هواتف واسْعَ إلى استعمال هاتفٍ أحدث عند إجرائك مكالماتٍ حساسة. إن لم يكن هذا الهاتف ينتمي لآخر جيل من الهواتف، قد يكون سعره منخفضاً.

٣) إستعمال شرائح هاتفية مسجّلة

نعلم أنّ السلطات الأمنية تسعى دائماً من أجل أن تتمكّن من ربط النشاط عبر شبكة الهاتف النقّال بالهويّة الحقيقيّة لمستعمليه. لدى إجرائك مكالماتٍ حساسةٍ، تجنّب بأيّ ثمنٍ استعمال الشرائح

التي تمّ شراؤها وتسجيلها باسمك أواسم شخص تعرفه. إحتفظ بهاتفٍ يحمل شريحةً مسجلةً بهدف إجراء مكالماتٍ «بريئة» مع عائلتك وأصدقائك، فلا تخلط الهواتف والشرائح الخاصة مع تلك التي تستعملها «للعمل». وتجدر الإشارة إلى أنّه من الضروري أن يتمّ استعمال الشريحة غير المعروفة مع جهازٍ هاتفيٍّ غير معروفٍ بدوره، إذ يسهل تعقّب الهاتف بواسطة الرقم التسلسلي الذي يعرف اختصاراً برقم IMEI، والذي تقوم الشركات المشغّلة بربطه بالشريحة التي يتمّ استخدامها (من الممكن للشركة مثلاً أن تقوم بربط رقمي IMEI لهاتفين منفصلين بالشريحة نفسها إذا تم استخدامها فيهما، وبالتالي سيصبح من السهل الإستنتاج أن الهاتفين يعودان للشخص نفسه). كما أنّه عليك أن تحتاط لدى استعمالك بطاقةً «محروقة»، أي بطاقةً كان يستعملها أشخاصٌ آخرون قبلك. ويجب أن تكون جاهزاً لتتخلص من الشريحة، لأنّه إذا تم القبض عليك وهي بحوزتك، سيتم نسب كلّ الإتّصالات والرسائل النصيّة القديمة إليك.

٤) التعرّض للتعقب من خلال الهاتف المحمول

هل تدرك أنّ موقعك معروفٌ ومسجّلٌ على الدوام طالما أنّ هاتفك مشغّلٌ؟ إذ إنّ بإمكان الشركات المشغّلة للهاتف المحمول أن تحدّد مكانك بغاية الدقّة عبر تشغيل «نظام التموضع العالمي» (GPS) وهي خاصيّة يتمّ استعمالها عادةً في الحالات الطارئة، إلا أنّها من الممكن أن تكون مصدر خطرٍ في حال كنت تود أن تُبقيَ مكانك سرّياً. يُنصح في هذه الحالة بتعطيل نظام GPS يدويّاً عبر تعطيل الهوائي الخاص بهذا النظام. بالإضافة إلى ذلك، من الممكن تحديد موقع الهاتف من دون اللّجوء إلى استخدام الGPS، وذلك عبر تقاطع الإشارة الصادرة عن الجهاز مع عدّة أبراج اتصال. لذا، فمن المستحسن أن تقوم بنزع الشّريحة من الهاتف إذا كنت تستعمله بهدف التصوير. وقد يساعد تشغيل الهاتف بنظام الطيران (Flight/Airplane Mode) أو إقفاله في المحافظة على سريّة الأماكن التي تتواجد فيها. كما أنّ نزع البطاريّة يوفّر حمايةً إضافيةً، إذ إنّ ذلك يمنع احتمال تشغيل الهاتف وهو في جيبك. ولكن تذكّر أن تقوم بإطفائه قبل التوجّه إلى المكان الذي تقصده وألا تشغّله مجدداً فور خروجك من ذلك المكان بغرض قراءة رسائلك مثلاً.

٥) كتابة تفاصيل عن النشاطات في رسائل نصية واضحة

تقوم الشركات المشغّلة لشبكة الهواتف النقّالة بتخزين جميع الرسائل النصيّة لمدة طويلة، حتى تلك العائدة لأشخاصٍ غير ملاحقين، كما تقوم البرامج التي تنتقي الكلمات الدلاليّة (Keyword Filters) بإبراز الرسائل النصيّة التي تبدو مهمّة بالنّسبة لضباط الأمن. فإذا كنت شخصاً «مثيراً للإهتمام»، ستخضع جميع رسائلك -- تلك التي ترسلها كما التي تصلك -- للمراقبة بشكل روتيني. لذا، تجنّب الإعلان بشكلٍ مفصّلٍ عن المواضيع التي تتعلق بأيّ نشاط، واستعمل عوضاً عن ذلك رسائل مشفّرة تحوي أسماءً وأرقاماً متفقاً عليها مسبقاً.

٦) عدم إقفال الشاشة

يستصعب الكثير من الناس استعمال كلمة سرٍ لإقفال الشاشة في «الهواتف الذكية» (Smart) Phones)، فهم يفضّلون أن يتمكّنوا من استعمال هواتفهم بسرعة. ولكنّ ذلك يجعل من السّهل على أيٍّ كان أن يفتح هاتفك إذا ما تركته لثلاث دقائق من دون مراقبةٍ أو نسيته في مكان ما، كما أنّ تنزيل برنامجٍ للتجسّس على الهواتف الذكية لا يستغرق أكثر من ثلاث دقائق. وبالإضافة إلى ذلك، يعمد معظم من يجد هاتفاً، وقبل أيّ شيءٍ آخر، إلى قراءة الرّسائل النصيّة وأرقام الهاتف المسجّلة. إنّ معظم الهواتف الحديثة تُظهرعلى شاشاتها الوقت والرسائل الواردة وهي مقفلة. لذا، لا يوجد أي سبب يمنعك من استعمال قفل شاشة هاتفك.

أما فيما يتعلّق بكلمة السر المستعملة لإقفال الشّاشة، فمن المهم أن يكون اكتشافها صعباً وذلك بهدف إعطاء هاتفك الحماية اللازمة. وهنا تجدر الإشارة إلى أنّ أكثر من خمسين بالمئة من الناس يعمدون إلى استعمال واحد من الرموز السرية العشرة الأكثر رواجاً، لذا حاول أن تختار رمزاً يحتوي على أكثر من أربعة أرقام (نعم، يمكنك فعل ذلك)، وحاول استعمال الحروف إذا أمكن. وطبعاً، لا تستعمل أي رمزٍ يسهل تخمينه، مثل: 0000، 1234، 5555، 1397 أو ما شابه ذلك. أمّا رمز التعريف الشخصي (PIN)، فهو لا يصلح سوى لحماية شريحة الهاتف، ولا يحمي المعلومات المخزّنة على الهاتف نفسه.

٧) الصور والرسائل المخزنة

بالرغم من أنّ كل الرسائل يتم الإحتفاظ بها في الشبكة المشغلة للهاتف، حاول أن تتجنّب كشف الرسائل النصيّة المرسلة إليك أو تلك التي تتلقّاها، وذلك لحماية بياناتك في حال أضعت هاتفك أو تعرّضت للتفتيش المفاجئ من قبل أحد عناصر الأمن. لفعل ذلك، قم بإبطال خيار تخزين الرسائل التي ترسلها وتعوّد أن تمسح الرسائل التي تردك مباشرةً بعد قراءتها. أيضاً، تعلّم كيف تجري إعادة ضبط «إعدادات المصنع» (Factory Settings)، وهو خيار يتيح العودة إلى خصائص الهاتف التي كانت موجودة قبل استعماله

للمرة الأولى، وذلك عبر إدخال رمزٍ خاص. تمتاز معظم الهواتف بوجود هذا الرمز السري، ويمكنك أن تحفظه وتربطه بمفتاح الإتصال السريع. الضغط على الرقم ٨ بشكل متواصل مثلاً، ينتج عنه مسح معظم المعلومات الموجودة على الهاتف. تأكّد من محو المعلومات الموجودة على بطاقة الذاكرة أيضاً، لأنه في معظم الأحيان ذلك لا يحصل تلقائياً. عليك أن تتنبّه أيضاً إلى أنّه من الممكن إعادة كل المعلومات المزالة عبر استخدام برامج خاصة.

٨) دليل الهاتف المليء بالأسماء

يمكنك أن تخفي أجزاءً من شبكة الأشخاص الذين تتواصل معهم عبر تغيير شريحة الهاتف بشكلٍ متكرر، ولكن إذا قمت بتخزين جميع الاسماء وأرقام الهاتف التي بحوزتك في هاتفك، ستخاطر بكشف أرقام الهاتف التي تعود لجميع الأشخاص الذين تعرفهم وليس فقط أولئك الذين كنت قد اتّصلت بهم. فضلاًعن ذلك، قد ينتهي الأمر بكشف هوية أشخاص آخرين يستعملون شرائح هاتفية مجهولة. إن كنت تملك وسيلةً أخرى لحفظ هذه الأرقام فعليك اعتمادها. حاول ألا تخزّن الأسماء والأرقام معاً، وأن تكتفي بتسجيل الأرقام التي تحتاجها بصورة ملحّة فقط في الهواتف المختلفة التي تستعملها.

٩) إعارة الهاتف أو تركه من دون مراقبة

هل تحمل هاتفك على الدوام؟ هل أنت فعلاً لا تتركه من دون مراقبة ولو لبضع دقائق؟ من الممكن إجراء تغييرات في هاتفك وتحويله إلى ميكروفون بعيد ينقل كل ما تقول، حتى إذا قمت بإقفال الشاشة. فهذه العملية لا تتطلب الكثير من الوقت وهي صعبة الإكتشاف. ومن السهل أيضاً سحب كل المعلومات من الهاتف، بالرغم من استعمال قفل الشاشة أو رمز التعريف الشخصي. أمّا إذا تركت هاتفك مفتوحاً، سيتمكن شخصٌ آخر من انتحال شخصيتك أو العبث بالأسماء والأرقام المخزّنة. فمن الأفضل أن تبقي هاتفك تحت أنظارك وألا تعيره لأناسٍ لا تثق بهم تمام الثقة ولاتكون متأكداً من أنهم لن يفتحوه أو يعيروه لأحد آخر.

إذا حدث أن أضعت هاتفك، أو تمت سرقته أو مصادرته أثناء التحقيق معك، أو أعطيته لأحد ما من أجل إصلاحه، عليك أن تتعامل معه بحذرٍ شديد بعد استرجاعه، وأن تأخذ بعين الإعتبار أنّك قد لن تستعمله بعد ذلك. يمكنك مثلاً بيعه في السوق السوداء والتخلص من الشريحة التي في داخله. وإن كنت مصرّاً على استعماله مجدداً، عليك أن تتأكّد من خلوّه من أي آثار مادية قد تبيّن أنّه تم العبث به، مثل إزالة الأختام أوالملصقات، أو آثار تدل أن الهاتف قد تعرض للفتح، أو على الأقل، عليك أن تجري إعادة ضبط «إعدادات المصنع».

١٠) عدم الإحتفاظ بنسخ إضافية للمعلومات (Backup)

كلما زادت أهميّة المعلومات والأسماء والأرقام والرسائل التي تحتفظ بها في هاتفك – مع العلم أنّنا قلنا أنه من المستحسن ألا تخزّن الرسائل النصّية – سيزداد ترددك في مسح هذه البيانات عند شعورك بقرب الخطر. لذا، فإنه من الأفضل أن تقوم بشكل دوري بخلق نسخ إضافية (Backup) من المعلومات التي تريد الإحتفاظ بها، وذلك بالإستعانة ببرامج خاصةٍ يكون هاتفك مرفقاً بها لدى شرائه. عليك أن تتنبّه للمكان الذي يقوم به هذا البرنامج بتخزين المعلومات في هاتفك وأن تخزّن هذه المعلومات مباشرةً في ملف مشفّر (للمزيد من المعلومات، راجع المقال حول ال TrueCrypt).

فالخلاصة إذن هي التالية: قبل أي شيءٍ، لا تثق بهاتفك، واعلم أنّ إجراءات الحماية تبقى محدودة الفعاليّة.

الإجراءات التي تحمي الهاتف المحمول...
غير موجودة!

* من الممكن التنصت على كل محادثاتك وتخزين كل رسائلك النصية.
*إذا قمت باستعمال شريحتي اتّصالٍ مختلفتين في الهاتف نفسه سيكون من السهل كشف الصلة بينهما.
* من الممكن استرجاع المعلومات الممسوحة.
* معظم كلمات المرور ورموز التعريف الشخصي يمكن كشفها بسهولة.
*الهواتف البسيطة (مثلSymbian ٤٠) لا يمكنها تشفير الحركة على شبكة الإنترت، فتنتقل كلمات المرور ومحتوى النشاط عبرها بشكلٍ مفتوحٍ.
*عندما يكون الهاتف مشغّلاً، تستطيع الشبكة أن تحدّد مكان تواجدك والمكان الذي كنت فيه قبل ذلك بشكلٍ دقيقٍ جداً.
إن كنت تملك هاتفاً ذكياً ويهمك مصير المعلومات المسجلة فيه كالرسائل النصيّة والصور ومقاطع الفيديو وتاريخ التصفّح، إلخ، عليك أن تعلم التالي:
* إنّه من السهل كشف المعلومات التي تحتويها هواتف «نوكيا سمبيان»، فالعديد من الناس يعرفون كيفية كشف رمز التعريف الشخصي وحتى كشف التشفير.
*بالنسبة «للأيفون»، توجد عدّة برامج متخصّصةٍ يمكنها فتح الهواتف المحميّة بكلمة سرّ وتلك المشفّرة في غضون ٣٠ دقيقة.
* يتمتّع هاتف «البلاكبيري» بعدة خصائص جيّدةٍ تمكّنك من حماية بياناتك، وهو يقدم واحدةً من أكثر مساحات التواصل أماناً، ولكن توجد عدة برامج متخصّصة في التجسس على مستخدمي «البلاكبيري». فبالرغم من كونه «آمن»، يتعرض «البلاكبيري» للمراقبة من قبل الحكومات في كل من بريطانيا والسعودية والإمارات، بالإضافة إلى دولٍ أخرى.
* إن «الأندرويد» ليس نظاماً واحداً، إذ تقوم كلّ شركةٍ بتغيير هذا النظام قليلاً. فعملية التهيئة (Configuration) العاديّة غالباً ما تكون قديمة وغير آمنة. لكن بما أنّ هذا النظام مفتوح المصدر، يستطيع المستخدمون ذوو الخبرة من إجراء تغييراتٍ كثيرةٍ من شأنها أن تحسّن مستوى الأمان ولو قليلاً.

ولكن لا بد من اتباع الخطوات التاليةً:

* فكّر ملياً بما ستقوم بقوله أو بكتابته أو تخزينه في هاتفك المحمول.
* تعلم كيف تمسح المعلومات المحفوظة في هاتفك
* إستعمل كلمة مرور يصعب اكتشافها.
* إنزع البطاريّة من الهاتف إذا أردت أن تحمي نفسك من التعقّب وأنت ذاهب إلى مكانٍ سريٍّ، ولا تعيدها قبل أن تتأكد أنّك أصبحت في مكانٍ آمنٍ (لا تعيد وضع البطارية وأنت في طريق العودة).
وأخيراً، قم بزيارة المواقع التالية من أجل الحصول على آخر المعلومات حول الإستعمال الآمن للهواتف المحمولة
http://safermobile.org و www.cyber-arabs.com.

مقابلة مع رونا سانفيك

برنامج «تور» يتصدّى للتجسّس على مستخدمي الإنترت

مع تزايد الإعتماد على الإنترت في شتّى مجالات الحياة، أصبحت الشبكة نفسها مصدراً قيّماً للمعلومات لكلٍّ من الشركات التجاريّة والأجهزة الأمنيّة، تُتيح لها التجسّس على المستخدمين عبر جمع شتّى أنواع البيانات عنهم. برزت إزاء هذا الواقع عدة مشاريعٍ تهدف إلى مكافحة المراقبة التي يخضع لها مستخدمو الشبكة الإلكترونية، من بينها «تور»، وهو برنامجٌ مفتوح المصدر يتيح الإستخدام الآمن للإنترت.

إلتقى فريق «سايبر أرابز» برونا ساندفيك، الباحثة والمطوِّرة التي تعمل على مشروع «تور»، فكان حديثٌ عن الفكرة التي انثبق منها المشروع وأهميّة التزوّد بالمعرفة حول الأمن الرقمي وسُبل حماية الخصوصيّة على الشبكة العنكبوتيّة.

هل لكِ أن تعرّفينا عن نفسكِ باختصار؟

أبلغ من العمر ٢٥ سنةً. ولدت في النروج، إلا أنّني عشت في لندن، بريطانيا، خلال السنة الماضية تقريباً. أعمل بدوامٍ كاملٍ في مشروع «تور» حيث أقوم بأعمالٍ كثيرةٍ ومختلفة. أملك بعض الخبرة كمستشارةٍ في شؤون أمن المعلومات وأساعد العديد من الشركات الكبيرة على حماية أنظمتها، وتطبيقاتها، وشبكاتها.

هل تستخدمين برنامج «تور» (Tor) عندما تتصفّحين الإنترنت؟

نعم، أقوم بذلك. يُعتبَر برنامج «تور» أداةً رائعةً للمستخدمين الذين يرغبون بحماية خصوصيتهم عند تصفحهم الإنترنت والبقاء مجهولي الهوية. واستخدام برنامج «تور» عند تصفحك الإنترنت يعني أنّك لست مضطراً للوثوق بمدير الشبكة، أو مزود خدمة الإنترنت (ISP)، أو أيّ جهةٍ أخرى ستقوم بالتجسس على حركتك أو الإنفراد بالقرار بشأن المواقع التي يمكن أو لا يمكن لك زيارتها.

ما هو الدور الذي تؤدّينه في مشروع «شبكة تور» وما هي الدوافع التي تحفزكِ على المشاركة فيه؟

دوري يتنوّع بين أمورٍ مختلفة، بدءاً بالأبحاث المتعلّقة بأمن المعلومات والتطوير ووصولاً إلى إدارة المشاريع، والتدريب، والدعم، وتنسيق الترجمة.

أعتقد أن أكثر ما يحفّزني هو فرصة العمل على مسألة تعني الكثير بالنسبة لآلاف الأشخاص. وأحبّ العمل على مشاريع قائمة، والتعاون مع أشخاصٍ آخرين، وتعلّم أمورٍ جديدة.

هل تعتبرين عملك رسالةً؟ وماذا يعني الأمن الرقمي بالنسبة لك؟

أعتبر عملي مهماً، وأحب ما أقوم به، إلا أنني لا أعتقد أنني قد أصف عملي «بالرسالةً». بالنسبة لي، يتمثل الأمن الرقمي بالأمور التي من الممكن أن تقوم بها لحماية نفسك عند تصفّحك الإنترنت. ويشمل هذا الأمر استخدام كلمات سرٍّ معقدةٍ، وعدم استخدام كلمة السر نفسها على مواقع مختلفة، واستخدام نظام HTTPS لدى الدخول إلى مواقع مثل «فيسبوك» و«تويتر». بإمكانك أيضاً تشفير البريد الإلكتروني الذي ترسله لتقتصر إمكانية قراءته على الشخص المعني بتلقيه فقط، وبإمكانك أيضاً استخدام «تور».

من المهم جداً أن نتذكّر أنّ اكتساب الخبرة هو أساس كل شيء. قم بإخبار الأصدقاء بالأمور التي تعلمتها عن أمن المعلومات وتأكد من بقائهم آمنين لدى تصفّحهم الإنترنت أيضاً.

هل بإمكانكِ شرح كيفية عمل «تور» وكيفيّة استخدامه بعباراتٍ مختصرةٍ ومُبَسَّطةٍ ؟

يتمّ العمل ببرنامج «تور» من خلال إرسال حركة تصفحك عبر ثلاثة خوادم (Servers) ضمن شبكة «تور»، قبل أن تعود هذه الحركة إلى شبكة الإنترنت العامة. الفكرة تشبه استخدام طريقٍ متعرّجة وصعبة التتبّع للتخلص من أحد يتعقبك، ومن ثم التخلّص بشكلٍ منتظمٍ من آثار حركتك.

وبدلاً من اتخاذ مسارٍ مباشرٍ من حاسوبك إلى الموقع الذي تريد زيارته، يختار «تور» ثلاثة خوادم يمرّر خلالها بياناتك أولاً، ثم تقوم بعد ذلك هذه الخوادم بتغطيةٍ آثار حركتك على الإنترنت كي لا يتمكن أيّ مراقب عند أيّة نقطة محددة من معرفة مصدر هذه الحركة ووجهتها.

ويتمّ استخدام «تور» يومياً لأهدافٍ متنوّعةٍ من قبل أشخاص عاديين، وعسكريّين، وصحفيّين، وعناصر أمنيّة، وناشطين، وأفراد آخرين. وإن كنت ممّن يهتمون لأمر خصوصيتهم، وإذا لم تكن تريد لشركة «غوغل» أن تعرف عما تبحث، أو إذا لم تكن تريد لموقع «فيسبوك» أن يتتبّعك عندما تتصفّح الإنترنت، قم باستخدام «تور».

أنصحك بزيارة الموقع التالي للحصول على معلوماتٍ مفصّلةٍ وصورٍ بإمكانها المساهمة في شرح الجوانب المتعلقة بعمل «تور» :
https://www.torproject.org/about/overview.html.en#thesolution

لمَ يجب أن أكون مجهول الهوية عندما أتصفح الإنترنت؟ فقد يعتبر بعض الأشخاص أنهم ليسوا مضطرين لإخفاء أي نشاط لهم في شبكة الإنترنت

إنّ برنامج «تور» لا يخوّلك أن تكون مجهول الهوية فحسب، إنما يساعدك أيضاً على حماية خصوصيتك. فآلاف الأشخاص مثلك ومثلي يستخدمون هذا البرنامج يومياً. هم يستخدمون «تور» لأنهم لا يريدون أن يطّلع موقع «غوغل» (أو مديرهم، أو أصدقاؤهم، أو أهلهم) على غرض بحثهم عبر الإنترنت. كما أنّهم يلجأون إليه لأنّهم لا يريدون أن يتتبعهم موقع «فايسبوك» عند تصفّحهم الإنترنت ولأنهم يرغبون بالنفاذ إلى شبكة إنترنت غير خاضعة للرقابة وحتى إذا اقتصر الأمر على النفاذ إلى مواقع مثل «تويتر» و«يوتيوب».

من هي الجهة التي تقف وراء «تور»؟

تمّ تصميم «تور» وتنفيذه ونشره في إطار مشروع توجيه طبقات (Onion Routing) في «مختبر أبحاث البحرية الأميركية». ويُذكَر في هذا الصدد أنّ في سنة ٢٠٠٤، تقدّم كلّ من روجر دنغلداين، ونيك ماثيوسن، وساموبل جونسون، وتيلور كوري، وبول سيفرسون ببرنامج «تور» خلال مؤتمر في سان دييغو، كاليفورنيا، والبرنامج كناية عن موجه طبقات (Onion Router) من الجيل الثاني. ومنذ ذلك الحين، تحوّل «تور» إلى مصدر مفتوح.

شعاركم هو رسمٌ لبصْلة. لماذا؟

بطريقةٍ أو بأخرى، يمثل الشعار التشفير المستخدم عندما يتمّ إرسال حركتك على الإنترنت من خلال شبكة «تور». وقبل إرسال حركتك من خلال ثلاثة خوادم، سيقوم عميل «تور» بتشفير حركتك إلى مفتاح A للخادم الأوّل، ومفتاح B للخادم الثاني، والمفتاح C للخادم الثالث. ثم سيقوم بلفّ حركتك في ثلاث طبقات من التشفير، لتقوم على التوالي ثلاثة خوادم بـ«نزع» هذه الطبقات بهدف إدراك ما يجب فعله بالحركة (مثلاً إرسالها إلى خادم آخر في الشبكة، أو إرسالها إلى شبكة الإنترنت العامة).

ألستِ قلقةً من وقوع «تور» في يد الأشخاص «غير المناسبين»، مثلاً ممن لديهم نوايا سيئة ويسعون لحجب هويتهم لأسباب جرمية؟
عند الحديث عن الأشخاص السيئين الذين يستخدمون «تور» لأسبابٍ خاطئة، من المهم أن نتذكّر أنه في حال لم يكن «تور» متوفراً، لكانوا استخدموا وسيلةً أخرى ببساطة. وفي الوقت نفسه، من المهم تذكّر عدد الأشخاص الصالحين الذين يستخدمون «تور» لأسباب جيّدة، وعدد الأشخاص الذين هم بحاجة لاستخدام «تور» للإختباء من هؤلاء الأشخاص السيّئين. ولا بد من الإشارة إلى أنّ «تور» لا يقيّد حركتك على الإطلاق، وأنك حرّ التّصرف بالطريقة التي تريدها.

أي متصفّح يتلاءم مع «تور»؟
نحن، ولأسبابٍ أمنية، ننصح باستخدام «فاير فوكس» فقط الذي يرافقه مفتاح «تور» (Torbutton) بحيث يتمّ تنصيبه عندما يتم الإتصال بشبكة «تور». ومن المهم أن نشير إلى أنّ استخدام متصفحات أخرى مثل «إنترنت إكسبلورير» (Internet Explorer)، و«كروم» (Chrome)، و«سافاري» (Safari) بإمكانه أن يتسبّب بتسرّب معلوماتٍ عن حاسوبك بطرقٍ عديدة.

لماذا؟ هل يخاطر المستخدم بشكف هويته في حال شغّل تسجيلاتٍ توجيهية على شكل فلاش فيديو أو تسجيلات فيديو على موقع «فيسبوك»؟
ما من وسيلة لحماية هويتنا من الكشف عند اطّلاعنا على تسجيلات فيديو فلاش. إلا أنّه في حال لم نكن قلقين حيال تتبّعنا من قبل هذه المواقع (مثلاً يوتيوب) وحيال المواقع التي تنتحل الهوية نفسها، وفي حال كنتم عدم مكترثين بإمكانية أن تتنبّه جهات الرقابة المحلية إلى أنّكم تقومون بزيارة هذه المواقع، بإمكانكم عندئذٍ تمكين إضافات الفلاش (Flash Plugin) والإطّلاع على أي تسجيل فيديو.

بعض الأشخاص يجدون أنّ الإنترنت لديهم تصبح بطيئةً جداً عند استخدام «تور». هل هذا صحيح؟
نعم، من الممكن أن يصبح العمل ببرنامج «تور» أبطأ من استعمال الإنترنت بطريقة عاديّة. هناك بعض الأسباب وراء هذا الأمر: (١) يتم إرسال حركتك عبر ثلاثة خوادم في الشبكة ويمكن لهذه الخوادم أن يكون مقرها في أيّ مكان في العالم، (٢) يستخدم ما يقارب ٨٠٠ ألف شخص «تور» يومياً، إلا أنّ الشّبكة لا تتضمّن سوى ٢٥٠٠ خادم للتعامل مع هذه الحركة، (٣) يستخدم البعض شبكة «تور» لتنزيل ملفات كبيرة (مثلاً أفلام عبر برنامج «بت تورنت» BitTorrent).

هل بإمكانكِ ذكر أعدادٍ لمستخدمي «تور» تم إحصاؤها مؤخراً؟

ابتداءً من ٣ تشرين الأول/أكتوبر٢٠١١ نقدّر أنّ عدد المتصلين مباشرةً بشبكة «تور» قد بلغ ٤٠٠ ألف مستخدم، إضافةً إلى ٤٠٠ ألف مستخدمٍ آخرين متصلين عبر خوادم وسيطة (Bridges). والخادم الوسيط هو ببساطةٍ خادمٌ بإمكان أحدهم استعماله للإتّصال بالجزء المتبقي من شبكة «تور».

هل لديكِ أي تعليق بشأن هذه الأرقام أو التطورات الأخيرة؟ هل هناك أية مفاجآت؟ أو أي تطورات أساسية؟

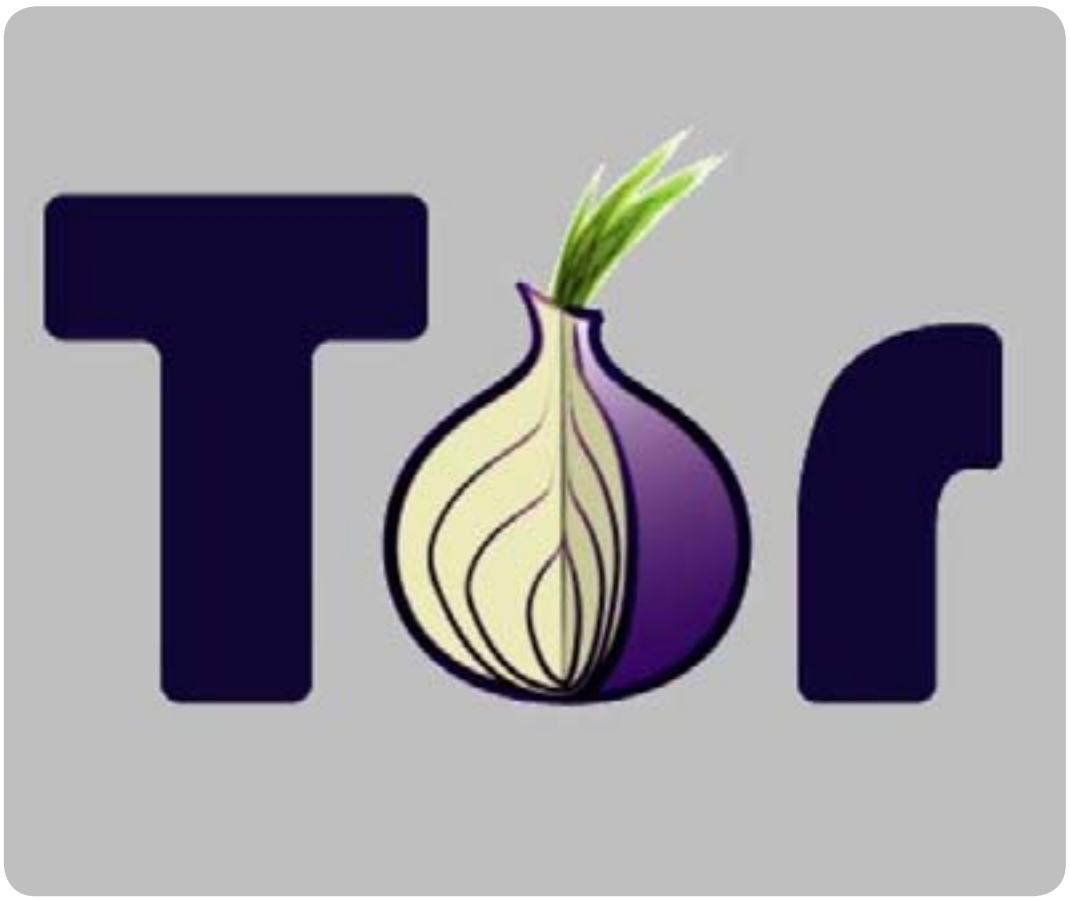
لا شكّ أننا شهدنا زيادة كبيرة في عدد المستخدمين في نيسان/أبريل ٢٠١١ تقريباً. وبإمكاننا عزو ذلك إلى الربيع العربي، إلا أنه في أي حال، من الرائع رؤية المزيد من الأشخاص يستخدمون «تور» لتصفّح الإنترنت بأمان.

و تجدر الإشارة إلى أنّه من وقتٍ إلى آخر، قد يعمد أحدهم إلى حجب «تور» وربما قد نشهد تراجع عدد المستخدمين من بلدٍ معيّن. فقد قررت إيران مثلاً حجب «تور» في بداية أيلول/سبتمبر لتحول بالتالي دون وصول المستخدمين إلى خدمة إنترنت غير خاضعة للرقابة. إلّا أنّنا عالجنا المشكلة في يوم واحد وأطلقنا نسخةً جديدةً من «تور» الذي يسمح مجدداً للإيرانيين بالإتصال بشبكة «تور».

هل تعتقدين أنّ مستخدمي الإنترنت على اطلاعٍ جيّدٍ بوسيلة مماثلة لتجنب الرقابة وحماية خصوصيتهم ؟

أعتقد أنّ مستخدمي الإنترت يدركون أنّ الأدوات المضادة للرقابة متوفّرة، إنما ربما ليس «تور» على وجه التحديد. هناك حلول عديدة متوفرة على الإنترنت قد تسمح لك بتخطّي الرقابة، إلا أنّ قليلٌ هو عدد هذه الحلول الذي سيبقيك فعلياً آمناً ومجهول الهوية في الوقت نفسه. نحاول إيصال هذه الفكرة بأفضل طريقةٍ ممكنةٍ والسفر إلى كافة أنحاء العالم للقيام بدورات تدريبيّة ومحادثات.

«Hide My Ass!» هو برنامج «بروكسي» و «شبكة افتراضية خاصة» (VPN) يسمح لك بتخطي الرقابة. يدّعي القيّمون على هذا البرنامج في موقعهم الإلكتروني أن الحلّ آمن وأنه يمكّنك من التصفح وأنت مجهول الهوية. إلا أنه منذ أسبوع أو أسبوعين، علمنا أنّ هذه الخدمة أبقت على سجلات عمليات الدخول لمستخدميها، والمصدر من حيث يقومون بالإتصال إلخ. وذكر القيّمون على الموقع في إحدى مدوناتهم أيضاً أنّهم قد يتعاونون مع سلطات تنفيذ القانون في حال تلقّوا أمراً من المحكمة.



وأمّا «تور»، فلا يبقي على سجلاتٍ لعمليات الدخول الخاصة بمستخدمي الشبكة. لا ندري من أنتم، وماذا تفعلون عندما تستخدمون «تور». كما أنّنا لا نعلم مع من تتواصلون، ومدى استخدامكم لبرنامج «تور» أو متى قمتم بتنزيله. هذه ميزةٌ من بين ميّزاتٍ كثيرةٍ تجعل «تور» مختلفاً عن الأدوات المضادة للرقابة المتوفرة.

هل هناك دول لا يعمل برنامج «تور» فيها؟

لم نسمع أنّ برنامج «تور» لا يعمل في دولة محدّدة. إلا أنّه ما لم يخبرنا المستخدمون أنّ البرنامج لا يعمل، لن نتمكّن من اكتشاف الأمر. وتحاول في هذا الصدد بعض الحكومات أن تحجب «تور»، وهي تنجح في هذا المسعى إلى حدّ ما. إلا أنّه من الصعب حجب «تور» كلياً.

حماية الخصوصية باستخدام برنامج «تور»

كاردوخ كال

حماية الخصوصية في الدول التي تراقب الإنترنت هي من الأمور الضروريّة للناشطين الذين يعتمدون بشكلٍ أساسيٍ على هذه الشبكة للتواصل فيما بينهم وإيصال ما يحصل من أحداثٍ في دولهم إلى العالم.

ولذلك نجد العديد من مطوّري البرمجيّات يعملون على تطوير التطبيقات والأدوات التي تُساعد الناشطين على التخفّي وحماية خصوصيّتهم، ويُعتبر برنامج «تور» (Tor) من أشهرها، ومهمّته الأساسيّة إخفاء هويّة المُستخدم خلال تصفّح الإنترنت. ويشترك الناشطون حول العالم في برنامج «تور» من أجل الإستفادة من حماية الخصوصيّة، حتى أنّ بعضهم يستعمل حاسوبه الشخصي لتقديم المساعدة للعديد من الناشطين الآخرين. هذا يعني أنّ التشاركيّة

لمحة تاريخية:

تمّ إطلاق المبدأ الأساسي لعمل تكنولوجيا «تور» في ٢٠ أيلول/سبتمبر من العام ٢٠٠٢، وذلك بواسطة مجموعة من مُطوّري برامج الحماية عبر الإنترنت الذين استمروا بتطوير «منتجهم» حتى وصل إلى شكله النهائي في ١٣ آب/أغسطس من العام ٢٠٠٤، وقد تمّ دعم البرنامج ماديّاً من قبل العديد من المنظمات الداعمة للحريات. ومن المهم أن نذكر أنّ «تور» كان أداةً فعّالةً في مساعدة الناشطين في الثورة المصريّة، والثورة السوريّة مُؤخّراً.

طريقة الإستعمال:

يمكن تحميل «تور» والمتصفّح الذي ينصح القيّمون على المشروع باستخدامه مباشرةً من الموقع التابع للمشروع. كخطوات أساسيّة لاستعمال برنامج «تور»، يتمّ الإتّصال بالإنترنت ثم تشغيل البرنامج قبل البدء بالتصفّح الخفي، مع الأخذ بالإعتبار أنّ «تور» لايصبح آمناً للإستخدام إلّا بعد أن يتغيّر لون البصلة من الأصفر إلى الأخضر.

مبدأ العمل:

يتّخذ برنامج TOR طبقات البصلة رمزاً له، وذلك بسبب اعتماده على تكنولوجيا الـ Onion Routing. وتقوم هذه التكنولوجيا بنقل البيانات وتحويلها من طبقة إلى أخرى، وتغيير ترميز التشفير والمكان الجُغرافي لكلّ طبقة بشكلٍ مُختلف عن الطبقة الأخرى قبل إعادة تجميعها في الطبقة الأخيرة، ومن ثمّ توجيه الطلب للمكان المطلوب في انتظار الرد. وعندما يأتي الرد، يقوم برنامج «تور» بعكس العمليّة ثم عكس

لمحة تاريخية:

تمّ إطلاق المبدأ الأساسي لعمل تكنولوجيا «تور» في ٢٠ أيلول/سبتمبر من العام ٢٠٠٢، وذلك بواسطة مجموعة من مُطوّري برامج الحماية عبر الإنترنت الذين استمروا بتطوير «منتجهم» حتى وصل إلى شكله النهائي في ١٣ آب/أغسطس من العام ٢٠٠٤، وقد تمّ دعم البرنامج ماديّاً من قبل العديد من المنظمات الداعمة للحريات. ومن المهم أن نذكر أنّ «تور» كان أداةً فعّالةً في مساعدة الناشطين في الثورة المصريّة، والثورة السوريّة مُؤخّراً.

طريقة الإستعمال:

يمكن تحميل «تور» والمتصفّح الذي ينصح القيّمون على المشروع باستخدامه مباشرةً من الموقع التابع للمشروع. كخطوات أساسيّة لاستعمال برنامج «تور»، يتمّ الإتّصال بالإنترنت ثم تشغيل البرنامج قبل البدء بالتصفُّح الخفي، مع الأخذ بالإعتبار أنّ «تور» لايصبح آمناً للإستخدام إلّا بعد أن يتغيّر لون البصلة من الأصفر إلى الأخضر.

مبدأ العمل:

يتّخذ برنامج TOR طبقات البصلة رمزاً له، وذلك بسبب اعتماده على تكنولوجيا الـ Onion Routing. وتقوم هذه التكنولوجيا بنقل البيانات وتحويلها من طبقة إلى أخرى، وتغيير ترميز التشفير والمكان الجُغرافي لكلّ طبقةٍ بشكلٍ مُختلف عن الطبقة الأخرى قبل إعادة تجميعها في الطبقة الأخيرة، ومن ثمّ توجيه الطلب للمكان المطلوب في انتظار الرد. وعندما يأتي الرد، يقوم برنامج «تور» بعكس العمليّة ثم عكس عملية التشفير حتى يتم الوصول لجهاز حاسوبك وإعادة تجميع البيانات وفك تشفيرها.

وتتكوّن البيانات الصّادرة من أجهزة الحاسوب من قسمين: القسم الأول هو رأس التوجيه الخاص بالمعلومات (Header)، وهو يُظهر مصدر المعلومات ووجهتها. أمّا القسم الثاني فهو الخاصّ بالبيانات المحمولة (Data Payload)، وهي أيّ شيءٍ يجري إرساله، مثل رسالة إلكترونية أو موقع على الإنترت أو مقطع فيديو، إلخ.

تتمكّن مزوّدات خدمة الإنترنت (ISPs) عادةً من معرفة مصدر المعلومات التي خرجت ووجهتها لكون ذلك موجود في رأس التوجيه، حتى وإن كانت المعلومات التي يتبادلها المستخدم مشفّرةً. لذا، يصبح من الممكن تتبّع نشاط المستخدم عبر الإنترت وجمع قدرٍ وافرٍ من المعلومات عنه.

أما الفكرة وراء «تور»، فتشبه إلى حدٍ بعيدٍ سلوك شخصٍ ما طريقٍ متعرّجةٍ يصعب تتبّعها ثم إزالة الآثار المتروكة بعد مروره. إذ تكون هويّة المستخدِم والمواقع التي قام بتصفحّها مجهولةً بالنسبة لمزوّد الإنترنت.

لدى محاولة المستخدِم الإتّصال بموقعٍ معيّنٍ على الإنترت، يقوم «تور» بتحديد عدة عُقد (أونقاط اتصال) تستخدم «تور» بين المصدر والهدف، ويكون معظم هذه العقد أجهزة حاسوب شخصيّة. ينتقي «تور» عشوائياً طريقاً مؤلفاً من عدة عقد، فيجري إرسال معلوماتٍ مشفّرةٍ من عقدةٍ إلى التالية، إلى أن يصل طلب المعلومات إلى الهدف، حيث يتم فكّ التشفير لمعرفة محتوى الطلب. بالإضافة إلى بقاء مضمون المعلومات المنقولة مجهولاً لكونه مشفّراً، يبقى الطريق الكامل الذي سلكته هذه المعلومات مجهولاً أيضاً، فكلّ واحدة من هذه العُقد تسطيع أن تحدد العقدة الموجودة قبلها وتلك الموجودة بعدها فحسب. لذا، سيتعذر على الجهة التي تحاول تتبّع مرور المعلومات تحديد هوية المستخدم. وعند القيام بنشاطٍ جديدٍ، يقوم «تور» بإرسال المعلومات عبرطريقٍ جديدٍ، وذلك بهدف عدم ربط الأنشطة المتعددة بالمستخدم نفسه.

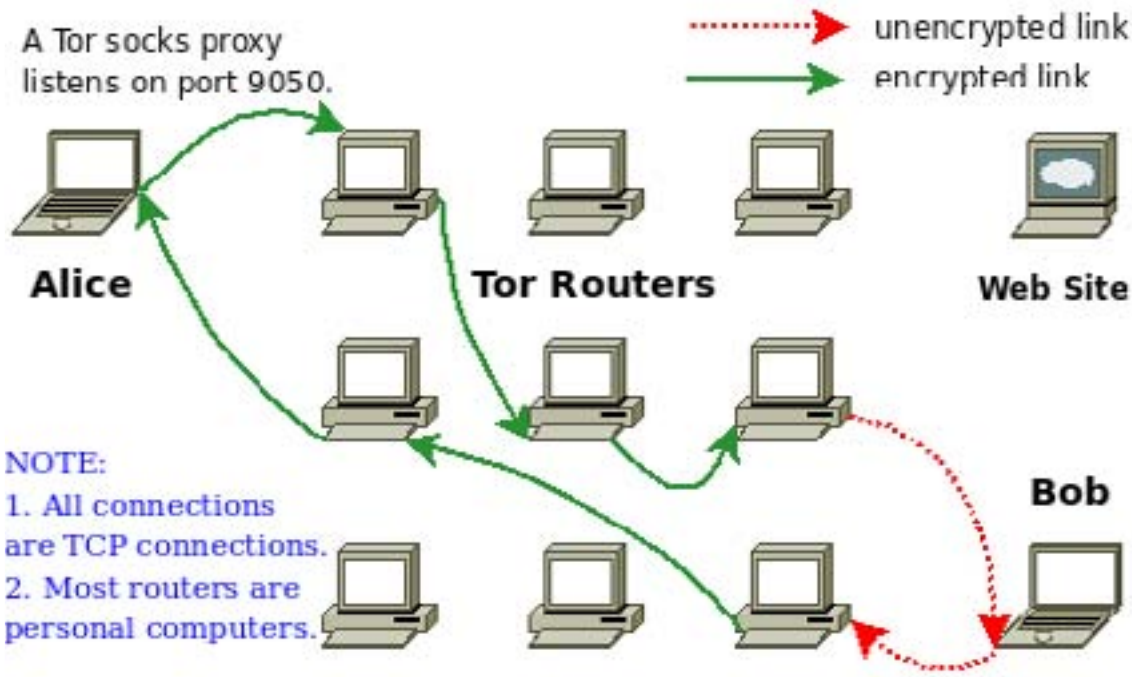
فلنأخذ المثال التالي: توجّهت سارة إلى موقع noreply.com، فظهر في بيانات الموقع أنّها تتّصل بالإنترنت من جامعة هارفرد Harvard. وعندما أعادت الكَرّة، حدث الأمر نفسه، وظهر أنّها تتّصل من ألمانيا مع أنّها كانت موجودة في السودان. فاستنتجت أن «تور» يُغيّر هويّتها عند كل طلب، مما يُساعدها على إخفاء هويّتها.

ويبدو مبدأ عمل برنامج «تور» واضحاً من خلال الرسم التالي:

لدي مخدم وموقع، هل يستطيع «تور» حمايتي؟

يُعدّ تدفُّق البيانات من جهاز الحاسوب الخاص بك، وبغضّ النظر عن التطبيق الذي تستخدمه، مثل (FTPClient–Messengers)، من الأمور التي تُسهّل الكشف والتعقُّب. ومن المُمكن أن يتم كشف كلمات السرّ التي تستخدمها مما يُعرّض مخدمك (Server) لخطر الإختراق والتدمير بشكلٍ دائم.

وفي هذا الإطار، وبُغية حمايتِك والحفاظ على سريّة نشاطاتك، يقوم «تور» بربط الأدوات التي تستخدمها لإدارة مواقعك عن طريق



مُوفّر التشفير (Encryption Provider) عبر بروتوكول للتشفير (Socks).
وبما أنّ التصفُّح هو من أهم الخدمات التي يقوم برنامج «تور» بتوفير الحماية والخصوصيّة لكلّ من يستخدمها، يُزوَّد برنامج «تور» بمتصفح الـ Firefox المحمول (Portable Version) مما يُوفّر الحماية للHttps. وهكذا يكون بالإمكان تشغيل برامج التراسُل كـ Skype أو Messenger عبر الـ (SOCKS 4 & SOCKS 5 protocols)، أي البروتوكولات التي يُوفرها برنامج Polipo المُرفق بـTor .

لا أملك معلومات خطيرة، فلماذا أحمي خصوصيّتي؟

لا تقتصر خدمات برنامج «تور» على تشفير البيانات وإخفاء مضمون الرسائل التي تقوم بإرسالها فحسب، بل تتضمّن أيضاً حماية خصوصيتك بشكل عام. فعلى سبيل المثال، تقوم العديد من المواقع والشركات بجمع البيانات من مصادر مُتعدّدة عن مُستخدميها عن طريق اختصاصيين في جمع المعلومات، ثم تعيد تجميعها، مما يُعرّض المُستخدمين للمزيد من اختراق الخصوصيّة.
إنّ توفير الحريّة والخصوصيّة هو من التحدّيات الكبرى التي تواجهنا في الوقت الحالي، وخصوصاً مع تزايد عدد الشركات التي تعمل على تحليل نشاطاتنا عبر الإنترنت وخلق الأدوات التي تجعلنا عرضةً للكشف، لاسيّما في الأعمال التجاريّة والنشاطات الإعلاميّة. ولذلك، فإنّ التطبيقات التشاركيّة كبرنامج «تور»، والتي لا تعود ملكيّتها لأشخاصٍ أو جهاتٍ مُعيّنة وتعمل على حماية خصوصيّتنا، تستحق الثقة ولا غنى لنا عنها.

تقارير عن استهداف أجهزة حاسوبٍ تعمل بنظام «ماك»

يبدو أنّ الحواسيب العاملة بنظام تشغيل «ماك» لم تعد بمأمنٍ من الهجمات الإلكترونية، بحسب ما تشير بعض التقارير، ممّا يُظهر ضرورة تحديث أنظمة الحماية من البرمجيات الخبيثة بشكل دوري بهدف الحفاظ على سلامة أجهزة الحاسوب. فقد تعرّضت عدّة منظمّات غير حكومية في إقليم التيبت – وهو إقليمٌ تحت السيطرة الصينيّة يسعى إلى نيل استقلاله – إلى سلسلةٍ من عمليّات القرصنة الإلكترونية المنظمّة، لم تستهدف الأجهزة العاملة بنُظُم «ويندوز» فحسب، بل تعدّتها إلى تلك العاملة بنظام «ماك» المنتجة من قبل شركة «أبل»، وهو نظام يسود الإعتقاد بأنّه بمأمنٍ من شر الفيروسات.

فقد بعث المهاجمون إلى هذه المنظّمات برسائل إلكترونيّةٍ تتضمّن إمّا ملفات «أوفيس» تحمل فيروسات وإمّا روابط إلى مواقع إلكترونية خبيثة. ومن الممكن لبعض ملفّات «أوفيس» الخاصة بنظام «ماك» أن تنقل الفيروسات إلى الأجهزة العاملة به، وذلك باستغلال ثغرةٍ أمنيّة موجودة في برنامج «أوفيس» الخاص بنظام «ماك». ورغم سدّ هذه الثغرة منذ ثلاث سنوات، إلا أنّ الحماية من هذه الإصابة لا تكون فاعلة إلا إذا قام المستخدم بتنصيب التحديث او الإضافة الخاصة بهذه المعالجة.

الروابط الموجودة في تلك الرسائل كانت تؤدّي إلى صفحاتٍ تحتوي على شيفرةٍ خبيثةٍ خاصةٍ بنظام «جافا»، تعمل على استغلال ثغرة (CVE–٢٠١١–٣٥٤٤)، مع العلم أنّ هذه الثغرة كانت قد أُقفلت في شهر تشرين الثاني/نوفمبر الماضي. والعنصر المميّز في هذه الهجمة كان وجود مُسقِط (Dropper) – وهو نوعٌ من البرامج يتيح تنصيب برمجيّاتٍ خبيثةٍ بشكلٍ يصعب اكتشافه – على المواقع الإلكترونية الخبيثة، بمقدوره أن يصيب الأجهزة العاملة بكلّ من نظامي «ماك» و «ويندوز»، إذا لم يكن الجهاز يتمتع بنظام «جافا» مُحدَّث.

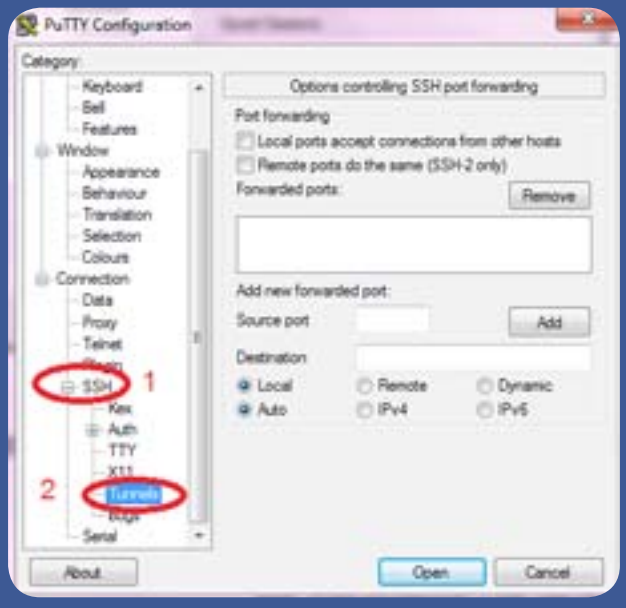
ويقوم المُسقِط بتحديد نظام التشغيل المستعمل في الحاسوب عبر فحص متوالية عميل المستخدم (User Agent String) من المتصفّح، ومن ثمّ انتقاء الحمل الصافي (Payload) – وهو المصطلح الذي يشير إلى محتوى المعلومات التي تتنقّل عبر الإنترت – المناسب والقادر على فتح بابٍ خلفيٍّ في نظام التشغيل يتيح للمهاجمين الدخول. فالحمل الصافي الذي نشره هذا المُسقِط على الأجهزة العاملة بنظام «ويندوز» هو أحد أشكال Ghost RAT، وهو «تروجان» يتيح النفاذ البعيد (Remote Access) . أما في الأجهزة العاملة بنظام «ماك»، فقد استُخدِم حملٌ صافيٌ جديدٌ يشار إليه باسم OSX/Lamadai.A، قامت مؤسسة «إيسِت» (Eset) بتحليله، فوجدت أنّه قد قام بنسخ نفسه إلى: //Library/Audio/Plug–Ins/AudioServer ، فيُظهر لمستخدمي نظام OS X 10.7.2 أنّه ليس دائماً. بعد أن يتم تنصيب هذا الحمل الصافي، يحاول الأخير الإتّصال بخادم التحكم والسيطرة (C&C Server) بشكلٍ مشفّرٍ. وقد استطاعت «ايسِت» أن ترصد مهاجماً يتّصل بآلة اختبار (Test Machine)، ويتصفّح نظام الملفّات (File System) ويستحوذ على نظام علاقة المفاتيح (Keychain File) – البرنامج الخاص ب «ماك» الذي يتيح تنظيم كلمات السر – وملفات «الكوكيز» الخاصة بمتصفّح «سافاري». وقد تم سدّ الثغرة في نظام «جافا» المستخدم في «ماك» في تحديثين هما Mac OS X 10.7.1 Update وMac OS X 10.6 Update الذين أُطلقا في شهر تشرين الثاني/نوفمبر الماضي.

تشفير الإتصال وتجاوز البروكسي بواسطة الـ SSH

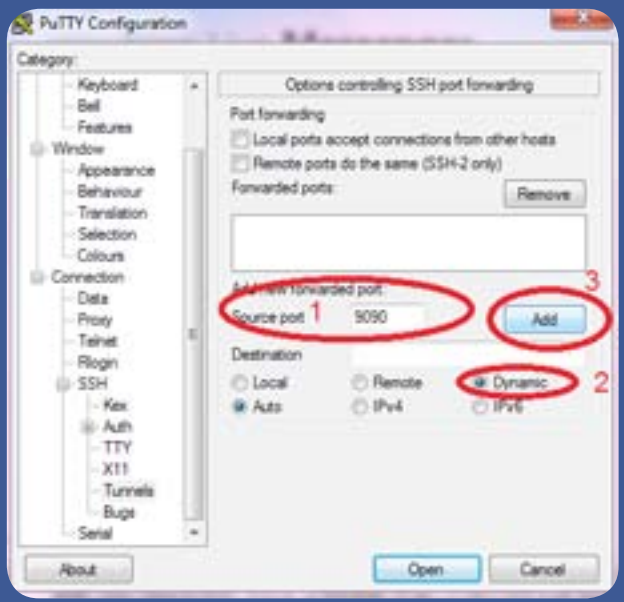
إنّ SSH (Secure Shell أو «الصدفة الآمنة») هو أحد بروتوكولات شبكة الإنترنت، وهو البروتوكول المسؤول عن حماية البيانات التي تتدفّق عبر الشبكة عن طريق تشفيرها أثناء الإرسال وإعادة فكّها أثناء الإستقبال.
لكون الـ SSH بروتوكول، فهو ليس برنامجاً، إلا أنّنا نحتاج لبرامج كي نتحّمن من استخدامه.
نحتاج من أجل تشغيل هذا البروتوكول لما يلي:
– عنوان المخدم أو المعرّف الرقمي IP Address
– المَنفَذ PORT
– إسم المستخدم
– كلمة السرّ
يتمّ إرسال هذه البيانات بواسطة قناة اتّصال مشفّرة (SSL).
نستطيع الإستفادة من خدمةٍ مهمّةٍ جداً عن طريق الـSSH ألا وهي الTunneling التي تتيح إنشاء قناةٍ آمنةٍ لتبادل بيانات الإنترنت وذلك بتفعيل الـSOCKS5 الداخلي ونستطيع بذلك انشاء قناةٍ آمنةٍ للمتصفّحات بجميع أنواعها، بالإضافة إلى برامج التواصل مثل«سكايب» (Skype)... الخ.
– في البداية، نحتاج لبرنامج PUTTY الذي سيعمل كعميل لبروتوكول الـSSH.

تحميل SSH لمستخدمي الويندوز

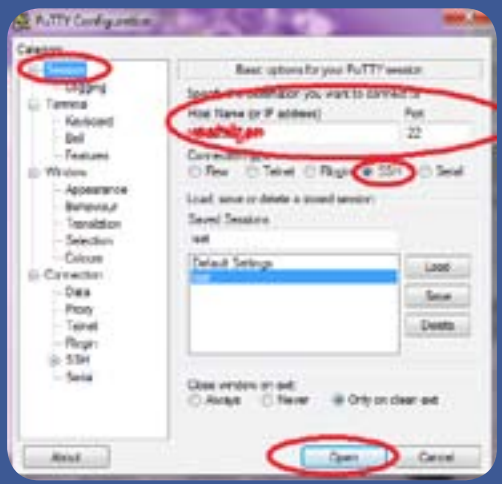
بدايةً، علينا أن نقوم بتنزيل ملف Putty. لكي يعمل البرنامج يجب أن يكون الحاسوب متّصلاً بالإنترنت.
نقوم بفتح البرنامج والذي ستكون واجهته كالتالي:
نقوم تالياً بالضغط على الخيار SSH من القائمة اليُسرى ونتّجه إلى Tunnels.
تعتبر الـ SSH Tunnels إحدى خدمات بروتوكول الـ SSH والتي بدورها تقوم بتحويل الجهاز المراد الإتّصال به الى بروكسي يدعم الـ SOCKS5.



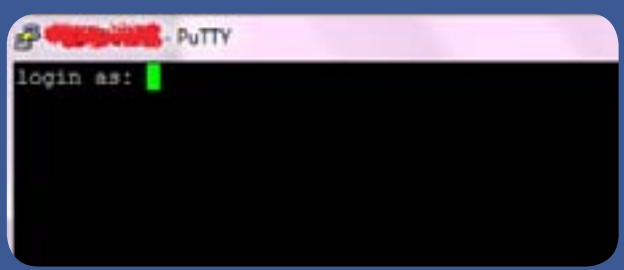
– نقوم بكتابة رقم المَنفَذ المراد فتحه داخلياً من أجل تفعيل الـ SOCKS5 في مربع الـ Source Port ، مثلاً 9090
– ونقوم بتحديد خيار Dynamic من الخيارات، ومن ثم الضغط على Add كما هو مبيّن في الصورة أدناه.



– بعدها يتم الضغط على الخيار Session من مجموعة الخيارات في الجهة اليسرى، وكتابة البيانات التي تم تزويدكم بها.
– HOST NAME وهو عنوان المخدم من الممكن أن يكون IP Address أو قد يكون نطاقاً إلكترونياً (Domain).
– Port وهو المَنفَذ المفتوح في المخدم.
– تحديد خيار SSH كما هو مبيّن.
– الضغط على Open في الأسفل.

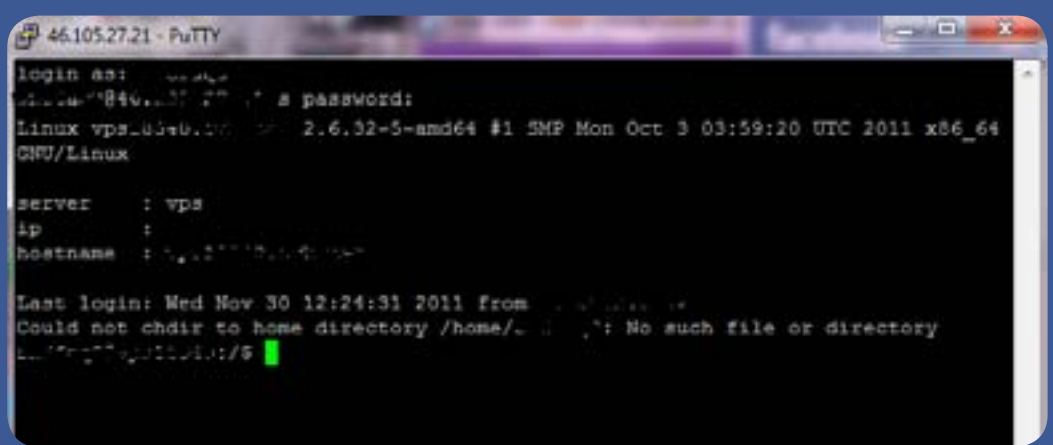


– ستظهر النافذة التالية:



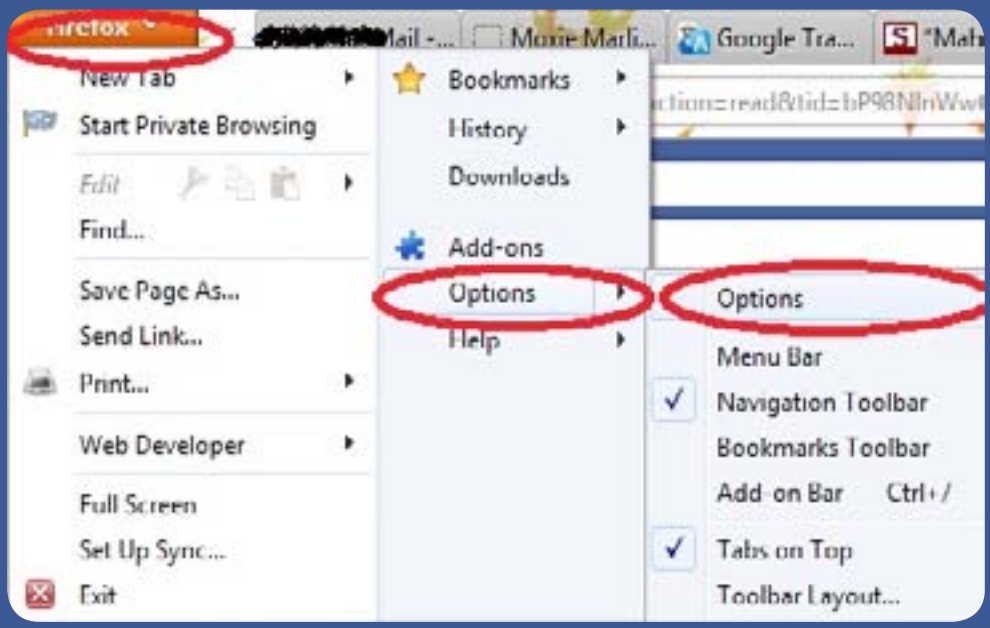
قوموا بإدخال إسم المستخدم والضغط على Enter ومن ثم كتابة كلمة السر، علماً أن كلمة السر لا تظهر لا كنجوم ولا كأحرف.

بعد ظهور هذه الرسالة، والتي تعني أنه تمّ الإتّصال بنجاح بالمخدم عن طريق الـ SSH، سنقوم بتشغيل متصفح «الفايرفوكس» وبرنامج «السكايب» عبر هذا الإتّصال.

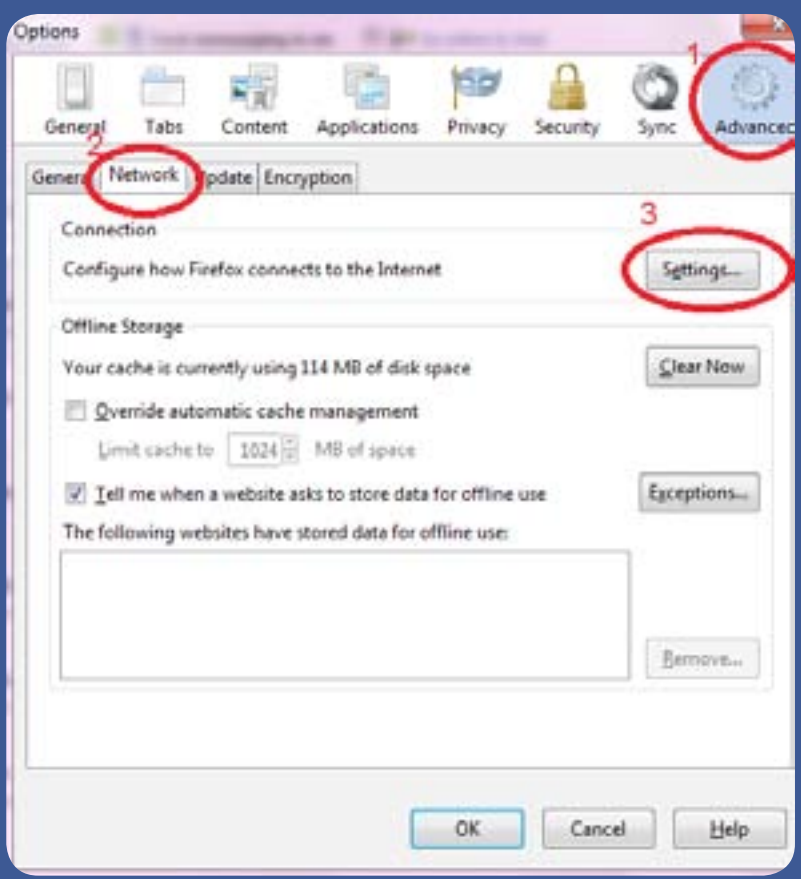


FireFox –:

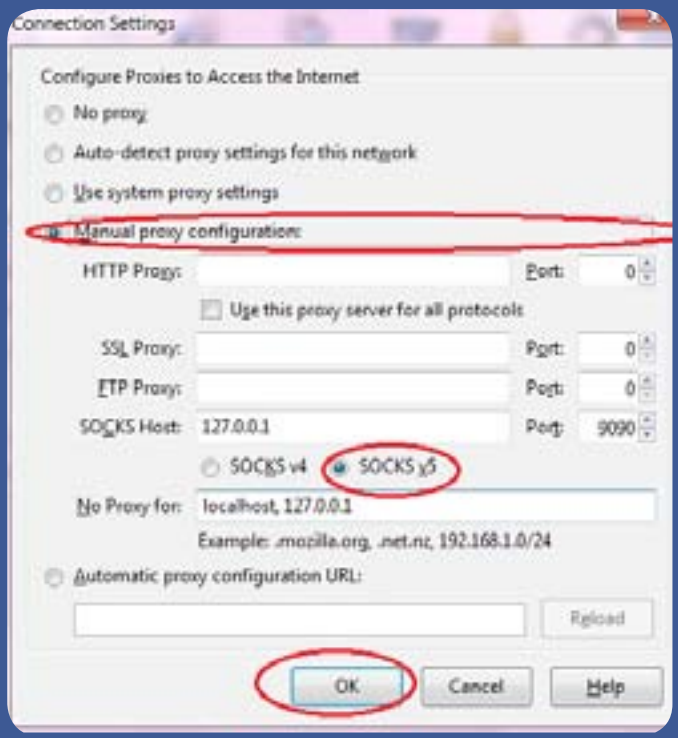
نتجه لقائمة Firefox ومن ثم Options ومن ثم Options مرّة أُخرى.



بعد فتح الخيارات نتجه لخصائص الـ Network كما هو مبيّن في الصورة التالية.

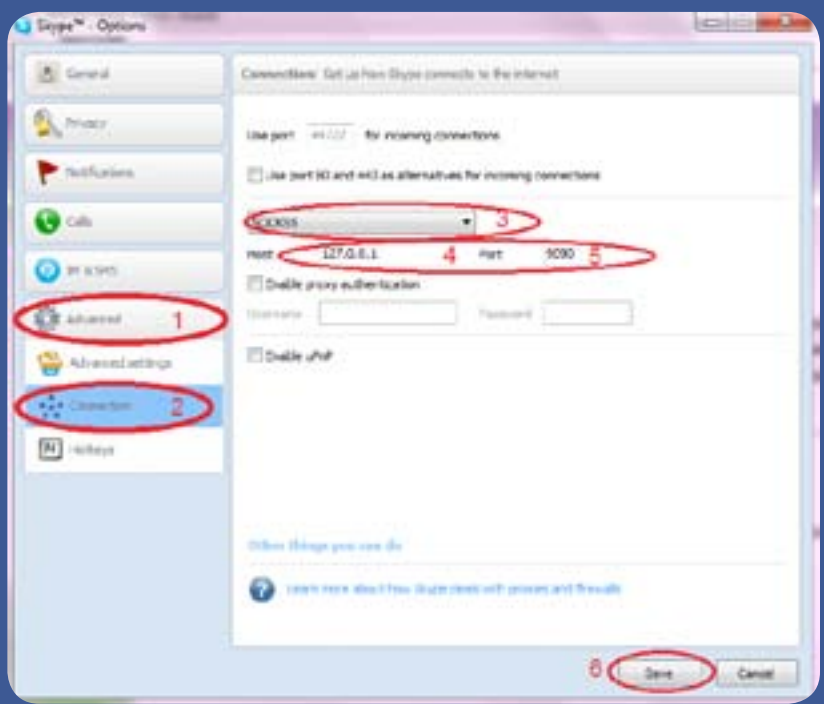


بعدها ستظهر النافذة التالية. يرجى إدخال الأرقام كما هي مع مراعاة تواجد الرقم 0 في مستطيلات المنفذ
والتأكد من إضافة الـ SOCKS Host 127.0.0.1 والبورت الخاص به 9090



- لتشغيل برنامج «سكايب»:

من قائمة Tools نتوجه لخيار Options ومن ثم نتبع الخطوات التالية:



يتوجّب بعد ذلك إعادة تشغيل برنامج «سكايب» وبهذا يكون اتّصالكم مؤمّناً بنسبة مئةٍ بالمئة.

أفضل اختصارات لوحة المفاتيح

أفضل اختصارات لوحة المفاتيح (Keyboard Shortcuts) لتسهيل استعمال الإنترنت والكمبيوتر

تمكّنك اختصارات لوحة المفاتيح من تسريع نشاطاتك اليوميّة أثناء استخدام الإنترنت وإراحة معصمك من النقر على فأرة الكمبيوتر أو الماوس (Mouse). فهناك اختصاراتٌ مُتوفّرةٌ لكل ما يخطر في بالك، من تحرير المحتوى إلى السيطرة على البرامج وتصفُّح صفحات الويب. مثلاً، بإمكانك أن تستعمل اختصاراتٍ لحفظ الرسائل في جيميل (Gmail)، وإضافة روابط إلى مستندات وورد (Word) عدا عن تعيين (Bookmark) الصفحات المفضّلة على الإنترنت.

في هذه المقالة، سيتم التطرّق إلى أفضل الإختصارات المستعملة في لوحة المفاتيح وأكثرها إفادةً في توفير الوقت والجهد عند القيام بمهامٍ على الكمبيوتر.

إختصارات ويندوز الضروريّة

مُعظم اختصارات لوحة المفاتيح التالية يمكن استخدامها في أنظمةٍ مختلفة، إذ تعمل في العديد من برامج الويندوز بالإضافة إلى إصدارات نظام التشغيل مايكروسوفت المُختلفة. من المُمكن أن تكون قد تعرّفت على هذه الإختصارات من قبل، ولكن من المُفيد أن يتُم تذكيرك بإفادتها وطريقة استعمالها.

F1

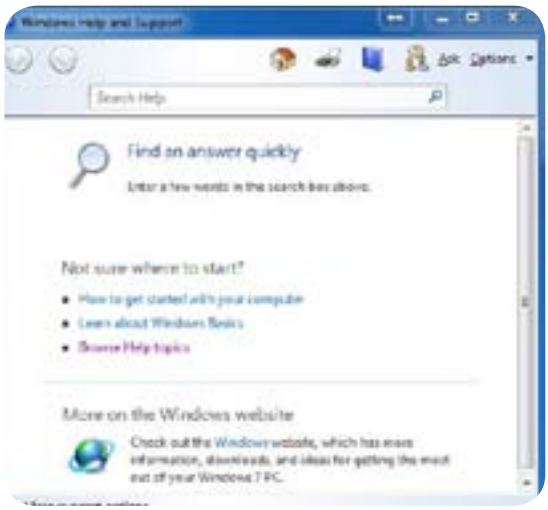
إحصل على المُساعدة (Help)

إذا كنت بحاجةٍ للمساعدة في ويندوز أو في برنامجٍ مُعيّنٍ، قم بالضغط على مُفتاح F1 للحصول على خيارات فتح ملّفات المساعدة ذات الصلة. وتختلف النتائج تبعاً للبرنامج الذي تقوم باستخدامه، لا سيّما أنّ بعض البرامج لا تمتلك خاصيّات المساعدة. أمّا إذا لم يُساهم الضغط على هذا المُفتاح بالحصول على خيارات الدعم، تأكّد أنّ زر Function Lock أو F lock في وضع التشغيل.

Ctrl + C

نسخ المُحتوى (Copy Content)

جنباً إلى جنب مع Ctrl+V، هذا الإختصار هو أحد أهم



الإختصارات التي يفيد أن نعرفها. حدّد أي شيء – نصاً أو ملفاً على سطح المكتب (Desktop) على سبيل المثال – واضغط على هذين المفتاحين لنسخ المحتوى إلى حافظة ويندوز.

Ctrl + X

قطع أو قصّ المحتوى (Cut Content)

وهو يعمل بالطريقة نفسها التي يعمل بها Ctrl+C، إلا أنّه ينقل الملف المُحّدد إلى الحافظة بدلاً من نسخه.

Ctrl + V

لصق المحتوى (Paste Content)

باستخدامه بعد Ctrl+X/Ctrl+C، يقوم هذا الإختصار بلصق المحتوى المنسوخ حيث تضع المؤشّر (Cursor).

Ctrl + A

تحديد الكل (Select All)

وهذا الإختصار يُحدّد كافة الملّفات الموجودة في مجلّد، أو كلّ النصوص/الرسومات في مُستندٍ أو على صفحة ويب.

F2

إعادة تسمية أو تغيير إسم الملفات أو المجلّدات (Rename)

قد يُؤدّي تغيير إسم الملفات إلى إطلاق أو فتح تلك الملفات دفعةً واحدةً. حدّد الملف الذي تريد تغيير إسمه، ثم إضغط على زر أو مفتاح F2 لإعادة تسمية الملف على الفور.

F5

تجديد أو تحديث الصفحة (Refresh)

ويُجدّد هذا المفتاح نافذة صفحة الويب المفتوحة، سطح المكتب، أو المجلد، إلخ.

F10

فتح خيارات القائمة (Open Menu Options)

وظيفة هذا المفتاح هي تفعيل خيارات القائمة. إضغط على F10 متبوعاً بأيٍّ حرفٍ (T لـ Tools أو أدوات على سبيل المثال) لفتح القائمة. كما أنّ الضغط على Alt له الوظيفة ذاتها. ويعمل هذه الإختصار أيضاً في Microsoft Office.

Shift + F10

فتح قائمة الزرّ الأيمن لأيّ ملفٍ أو مُجلّد (View Right-Click Menu)

حدّد الملف أو المُجلّد ثُمّ إضغط على هذين المفتاحين على لوحة المفاتيح لعرض القائمة، وهو ما يعادل النقر على الزر الأيمن من الماوس لتحديد خيار ما.

Ctrl + Z

التراجُع عن الإجراء (Undo Action)

إذا قمت بخطأ في تطبيق ما، سيؤدي هذا الجمع بين المُفتاحين إلى التراجع عن الإجراء الأخير. إستمرّ بالضغط على المُفتاحين للتراجُع عن الإجراء أو العمليّة التي تقوم بها.

Ctrl + Y

إعادة العمليّة (Redo Action)

إذا تراجعت عن إجراء باستخدام Ctrl+Z ثم غيّرت رأيك، إضغط على هذه المفاتيح لاستبدال التراجع.

Alt + Tab

التنقُّل بين نوافذ البرامج (Switch Between Windows)

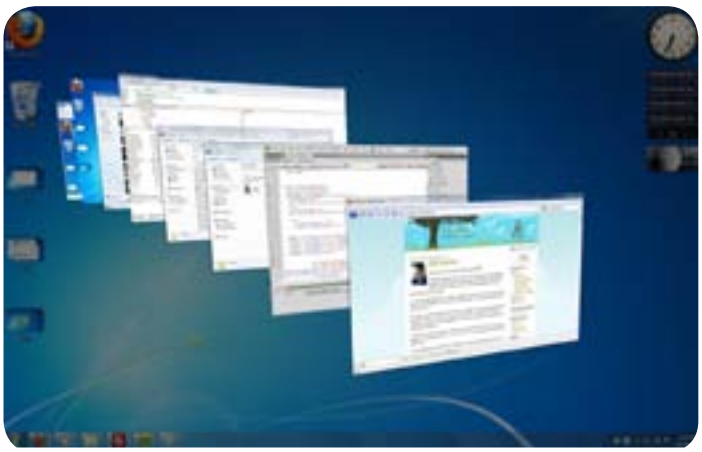
إضغط على هذين المفتاحين فتظهر أمامك قائمةٌ بجميع البرامج أو النوافذ المفتوحة في ذات الوقت. وهكذا تستطيع التنقّل بين هذه البرامج دون استخدام الماوس. وعندما تصل الى النافذة

التي تريدها، توقّف عن الضغط.

Ctrl + Windows شعار مفتاح + Tab

التنقُّل الثلاثي الأبعاد بين نوافذ البرامج (Switch Between Windows in 3D)

التنقُّل الثلاثي الأبعاد هو مهمة تحويل بديلة متوفّرة في ويندوز 7 وفيستا (شرط أن تقوم بتشغيل الإيرو – AERO). إضغط Tab لتصفُّح البرامج المفتوحة في 3D.



Ctrl + Alt + Del

إعادة تشغيل ويندوز (Restart Windows)

يُمكن استخدام هذا الإختصار المعروف بـ»تحيّة الأصابع الثلاثة» لإعادة تشغيل ويندوز، وإطلاق إدارة المهام (Task Manager)، إقفال الكمبيوتر، وتبديل المستخدمين، وتغيير كلمة السرّ الخاصة بك.

Alt + F4

إغلاق البرنامج المفتوح (Close Program)

هذا الإختصار يوفّر عليك الحاجة إلى تحريك الفأرة للضّغط على الرمز X في أعلى الزاوية اليسرى من النافذة.

Ctrl + F4

إغلاق الصفحات أو المُستندات المفتوحة (Close Window)

هذا الإختصار مفيد في حال كان لديك مُستنداتٌ مختلفةٌ مفتوحةٌ في برنامج ما وتريد إغلاق أحدها دون إغلاق البرنامج.

Shift + Delete

حذف الملفّات بصفة دائمة (Delete Files Permanently)

تجاوز سلة المحذوفات (Recycle Bin) من خلال الضغط على Shift عند حذف ملف أو مُجلّد أو مُستند غير مرغوب فيه.

Alt + F6

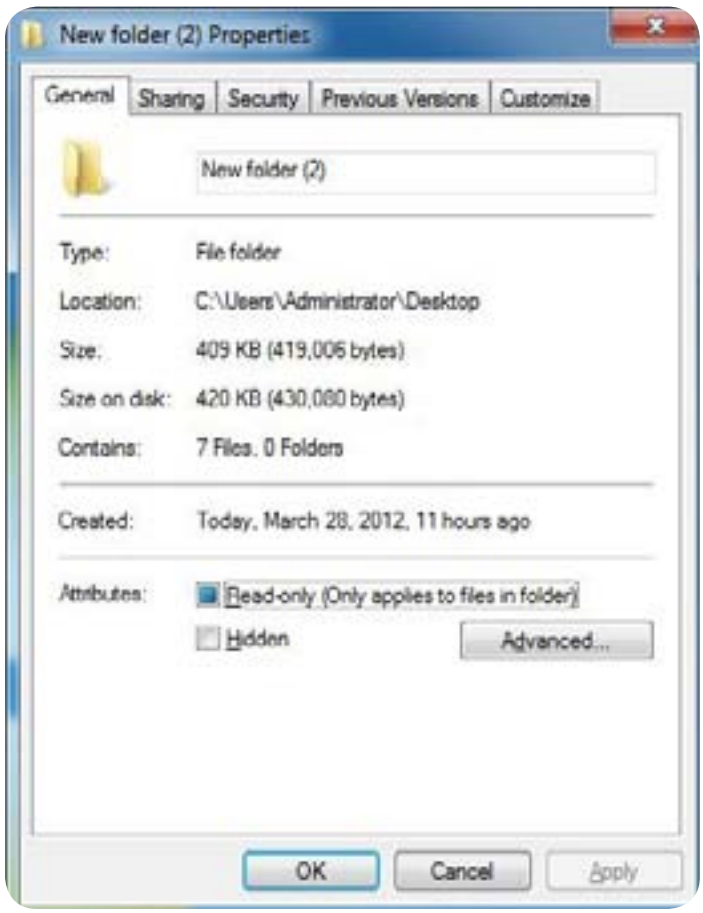
التبديل بين نوافذ البرنامج (Switch between Program Windows)

يتيح لك هذا الإختصار التبديل بين النوافذ المتعددة في البرنامج ذاته، في حال كان لديك أكثر من جزءٍ واحدٍ مفتوحٍ في متصفح الويب الخاص بك، على سبيل المثال.

Alt + Enter

عرض أو إظهار الخصائص (View Properties)

حدّد الملف أو المُجلّد ثم استخدم هذه التركيبة لفتح مربّع أو نافذة الخصائص التابعة له.

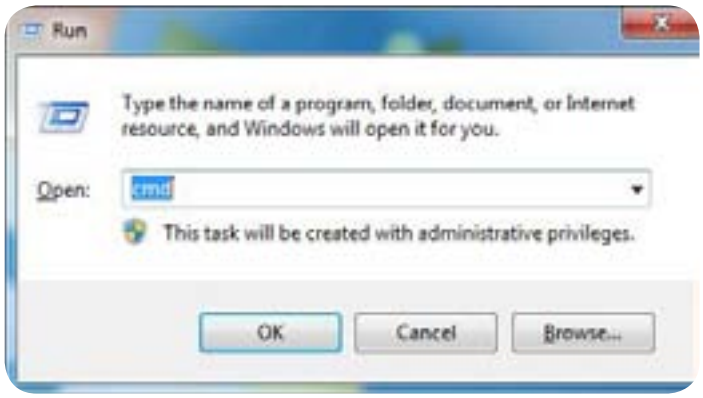


R + مفتاح أو زر شعار Windows

لفتح نافذة تشغيل (Launch Run)

يفتح هذا الإختصار نافذة التشغيل التي تُتيح لك إطلاق ميّزات النظام، مثل:

موجّه الأوامر (Command Prompt) عن طريق كتابة «cmd» بدون علامات الإقتباس « ».



E + مفتاح أو زر شعار Windows

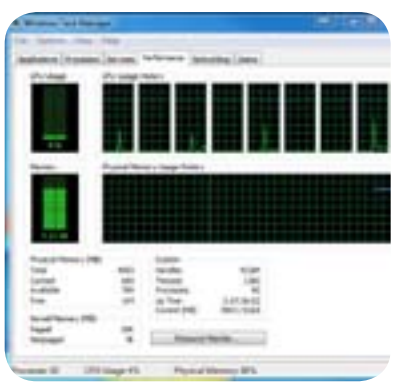
إطلاق أو عرض نافذة ويندوز إكسبلورر (Launch Windows Explorer)

إذا توفّر زر شعار Windows على لوحة المفاتيح، سيتم إطلاق ويندوز إكسبلورر من خلال الضغط على هذين المُفتاحين.

D + مفتاح أو زر شعار Windows

عرض سطح المكتب (View Desktop)

هذا اختصارٌ مفيدٌ عندما تحتاج أن تصل سريعاً إلى سطح المكتب. من خلال الضغط عليه مرّةً واحدةً، سيقوم ويندوز بتصغير (Minimize) جميع البرامج أو النوافذ أو المجلّدات المفتوحة. إضغط عليه مرةً أخرى لاستعادتها.



Ctrl + Shift + Esc

إغلاق البرامج (Close Programs)

برنامج إدارة المهام في ويندوز يتيح لك الوصول إلى بعض المعلومات المفيدة، وإغلاق البرامج التي لا تستجيب.

ويمكنك تشغيله من خلال الضغط بالزرّ الأيمن على شريط المهام (Taskbar) واختيار بدء إدارة المهام (Start Task Manager)، إلّا أنّ استعمال هذا الإختصار في لوحة المفاتيح هو بديلٌ أسرع.

Windows زر + Shift + Left/Right

التنقّل بين الشاشات (Move between Monitors)

هذا اختصارٌ مفيدٌ لأيّ شخص يُشغّل شاشاتٍ مزدوجةً (Dual Monitors) في ويندوز 7 أو فيستا. حدّد النافذة ثم نفّذ هذا الإختصار لنقلها من شاشةٍ إلى أخرى.

إختصارات مُتصفّح الويب

مُعظم إختصارات المُتصفّح التالية تعمل في إنترنت اكسبلورر، وفايرفوكس، وكروم، ويُمكن أن تسهّل وتزيد من سرعة أداء المهام التي تقوم بها على الإنترنت.

Ctrl + T

فتح علامة التبويب (Open New Tab)؛ فتح علامة تبويب جديدة في المتصفح.

Ctrl + W

إغلاق علامة التبويب (Close Tab)؛ إغلاقٌ تلقائيٌ لعلامة التبويب المفتوحة.

Ctrl + Shift + T

إعادة فتح علامة التبويب (Reopen Tab)

إذا قمت بإغلاق التبويب عن طريق الخطأ، إستخدم هذا الإختصار لإعادة فتحه.

Ctrl + Alt + F4

إغلاق كافة علامات التبويب ما عدا واحدة (Close all but one Tab)

هذا الإختصار يعمل في برنامج Internet Explorer فحسب، يُغلق كافة علامات التبويب المفتوحة باستثناء تلك التي كنت تقوم بالإطّلاع عليها.

Ctrl + Tab

تبديل علامات التبويب (Switch Tab)

تستطيع من خلال هذا الإختصار أن تقفز أو تنتقل من علامة تبويبٍ مفتوحةٍ واحدةٍ إلى أخرى دون الحاجة إلى الضّغط على كل منها على حدة.

Ctrl + 1 – 9

تحديد علامات التبويب (Select Tab 1-9) إضغط على مفتاح Ctrl وعلى عددٍ معيّنٍ للإنتقال إلى علامة تبويب مفتوحة محددة. على سبيل المثال، Ctrl + 3 تفتح لك التبويب الثالث من اليسار.

Ctrl + F

البحث على (Find) إذا كنت تبحث عن كلمةٍ أو عبارةٍ على صفحة الإنترنت، سيفتح لك هذا الإختصار نافذة البحث (أو مربع البحث). بعد أن تفتح النافذة، أدخل مُصطلح البحث للعثور على ما تبحث عنه في الصفحة.
ويعمل هذه الإختصار أيضاً في Microsoft Office.

Alt + N

العثور تالياً (Find Next) بعد أن تكون قد بحثت عن كلمةٍ في Ctrl + F، سيُساعدك هذا الإختصار الذي لا يعمل سوى في فايرفوكس على العثور على هذه الكلمة حيث ترد تالياً في الصفحة نفسها.

Ctrl + L

شريط أو مربّع العنوان/فتح (Address Bar/Open) ينقل التركيز إلى شريط العناوين في فايرفوكس وكروم، ويُسلّط الضوء على الرابط (URL) الحالي. أمّا في Internet Explorer، فهو سيعرض نافذة «فتح».

Ctrl + I

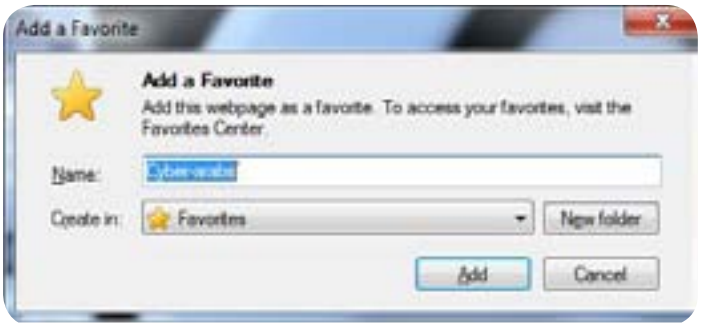
عرض الإشارات المرجعيّة (View Bookmarks) فتح الإشارات المرجعية في فايرفوكس ومجلّد «المفضلة» (Favorites) في إنترنت إكسبلورر. لا يوجد أيّ اختصارٍ مشابه في كروم (Chrome).

CTRL + H

عرض التاريخ (View History) يفتح سجل التصفح بحيث يمكنك الدخول إلى المواقع التي قمت بزيارتها سابقاً.

CTRL + D

إضافة الصفحة كمرجعيّة (Bookmark Page) تتيح لك إضافة صفحة الويب التي تريد الإطّلاع عليها لاحقاً كعلامة مرجعيّة.



مفتاح أو مؤشر مسطرة المسافة Spacebar

إنزل بالشاشة (Scroll Down)
إضغط على مؤشّر Space للنزول بالشاشة على موقع الإنترنت أو الإنتقال بها لأسفل بمقدار شاشةٍ واحدةٍ في وقتٍ واحدٍ. واضغط على Space + Shift للتدرُّج في الصفحة صعوداً.

Ctrl + Enter

إكمال عنوان الويب (Complete Web Address) أكتب إسم موقع على شبكة الإنترنت في شريط العنوان، واضغط على المفتاحين. هذا سيضيف «http://www» لبداية العنوان و «com.» إلى نهايته. أمّا الضغط على Ctrl + Shift + Enter فسيؤدي إلى إضافة «org.» والضغط على Enter +Alt + Shift سيؤدي إلى إضافة «net.» إلى العنوان. وبإمكانك أن تقوم بتغيير لواحق عنوان الموقع الإلكتروني في فايرفوكس باستخدام لاحقة URL المُضافة (https://addons.mozilla.org/en-US/firefox/addon/url-suffix)

Ctrl + +/--

تكبير الحجم (Zoom)
إبق أصبعك على مفتاح Ctrl ثم اضغط على مفتاح «+» للتكبير (Zoom In) ومفتاح «–» للتصغير (Zoom Out). لإعادة محتوى الصفحة إلى حجمه الأصلي، إضغط على Ctrl + 0.

Ctrl + Shift + P

التصفُّح الخاص (Browse in Private) يُشغّل التصفُّح الخاص في إنترنت إكسبلورر وفي فايرفوكس. وهذا يمنع المُتصفّح (Browser) من تخزين أنشطة الويب الخاصة بك.

إختصارات GMAIL

تدعم خدمة البريد الالكتروني التابعة لغوغل Google إختصارات لوحة المفاتيح. ويُمكنك تشغيل هذه الإختصارات أو إيقافها من خلال الذهاب إلى «الإعدادات» (Settings)، والتحقّق من اختصارات لوحة المفاتيح تحت التبويب (General)، والضغط على «حفظ التغييرات» (Save Change)

Ctrl + F5

تحديث صفحة الويب الحاليّة (Hard Refresh) يعمل هذا الإختصار على تحديث الصفحة وتنزيل جميع العناصر مرة أخرى عوضاً عن سحبها من ذاكرة التخزين المؤقت. وهذا يعني أنّه يمكنك الحصول على أحدث نسخة من الصفحة، مع آخر تحديث للمحتوى، بدلاً من المحتوى المُخزّن.

Esc

توقيف تحميل الصفحة (Stop) هذا الإختصار يُعطي أمراً بتوقيف تنزيل الصفحة الحاليّة، وتجميد صور GIF المتحركة حتى لا تضطرّ إلى انتظار تحميل كلّ عنصرٍ من عناصر الصفحة، في حين أنّ ما تريده فقط هو التأكّد من جزء معيّن.

Alt + Home

الذهاب الى الصفحة الرئيسة (Go Home) يُتيح هذا الإختصار تحميل الصفحة الرئيسة (التي كنت قد حددتها في وقت سابق) في التبويب الحالي للمتصفّح.

Ctrl + J

عرض التنزيلات أو التغذيات (View Downloads or Feeds) يفتح هذا الإختصار مدير التحميل في فايرفوكس وكروم، أو قائمة التغذية على RSS شبكة الإنترنت في Internet Explorer.

F7

إطلاق تصفُّح «Launch Caret Browsing» (Caret) وهذه الميزة ترتبط بتشغيل هذا النوع من التصفُّح في فايرفوكس وإنترنت إكسبلورر (ولكن ليس في كروم). مما يعني أنّه عوضاً عن التصفُّح عبر صفحات الإنترنت باستعمال الفأرة، تستطيع أن تضع المؤشّر (Cursor) على جانب الصفحة، والتنقّل في جميع أنحاء النص باستخدام مفاتيح الأسهُم على لوحة المفاتيح. وهذا النوع من التصفُّح مفيدٌ خصوصاً إذا كنت تعاني من مشاكل في الإستخدام، لأنّه يُخفّف من الضّغط على معصمك.

C

إنشاء (Compose)

إضغط على مفتاحC في أيّ صندوق بريد إلكتروني لفتح نافذة «إنشاء» أو كتابة رسالة جديد.ة

Shift+C

إنشاء رسالة في نافذة جديدة (Compose in New Window)

إستخدم هذا الإختصار لفتح مربّع إنشاء البريد (أو رسالة) في نافذة جديدة. وستحتاج إلى السّماح بالإطارات المنبثقة (Pop–ups) عن Gmail لتشغيل هذه الخاصيّة.

R

الرد أو الإجابة (Reply) عند الإنتهاء من قراءة الإيميل أو الرسالة، إضغط على مُفتاح R للرد عليها.

A

الرد على الكل (Reply to All) إذا كُنت تُفضّل الرد على الجميع في الوقت ذاته، تستطيع الضغط على مفتاح A وسيتم توجيه رسالتك الإلكترونيّة إلى الجميع.

F

إعادة توجيه الرسالة (Forward) يمكنك توجيه رسالة وُجّهت إليك إلى أيّ شخصٍ تختاره من خلال الضّغط على F وإدخال عنوان/ عناوين البريد الإلكتروني في حقل: «إلى» (To).

/

البحث (Search) للعثور على رسالةٍ في صندوق البريد الإلكتروني الخاص بك، إضغط على مفتاح «/» ممّا سينقلك إلى مربّع البحث (Search Bar)، ومن ثم إبدأ بكتابة إسم المُرسِل أو جزءٍ من موضوع الرسالة أو المحتوى.

!

إرسال إلى مُجلّد الرسائل غير المرغوب فيها (Send to Spam Folder)

إذا استلمت بريداً عشوائياً أو بريداً غير مرغوب فيه (Junk Mail)، حدّده من خلال وضع علامة (Select) ثم إضغط على مفتاح علامة التعجُّب لنقله إلى مُجلّد الرسائل غير المرغوب فيها.

S

إضافة مُحادثةٍ الى مُجلّد النجوم (Star Folder) أو تمييز مُحادثة برمز نجمة (Star Conversation)

لوضع رمز النجمة على محادثةٍ للإطّلاع عليها لاحقاً، حدّد المحادثة واضغط S. إذا كان قد تمّ تمكين (Enable) ميزة مختبرات النجوم (Superstars Lab Feature) التي يُمكنك الحصول عليها في (إعدادات ← مُختبرات)، فتستطيع الضغط بشكلٍ مُستمرٍ على المُفتاح S والذي سينقلك عبر رموز النجمة المُتاحة.

Y

إزالة الرسالة تلقائياً من العرض الحالي أو الواجهة أو من صندوق البريد الوارد (Remove) from View

قم بتحديد الرسالة أو الرسائل في البريد الإلكتروني، واضغط على Y لوضعها في الأرشيف. هذا يُزيلها من صندوق البريد الوارد الخاص بك (Inbox) ، ولكنّها سوف تكون متاحةً في كل البريد (All Mail). ويمكنك أيضاً أن تستخدم الإختصار ذاته لإزالة النجمة من قائمة البريد أو الرسائل المعلّمة بنجمةٍ (Starred Mailbox).

+

وضع علامة للأهميّة (Mark) إذا كنت تستخدم ميزة «صندوق البريد أو الرسائل الهامّة» (Priority Inbox Feature)، يمكنك استعمال هذا الاختصار لترتيب الرسائل في مجموعات بحسب أهميّتها (مهمة ولم تُقرأ، مهمة، المُعلّمة بعلامة النجمة، وكل شيء آخر).

-

إزالة العلامة أو وضع علامة لغير الأهمية (Unmark) إذا كان Gmail قد قام بنقل رسالة غير مهمّة الى «صندوق البريد الهام»، يمكنك الضغط على مفتاح «-» للإشارة الى عدم أهميّتها أو إزالتها من مجموعة الرسائل المهمة ووضعها في مجموعة أخرى.

#

حذف (Delete) حدّد الرسالة التي تُريد حذفها، واضغط على #. أيضاً، يُستخدم هذا المفتاح لإزالة المستخدمين غير المرغوب فيهم.

G + S

الإنتقال إلى الرسائل المميّزة أو المعلّمة بنجمة (Go to Starred)
إضغط على G ثم S للذهاب لإظهار الرّسائل المُعلّمة بنجمة. هذا سيُساهم في ظهور جميع الرسائل التي قمت بتمييزها بنجمة.

G + C

الإنتقال إلى جهات الإتّصالات (Go to Contacts) يُساهم الضغط على هذين المفتاحين بعرض جهات الإتّصال المحفوظة. وهكذا ستكون قادراً على استيرادها (Import) أو تصديرها (Export) أو تحريرها (Edit).

Tab + Enter

إرسال رسالة (Send Message) بمجرّد إنشاء الرسالة، إضغط على المفتاحَين في الترتيب المشار إليه لإرسالها تلقائياً.

؟

عرض الإختصارات (View Shortcuts) هناك المزيد من الإختصارات في Gmail. للإطّلاع عليها كلها إضغط على زر علامة الاستفهام.(Shift+/)

إختصارات قارئ غوغل (Google Reader)

يدعم قارئ غوغل إختصارات لوحة المفاتيح للملخّصات أو خُلاصات الأخبار RSS. أمّا الإختصارات التالية فتُسهّل استخدام هذه الخدمة، وتبادل المواد مع الأصدقاء.

J/K

الإنتقال بين التدوينات أو المواضيع (Navigate Items) هذه المفاتيح تُساعدك على التنقُّل بين التدوينات كلّ على حدة. الضغط علىJ يقودك إلى المدوّنات القديمة، أما الضغط علىK فيقودك إلى المدوّنات الجديدة.

E

إرسال موضوع معيّن عبر البريد الإلكتروني (Email Item) عندما تُعجبك قصةٌ ما، إضغط على هذا المفتاح لإرسال ملخصٍ عنها ورابط إلى أصدقائك. فقط قم بإدخال عناوينهم الإلكترونيّة مع مُلاحظة إختياريّة.

Shift + S

مُشاركة الموضوع (Share Item) يمكنك مشاركة المواضيع التي تُعجبك من خلال قارئ غوغل. وهكذا سيتمكّن أيّ شخص يُتابعك من رؤية الموضوع أو القصة أو المقالة، إلخ والتعليق عليه. أيضاً، ستكون قادراً على إضافة تعليقٍ خاصٍ بك.

Shift+D

تذييل ومشاركة (Annotate and Share) هذان المفتاحان يسمحان لك بإضافة مُلاحظة إلى القصة، وثم إضافتها إختيارياً إلى مواضيعك التي اخترت أن تُشاركها (مع أو دون وسوم «Tags»).

إختصارات برنامج أوفيس (Office)

إختصارات لوحة المفاتيح التالية تعمل في برامج مايكروسوفت أوفيس (Microsoft Office)
ووُرد (Word) وإكسل (Excel). وبعضها يعمل في أوبن أوفيس (OpenOffice) أيضاً.

Ctrl + N

فتح جديد (Open New) إنشاء مستندٍ فارغٍ (Document) في نافذةٍ جديدةٍ. وهذه المفاتيح تستخدم إعدادات القالب الإفتراضي (Default Template Settings).

Ctrl + O

فتح ملف محفوظ (Open Saved) يتيح لك هذا الإختصار فتح ملف تمّ حفظه أو تخزينه سابقاً. وهو يفتح المُجلّد الأخير الذي قمت بحفظ الملف فيه.

Ctrl + S

حفظ (Save) وهو يحفظ المُستند أو الملف الذي قمت بفتحه. وإذا لم يكن قد تمّ حفظه من قبل، فسيُطلب منك إدخال إسم للملف. وهذا الإختصار يعمل أيضاً في .Gmail

Ctrl + B

خط أسود عريض (Bold) حدّد (Select) الجزء الذي تريده من النص، ثُمّ إضغط على هذه المفاتيح لإضافة خطٍ أسود عريض عليه. إضغط عليه مرّة أُخرى لإزالة التنسيق .(Formatting)

Ctrl + I

خط مائل (Italicise) حدّد جزءاً من النص ثم إضغط على هذه التركيبة من المفاتيح لتمييله.

Ctrl + U

تسطير أو وضع خط تحت (Underline) حدّد جزءاً من النصّ ثم إضغط على هذه التركيبة من المفاتيح لوضع خط تحته.

Ctrl + K

إدراج أو إضافة رابط (Insert Link)

إستخدم هذا الإختصار للصق رابطٍ متشعّبٍ (Hyperlink) معيّنٍ في ملفٍ أو مُستند .Word ويمكنك اختيار النص الذي تُريد عرضه أو إبرازه.

Shift + F3

تغيير حالة الأحرف (Change Case)

قم باختيار كلمة أو كلمات مُتعدّدة واستخدم هذا الإختصار لتغيير حالة الأحرف اللاتينيّة من كبيرة أو صغيرة.

Ctrl + [أو]

تغيير حجم النص (Change Size) حدّد النص الذي تريد تغيير حجمه واستخدم هذه التركيبة في لوحة المفاتيح لتكبير الخط أو تصغيره بمقدار درجةٍ أو نقطةٍ واحدةٍ في كل مرّة.

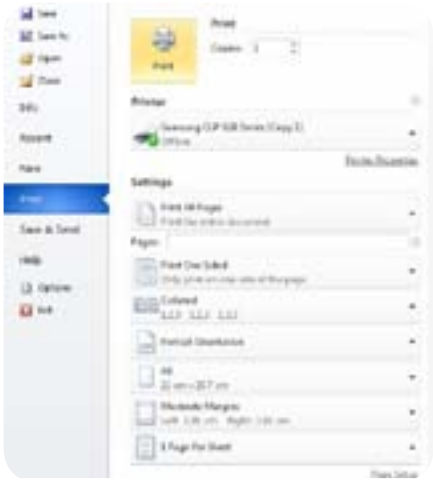
Ctrl + Shift + E

عرض التغييرات (View Changes) وتقوم بتشغيل ميزة مراجعة أو تتبُّع التغييرات (Marks Revision or Track Changes Feature) بحيث يُمكنك أن ترى التغييرات التي أجريتها على المستند.

Ctrl + P

طباعة (Print)

هذا الإختصار يفتح نافذة الطباعة. وهو يعمل أيضاً في متصفّحات الويب والبرامج الأخرى التي تملُك ميزة الطباعة.



Shift + End ثم Delete

حذف المقطع (Delete Section) هذا الإختصار المفيد يُمكّنك من حذف جزءٍ من سطر من النص. ضع المؤشر عند النقطة أو الجزء الذي تريد الإحتفاظ به ثم إضغط SHIFT+END لتحديد الجزء غير المرغوب فيه، واضغط على حذف (Delete) أو مفتاح الإرجاع (Backspace) لإزالته.

F7

التدقيق الإملائي (Spell Check)

إضغط على هذا المفتاح وسيقوم Word بتشغيل التدقيق الإملائي والنحوي باستخدام القاموس الإفتراضي (Default Dictionary).

Shift + F7

إستعمال قاموس المفردات (Use the Thesaurus)
حدّد كلمةً ما ثم إضغط على هذين المفتاحين للبحث عنها في قاموس المرادفات المدمج في البرنامج.

Ctrl + Space

إزالة التنسيق (Remove Formatting)
حدّد جزءاً من النص واستخدم هذا الإختصار لإزالة أي تنسيق منه (اللون الأسود الغامق، الخط المائل، والروابط التشعبيّة، إلخ). وهكذا سيعود النص إلى وضعه السابق قبل إجراء التعديلات أو التغييرات.

Alt + Ctrl + S

تقسيم النافذة (Split Window) وهذا الإختصار يقوم بتقسيم النافذة حتى تتمكّن من مشاهدة أجزاءٍ مختلفةٍ من مستندٍ طويلٍ أو جدول بيانات (Spread Sheet) مُعقّدٍ في الوقت ذاته. ولإزالة التقسيم ليس عليك سوى الضغط على Alt + Shift + C.

إختصارات خاصة برنامج Excel

Ctrl + ;

إدراج أو إضافة التاريخ (Insert Date) في برنامج Excel
قم بتحديد خليّةٍ فارغةٍ (Blank Cell) في Excel واضغط على هذه التركيبة من المفاتيح لإضافة التاريخ الحالي أو تاريخ اليوم.

Ctrl + Shift + ;

إدراج أو إضافة الوقت (Insert Time) كما هو الحال مع الإختصار أعلاه، حدّد خليةً فارغةً واضغط على هذه التركيبة من المفاتيح في لوحة المفاتيح لإدخال أو إضافة الوقت الحالي.

Ctrl + 9

إخفاء البيانات (Hide Data) بمساعدة هذا الإختصار، يمكنك إخفاء صفوف البيانات في Excel إذا كنت لا تريد أن يقوم أحّد بالإطّلاع عليها. فقط إضغط على خلية في الصف (Row)، ثم إضغط على مفاتيح التركيبة. وسوف تكون البيانات محفوظةً هناك، وإنّما فقط مخفيّة.

Ctrl + Shift + 9

إظهار البيانات (Unhide Data) عندما تقوم بإخفاء البيانات، قد ترغب بالإطّلاع عليها مرّة أخرى عند نقطة مُعيّنة. أنقر واسحب (Drag) لتحديد صفوف البيانات المخفيّة (يمكنك اختيار عدد الصفوف الذي تريده، وهو أمرٌ مفيدٌ في حال استعصى عليك تذكُّر المكان الذي وضعت فيه الصف المخفي)، ثم إضغط على هذا الإختصار.

إختصارات نظام التشغيل ماكنتوش MAC OS X

العديد من إختصارات الويندوز تعمل على أجهزة ماكنتوش أيضاً فقط إضغط على المفتاح أبل (Apple (Key أو مفتاح الأمر (Command Key) بدلاً من Ctrl. ولكن هناك أيضاً العديد من اختصارات لوحة المفاتيح الخاصة بنظام التشغيل (OS X).

Apple + Shift + Option + Delete

إفراغ سلّة المحذوفات أو المُهملات (Empty Trash) إذا كنت تُريد إفراغ سلة المهملات، قم باستخدام هذه التركيبة من المفاتيح، وسوف تقوم بالتخلُّص من الملفات غير المرغوب فيها دون طلب التأكيد منك.

Apple + Shift + Option + Esc

إغلاق إجباري (Force Quit) إذا كنت تواجه مشكلةً في إغلاق تطبيق (Application) معيّن، إستخدم هذا الإختصار لإجباره على الإغلاق. ليس هناك من حاجة لتأكيد الموافقة على هذا الإجراء.

Apple + Option + Y

عرض شرائح الصّور (View Photo Sildeshow) يُمكنك عرض الصور على القرص الثابت وملئ الشاشة من خلال تحديد الصور والضغط على هذا الإختصار. ستحتاج إلى تشغيل إصدار OS X 10.5.

Apple + Shift + U

فتح مُجلّد الخدمات أو المرافق (Open Utilities)

إستخدام هذا الإختصار مفيدٌ لفتح مُجلّد المرافق الذي يحتوي على أدواتٍ مفيدةٍ مثل برنامج Grab لالتقاط الصور عن الشاشة (Screen Grabbing)، وأداة السيطرة على الصوت (Voice Control)، وخاصيّة تسجيل الصوت (Voiceover) ومُراقبة النشاط (Activity Monitor)

Apple + Shift + Option + Q

تسجيل الخروج (Log Out) تستطيع البدء بتسجيل الخروج الفوري باستخدام هذا الإختصار. ليس هناك حاجة لتأكيد الموافقة على هذا الإجراء.

إختصارات نظام التشغيل لينُكس (Linux)

الإختصارات التالية كلها لأوبونتو (Ubuntu)-- أكثر توزيعات لينكس شعبيّةً في الإستخدام المنزلي -- ولكنّها تعمل أيضاً في غيرها من توزيعات نظام التشغيل هذا المفتوح المصدر.

Alt + F1

إطلاق التطبيقات (Launch Applications)

إضغط على هذه التركيبة من المفاتيح لفتح قائمة التطبيقات (Applications Menu) التي تسمح لك بالدخول إلى جميع البرامج والألعاب والوسائط المتعدّدة (Multimedia) على جهازك.

Ctrl + Alt + T

فتح نافذة الطرفيّة (Open Terminal Window)

إذا ضغطت على هذه المفاتيح، ستظهر وحدة (Console) لينكس حيث يُمكنك إدخال الأوامر (Commands).

Ctrl + Alt + Left/Right

التنقُّل بين مساحات العمل (Navigate Workspaces)

هذا الإختصار المفيد يسمح لك بالتنقُّل السريع بين مساحات العمل الأربع المُتاحة.

Ctrl + Alt + Shift + Left/Right

نقل النافذة (Move Window)

نقل النافذة المُحدّدة أو المُختارة مساحة عمل واحدة إلى اليسار أو اليمين.

Alt + F10

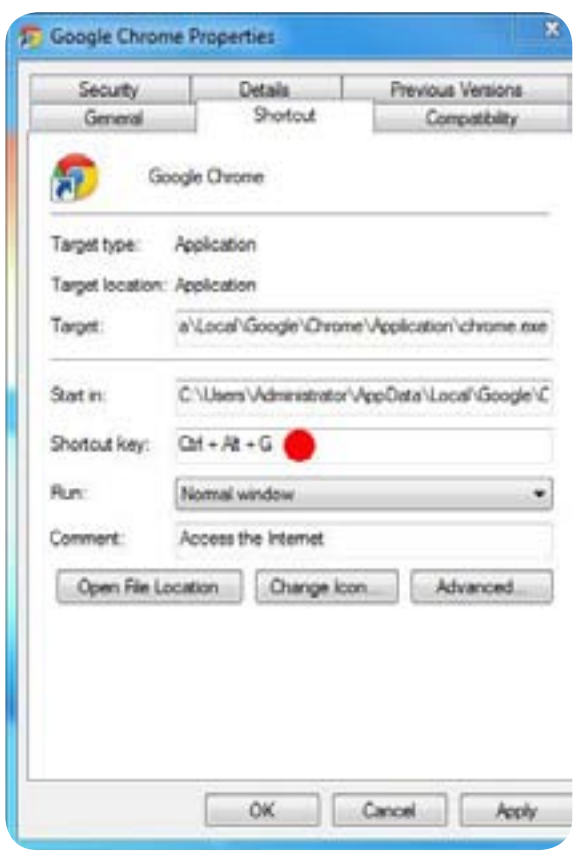
تكبير النافذة (Maximize Window) هذا الإختصار يقوم بتكبير نافذةٍ مفتوحةٍ. وبالإمكان إعادتها إلى حجمها الأصلي عن طريق الضغط على مفتاحي Alt + F5.

ورشة عمل مُصغّرة

كيف تقوم بإنشاء إختصاراتٍ خاصةٍ بك للوحة المفاتيح؟

١. يسمح لك برنامج ويندوز Windows بتعيين اختصاراتٍ للبرامج أو المُجلّدات أو صفحات الويب المفضلة لديك حتى تتمكّن من تشغيلها أو إطلاقها وفتحها باستخدام لوحة المفاتيح. للبدء، سنريك كيفيّة القيام بذلك من خلال اختصار أيّ برنامجٍ على سطح المكتب، كما أنّ الخطوات المتّبعة تعمل أيضاً مع العناصر الموجودة في قائمة البداية (Start Menu). إبدأ بالنقر على الجهة اليمنى من الماوس (Right Click) على الإختصار وقم باختيار «خصائص» (Properties).

٢. عندها ستفتح النافذة أو المربّع على تبويب الإختصار (Shortcut). أنقر داخل مُربّع مفتاح Shortcut، ثم إضغط على أي حرف على لوحة المفاتيح. من الأفضل أن يعتمد اختيار الحرف على البرنامج الذي تقوم بإطلاقه (مثلاً: G لبرنامج Google Chrome). وسيتم تعبئة بقيّة الإختصار تلقائياً مع تجنّب أي تعرُض مُحتمل مع تركيبات المفاتيح الموجودة.



الآن، وعندما تضغط على تركيبة المفاتيح في لوحة المفاتيح، سيبدأ البرنامج.

٣. لفتح مجلدٍ باستخدام لوحة المفاتيح، أولاً، قم بإنشاء اختصارٍ له على سطح المكتب. إضغط بالزر الأيمن فوق المجلد الأصلي وقم باختيار «أرسل إلى».(Send to) «سطح المكتب إنشاء إختصار». «(Desktop Create Shortcut)» إضغط على الإختصار الجديد من خلال الزر الأيمن، واختر «خصائص» (Properties) ، وكرّر الخطوة ٢.

٤ لإنشاء اختصار إلى موقع ما على شبكة الإنترنت، أُنقر بالزر الأيمن على سطح المكتب واختر «جديد» (New)، ثم«إختصار».(Shortcut) عندما يفتح «معالج إنشاء الإختصار»(Create Shortcut Wizard) أدخل عنوان الموقع(URL) واضغط على «التالي» أو (Next)، الآن، أعطِ إسماً للإختصار الجديد، ومن ثم انتهاء (Finish).
الان أنقر بالزر الايمن على الإختصار وأدخل مفتاح الإختصار الذي تريد استخدامه.

إمنع شبكة شركات الإعلانات من التجسُّس عليك!

أيتملكّك شعور بين الفينة والأخرى بأنّك مُراقب على الإنترنت؟ يكشُف روبرت إيرفن الأدوات والإضافة (Add-on) المجانيّة التي من شأنها إيقاف الشركات من رصد ما تقوم به على الشبكة الإلكترونيّة.

إمنع Gmail من قراءة رسائلك الإلكترونيّة

إذا كنت من مُستخدمي Gmail المُعتادين، فستكون قد لاحظت أنّ الإعلانات التي تظهر في أسفل جانب صندوق البريد الوارد (Inbox) غالباً ما تكون على صلة مُباشرة بمُحتوى رسائل البريد الإلكترونيّة (Emails). مثلاً، إذا كان هناك هاتفٌ محمولٌ مذكور في الرسالة التي تلقّيتها، فقد تُلاحظ روابط للمواقع (Links) التي تُقارن أحدث الصفقات على الشبكة الإلكترونيّة المتعلقة بالهواتف المحمولة. والسبب هو أنّ «غوغل» (Google) يقوم بمسحٍ كاملٍ لجميع رسائلك الإلكترونيّة ويرصد الكلمات الدلاليّة (Keywords)، وذلك من أجل إيصال أو نشر الإعلانات المُوجّهة، وهي عمليّةٌ يعتبرها الكثير من الناس انتهاكاً للخصوصيّة. ولكن، ولحُسن الحظ، هناك طريقةٌ تُمكّنك من منع Gmail من «قراءة» رسائلك الإلكترونية، بحيث يَعرُض صندوق البريد الوارد الإعلانات العامّة بدلاً من تلك الموجّهة. أمّا هذه الطريقة فتشمل عدّة خطوات، وهي:

– إضغط على الرمز «خيارات» (Options) في الزاوية اليُمنى العليا.

– قم باختيار «إعدادات البريد» (Mail Settings).

– إنتقل إلى قسم «إشارات الأهميّة للإعلانات» (Importance Signals for Ads).

– قم باختيار «الانسحاب» (Opt out).

لمعرفة المزيد عن الإعلانات في Gmail، راجع «صفحة الدعم» (Support Page) في «الإعلانات في جي ميل وبياناتك الشخصية». (Ads in Gmail and Your Personal Data)

إمنع الفايسبوك (Facebook) من مُلاحقتك

يظهر زر «الإعجاب» (Like Button) على الفايسبوك في الملايين من صفحات الويب كوسيلةٍ للتوصيّة بالمضمون الذي يحوز على إعجابك. ولكن هذا الزر، بالإضافة إلى زر الإتّصال (Connect Button)، قد أصبح مصدر قلق من ناحية الخصوصيّة.

وقد ذكرت مجلّة PC-PRO في عددها الصادر في أيلول/سبتمبر من العام ٢٠١١ أنّ أدوات مُشاركة الإحتكاك أو (Frictionless Sharing) على الفايسبوك تسمح بتعقُّب نشاطاتك على شبكة الإنترنت، حتى بعد تسجيل الخروج من حسابك.

لحسن الحظ، يمكنك وقف هذاالتعقّب من خلال استخدام إضافةٍ بسيطةٍ للمتصفّح (Browser Add-on) تُسمى «قطع إتّصال فايسبوك». (Facebook Disconnect)

وهذه الأداة المفيدة والمتوفّرة «للكروم» (Chrome) و«الفايرفوكس» (Firefox) و «السفاري» (Safari) تمنع المواقع من إرسال بياناتك إلى «الفايسبوك». أي أنّك تستطيع الدخول إلى حسابك في «الفايسبوك»

كالعادة، ولكن عند تسجيل الخروج، لن يقوم هذا الموقع بتعقّبك في أنحاء الشبكة الإلكترونيّة.

إمنع التعقُّب على الإنترنت (Block Web Tracking) باستخدام غوستري (Ghostery)

Ghostery هو إضافة (Add–on) رائعة للمُتصفّح، تعمل على كشف

عناصر التعقُّب الخفيّة في صفحات شبكة الإنترنت. أما هذه العناصر، فترصد كلّ تحرّكاتك وأنشطتك عند تصفُّح المواقع الإلكترونيّة، ثم تُبلّغ المعلومات للشركات المُهتمّة بالبيانات الشخصيّة.

يقوم «غوستري» بشكل تلقائي بتعداد حشرات الويب (Web Bugs) فحسب، ولكنّك تستطيع حماية خصوصيّتك من خلال منع المتعقّبين المحدّدين. عندما تعرض الإضافة قائمة بالمتعقّبين الذين وجدتهم في إحدى الصفحات، حرّك مؤشّر الفأرة فوق إدخال (Entry) وحدّد الخيار منع (Block). كبديل، قم باختيار خيارات (Options) من قائمة غوستري وحدّد خيار تفعيل منع الحشرات الإلكترونيّة (Enable Web BugBlocking).

يُمكنك اختيار الإدخالات أو المُشاركات الفرديّة (Individual Entries) مثلاً، في حال كنت تريد السماح «لفايسبوك» بمعرفة ما تفعله.

Ghostery مُتوفّر لجميع المتصفّحات الرئيسيّة على الويب، وقد أصدر مُؤخراً الإصدار الأوّل لبرنامج أوبرا «Opera Software».

إلغاء الإعلان السلوكي (Opt out of Behavioral Advertising)

تمّ إنشاء موقع خياراتك على الإنترنت أو (Your Online Choices) من قبل مكتب الإعلانات عبر شبكة الإنترنت (Internet Advertising Bureau) وذلك من أجل توفير المعلومات حول الإعلان السلوكي (النوع الذي يعرض الإعلانات على أساس الأنشطة التي تقوم بها على شبكة الإنترنت). إحدى ميّزات الموقع المفيدة هي صفحة خياراتك (Your Choices)، والتي تُتيح لك الإنسحاب/عدم الإنسحاب من اختيار عرض الإعلانات من قائمة طويلة من الشركات، من خلال الضغط على زر التشغيل (On) أو الإيقاف (Off) بجانب أسماء الشركات، أو إختيار إيقاف تشغيل جميع الشركات (Turn Off All Companies).

بالإضافة إلى ذلك، يُمكنك إلغاء تقنيّة «كوكي النقر المزدوج من غوغل» (Google Double Click Cookie) والتي تُساعد مُحرّك البحث (Search En دgine) على عرض الإعلانات، من خلال الضغط على زر الإلغاء (Opt Out Button) في صفحة الإعلان والخصوصيّة (Advertising and Privacy).

من المُفيد أيضاً تحميل إضافات للمُتصفّح، مثلاً للتحكُّم في خواص المتصفّح للكروم (Keep My Opt–Outs for Chrome) وبيف تاكو لفايرفوكس (Beef TACO for Firefox)، لقدرتهما على منع «كوكيز الإعلان السلوكي» تلقائيا.(Block Behavioral–Advertising Cookies)

ولكن الإنسحاب هنا لن يقوم بمنع أو حجب جميع الإعلانات على الإنترنت، ولذلك تستطيع أن تُجرّب مانع الإعلانات (Adblock Plus)، بالرغم من أنّه سيمنع فقط ظهور الإعلانات المُريبة والتي ستجعلك تشعر بأنّك مُراقب.

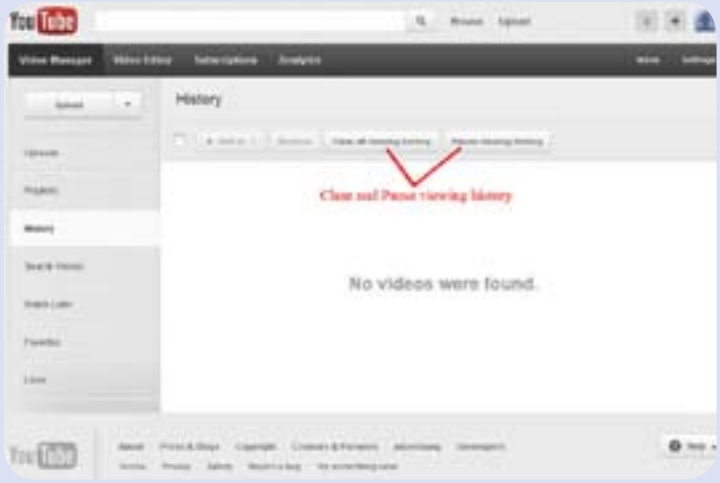
أوقف يوتيوب Youtube عن إخبارك بما يجب أن تشاهده

يقوم يوتيوب (Youtube) باقتراح عدد من الفيديوهات (Videos) على صفحته الرئيسيّة بناءً على الكليبّات (Clips) التي شاهدتها مُؤخراً، وكما هو الحال مع أمازون، إن هذه الإقتراحات ليست موضع

ترحيب في جميع الأوقات، وخصوصاً على جهاز كومبيوتر مُشترك.
ولكن الخبر السار هو أنّه هناك طريقةٌ لإيقاف هذه الإقتراحات دون الحاجة إلى تسجيل الخروج من الموقع:

– إضغط على «إسم حساب المُستخدم» الخاص بك (Account Name) في أعلى الزاوية اليُمنى من الصفحة
– قم باختيار «إعدادات» (Settings)
– إختر «فيديوهاتي وقائمة التشغيل» (My Videos & Play lists)
– إضغط على رابط «التاريخ» (History)، وإمّا قُم بإزالة جميع المُشاركات الفرديّة من قائمة تاريخ مُشاهداتك (My Viewing History) وذلك للتوقُّف عن تلقّي الإقتراحات المبنيّة على هذه الفيديوهات، أو إضغط على زر «مسح كل تاريخ المُشاهدة» (Clear All Viewing History) لمسحها جميعها. ومن ثم إضغط على ايقاف تاريخ المشاهدة (Pause Viewing History) لايقاف هذه الخدمة.

تشغيل حماية المُتصفّح من التعقُّب



تملُك جميع إصدارات المُتصفّحات الرئيسيّة أدوات إضافاتٍ لمنع المواقع الإلكترونيّة من رصد أو مُراقبة أنشطتك على الإنترنت.

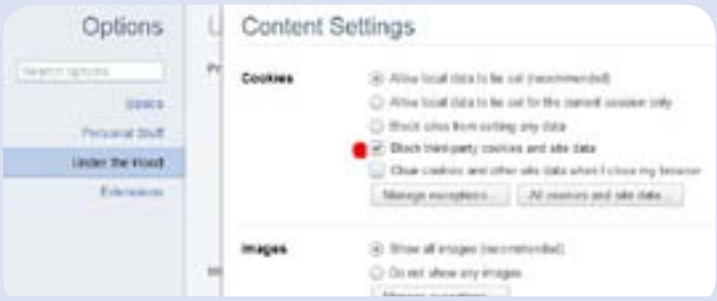
في فايرفوكس (Firefox):

– إذهب إلى أدوات، خيارات، وخصوصيّة (Tools, Options, Privacy)
– إختر خيار «أخبر المواقع الإلكترونيّة بأنني لا أرغب في أن أكون مُتعقّباً» (Tell Websites I Do Not Want to be Tracked)

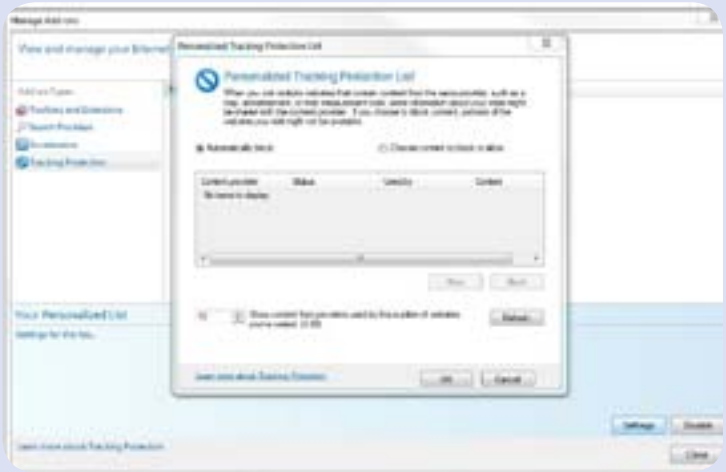
في كروم (Chrome):

– إضغط على أيقونة مفك البراغي أو المفك الإنكليزي (Spanner Icon)
– إختر «خيارات» (Options) ثم «تبويب» (Under the Hood) ثم «إعدادات المُحتوى» (Content Settings)
– قم باختيار «إمنع المواقع من ضبط البيانات» (Block Sites from Setting any Data) و«منع مواقع من طرف ثالث من وضع كوكيز» (Block Third–Party Cookies from Being Set)

في إنترنت إكسبلورر ٩ (Internet Explorer ٩):



– قم باختيار خيار الحماية من التعقُّب (Tracking Protection) من قائمة الأدوات (Tools) أو الأمان (Safety)
– حدّد خيار «قائمتك الشخصيّة» (Personalized Menu)، واضغط فوق تمكين (Enable)
– إختر خيار «إمنع تلقائياً» (Automatically Block)، واضغط على (OK).



إيقاف ملفات الإرتباط «كوكيز» من تخزين البيانات الشخصيّة في فلاش بلاير (Stop Flash Cookies (Storing Personal Data

يُعد برنامج «أدوبي فلاش بلاير» Adobe Flash Player، المعروف بمُشغّل الفلاش، من الإضافات الضّروريّة لتشغيل الفيديو، والألعاب، والرسوم المتحرّكة على الإنترنت، ولكنّه قد يقوم بالتجسُّس على نشاطاتك على الإنترنت. وفقاً لمُدوّنة شركة الأمن ESET، فإنّ «الفلاش كوكيز يسمح لشبكات الإعلان على الإنترنت بتعقُّب كل استخداماتك الإلكترونية بشكل سريّ وفريد. وبما أنّ «كوكيز الفلاش» يستطيع تحديد هويتك (أو تحديد الكومبيوتر الذي تستعمله) بطريقة فعّالة وفريدة، فهو يُسهّل على وكالات الإعلان على الإنترنت الحصول على معلوماتٍ وصنع ملفٍ عنك على وجه التحديد».

تُستخدم بعض خدمات فلاش كوكيز لأغراضٍ مشروعة، مثل تسجيل علاماتك العالية في الألعاب على الإنترنت، ولكن إذا كنت تشعر بعدم الإرتياح حيال مُشاركة بياناتك الشخصيّة، فتستطيع

منعها:

– إذهب إلى «مُدير إعدادات مُشغّل الفلاش» (Flash Player Settings Manager) على الموقع التالي : http://phtshp.us/flash279

– إضغط على لوحة إعدادات التخزين العالميّة (Global Storage Settings Panel)

– قُم بسحب شريط التمرير (Slider Bar) إلى أقصى اليسار لمنع المواقع من تخزين المعلومات على جهازك دون إذن منك.

– إلغاء خيار «السماح لمحتوى الفلاش التابع لطرف ثالث بتخزين البيانات على حاسوبك» (Allow Third–Party Flash Content to Store Data on Your Computer)

أما من جهة حذف «كوكيز الفلاش» (Flash Cookies) عن المتصفّح، فقم بالضغط على «لوحة إعدادات التخزين في الموقع» (Website Storage Settings Panel)، ثمّ اختر «إحذف كل المواقع» (Delete All Sites).

إخفِ آثارك من خلال الإضافة «إضغط ونظّف» (Click&CleanAdd–on)

إذا كنت حقاً قلقاً بشأن الخصوصيّة على الإنترنت، فقم بتحميل الإضافة «إضغط ونظّف» Click&Clean، المُتوفّرة للفايرفوكس وكروم.

وتُساعدك هذه الإضافة على إزالة آثار الأنشطة الخاصة بك على شبكة الإنترنت من المُتصفّح والقرص الثابت (Hard Disk) مع أدنى حد من الإزعاج.

بدجين

«بدجين» يربط بين برامج الدردشة المختلفة بشكلٍ آمنٍ

تتيح برامج الدردشة أوالتراسل الفوري (Instant Messaging) فرصة التواصل السريع وفي أغلب الأحيان المجاني، مما يسهّل الإتصال بين الأصدقاء أو الزملاء في العمل، فيوفّر ذلك المال والوقت على المستخدم. إلا أنّ المشكلة تبرز إذا كان أصدقاؤكم يستخدمون برامج مختلفة للتراسل الفوري، مما يحتّم عليكم أن تفتحوا أكثر من برنامج في وقت واحد.

يشكّل برنامج «بدجن» (Pidgin)، وهو مجانيٌّ ومتاحٌ للجميع، حلاً لهذه المشكلة، إذ يمكن للمستخدم أن يدير عدة برامج للتراسل الفوري من مكان واحد، مما يتيح التواصل مع مستخدمين آخرين يستعملون هذه البرامج المختلفة من خلال استعمال واجهةٍ واحدةٍ فحسب عوض فتح عدة برامج بشكل منفصل.

أما النقطة الأهم، فهي أنّ بمقدور «بدجين» أن يؤمّن التواصل الآمن عند تنصيب (OTR Off the Record)، وهو Plug-in يتيح تعطيل تسجيل المحادثات بالإضافة إلى تشفير محتواها. من أجل التمتّع بهذ الخدمة، يتوجّب على كلٍّ من الطرفين اللذين يجريان المحادثة أن يستخدما «بدجين» و OTR، كما يجب اختيار مفتاح تشفير لكل من برامج الدردشة على حدة («جي توك»، «ياهو»، إلخ) ، ويتوجّب تفعيل OTR من قبل الطرفين أيضاً.

يؤمن «بدجن» الدعم لستة عشرة برنامجٍ مختلفٍ للتراسل الفوري، بالإضافة إلى تلك التي تطبّق بروتوكول XMPP ، من دون الحاجة إلى تنصيب Plug-ins، وهي:

- AIM
- Bonjour
- Gadu-Gadu
- Google Talk
- Groupwise
- ICQ
- IRC
- MSN
- MXit
- MySpaceIM
- SILC
- SIMPLE
- Sametime
- Yahoo!
- Zephyr

ويتيح البرنامج أيضاً العمل مع برامج الدردشة الأخرى (غير تلك المذكورة أعلاه) إذا ما تمّت إضافة الـ Plug-ins المناسبة.

يعمل البرنامج مع أنظمة التشغيل المختلفة مثل «ويندوز» والأنظمة المفتوحة المصدر مثل الـ«لينوكس». ويمكن استخدام «بدجن» مع نظام «ماك»، إلا أنّ برنامج «أديوم» يتيح الخصائص نفسها إلى حدّ ما، ويتطابق

بشكل أفضل مع «ماك» لكونه مصمّماً خصيصاً له، كما أن «أديوم» يدعم بروتوكول OTR. ويشير موقع «بدجن» الرسمي إلى أن البرنامج يخضع للتطوير بشكلٍ دائم، كونه ذا مصدرٍ مفتوحٍ، إذ يساهم المستخدمون بشكلٍ دوريٍ في الإبلاغ عن العثرات البرمجية (Bugs) وإصلاحها. كما يمكن للمستخدمين أن يجروا تعديلاتٍ برمجية عليه من أجل أن يتناسب مع احتياجاتهم، إلا أنّ عليهم بالمقابل أن يعلنوا عن التغييرات التي يقومون بإجرائها.

تتوفّر التعليمات الخاصة بتنزيل «بدجن» وOTR باللّغة العربيّة عبر هذا الرابط، كما تتوفّر التعليمات حول تفعيل التشفير قبل البدء بالمحادثة الرابط التالي، كما بإمكانكم الإطلاع على التعليمات الضرورية في مقطع الفيديو التالي:

إضغط هنا للمشاهدة على يوتيوب