
cyberarabs
Digital Security for the Arab World
الأمن الرقمي في العالم العربي
العدد ٧ | سبتمبر/أيلول ٢٠١٣
نظام التشغيل لينكس
الإنترنت عبر الأقمار الصناعية
إزالة الملفات الخبيثة Malware

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

للإتصال بنا:

magazine@cyber-arabs.com

تابعنا على:

مقدمة

سوزان فيشر

أهلاً بكم في العدد السابع من مجلة «سايبر آرابز»
جميعنا لدينا أسرارنا؛ أفكار وملاحظات نود الاحتفاظ بها لأنفسنا وعدم مشاركتها مع الآخرين. في ما يتعلق بالأمن الرقمي، من الأساسي أن نبقي أسرارنا بمأمن حتى لا يتمكن من يحاول التلصص علينا من الوصول إليها بسهولة.
السرية مبدأ أساسي في الأمن. عندما تبقون أمراً ما سرياً أو مخبأً، تجعلون اختراقه مسألة أكثر صعوبة على الآخرين.
لذا، لمَ لا تنشئون ملف ملاحظات سرية على نظام «أندرويد»، لا يدري به أحد غيركم؟ يمكنكم أن تحملوا ملاحظاتكم السرية معكم دون أن تخافوا من أن يتمكن أي أحد ينظر إلى الهاتف من الإطلاع على أفكاركم الأكثر حميمية.
يمكنكم أيضاً أن تخبئوا ملفات على حاسوبكم بشكل يجعلها غير مرئية. سوف نريكم كيف تخبّئون ملفاً داخل ملف آخر. تخيلوا أحداً يبحث عن معلومات معينة على حاسوبكم يجد معلومات بريئة عن آخر زيارة لكم إلى السينما أو وصفة لإعداد طبق شهي، إلا أنه لا فكرة لديه أنّ داخل هذه الملفات التي تبدو بريئة توجد الأسرار المخبأة.
في بعض الأحيان، قد يكون من الضروري أيضاً إخفاء وجوه الناس الذين يظهرون في صور أخذناها. ثمة أدوات عدة تؤدي هذه المهمة، وسنعرفكم على تطبيق «أبسكيوراكام» الذي يمكن أن تستخدموه لإخفاء الوجوه على جهاز «أندرويد» الخاص بكم.
بالمناسبة، منذ آخر عدد من مجلة «سايبر آرابز»، تمكنّا من زيادة عدد متابعينا ٢٣,٠٠٠؛ نفخر الآن بتقديم خدماتنا لأكثر من ٥٢,٠٠٠ متابع عبر العالم العربي. نود أن نستمر في النمو، لذا أخبرونا بما يمكننا أن نفعله لخدمتكم بشكل أفضل للبقاء آمنين على الإنترنت، وذلك من خلال مراسلتنا عبر عنوان البريد الالكتروني magazine*cyber-arabs.com أو صفحتنا على موقع فيس بوك.
هل شاهدتم أفلام الفيديو الرائعة التي أنتجناها؟ تعرفوا إلى عارف وبرهان ومغامراتهما في العالم الرقمي عبر هذا الرابط

مع أفضل التمنيات من فريق «سايبر آرابز»

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

كتابة ملاحظات سرية باستخدام نظام التشغيل «أندرويد»

تُستعمل الهواتف الذكية غالباً لكتابة ملاحظات قصيرة عن أشياء عدة، مثل تدوين اقتباس رائع سمعتموه من أحد ما، أو اسم شخص التقيتموه وشعرتم بالإعجاب نحوه. هناك من لا يرغب في أن يطلع الآخرون على محتوى ملاحظاته، إلا أن الملاحظات على هواتفكم ليست مشفّرة، وإذا تمت مصادرة هاتفكم أو سرقته، يمكن لمن يستحوذ على الهاتف أن يطّلع على محتوى الملاحظات.

لتفادي هذا الأمر، يمكنكم تشفير هاتفكم، وقد كتب موقع «سايبر آرابز» عن هذا الأمر (الرابط). ثمة طريقة أخرى لحماية ملاحظاتكم، وهي استعمال تطبيق بسيط اسمه «نوت سايفر» NoteCipher. مع «نوت سايفر»، يمكنكم إنشاء ملاحظات وحفظها عبر استخدام معيار التشفير AES 256. من لا يمتلك كلمة المرور الخاصة بكم لن يتمكن من النفاذ إلى ملاحظاتكم.

استعمال «نوت سايفر» سهل للغاية. يمكنكم تحميل التطبيق من «غوغل بلاي ستور» (هنا) وفي حال كان الموقع محجوب يمكنكم الحصول عليه من هنا، وعند التشغيل للمرة الأولى، سيُطلب منكم إنشاء كلمة مرور قوية. يمكنكم قراءة هذا المقال وهذا ايضاً على موقع «سايبر آرابز» حول إنشاء كلمات المرور القوية. بعد ذلك، ستصلون إلى الإطلاع سريعاً على ملاحظاتكم. لإنشاء ملف ملاحظات، ببساطة انقروا

على الشاشة وأدخلوا عنواناً ورسالة. يمكنكم حفظ الملاحظة عبر استعمال زر الرجوع على هاتفكم، أو فتح القائمة واختيار «Save Note» (حفظ الملاحظة).

للتأكد من أن لا أحد يمكنه رؤية ملفات ملاحظاتكم، يتوجب عليكم إقفالها. يمكنكم فعل ذلك عبر الضغط على زر القائمة والنقر على «Lock Note» (إقفال الملاحظة).

تأمين عمل «جافا» في المتصفح

ما هو «جافا»؟

جافا هو برنامج وإضافة للمتصفح تعمل على كافة أنظمة التشغيل لكل من أجهزة الحاسوب والهاتف النقال، يساعد هذا البرنامج على تشغيل بعض البرامج الأخرى من ألعاب وخدمات محادثة وإجراء عمليات حسابية، بالإضافة إلى العديد من الوظائف الأخرى.
ويعتبر جافا أحد أكثر الإضافات استخداماً في أجهزة الحاسوب والمتصفحات، لكنه للأسف، يعتبر ضعيفاً أمنياً مما يجعله هدفاً أساسياً للمخترقين.

تنصيب احدث نسخة من الجافا

١- إذا لم يكن لديكم الحاجة لإستخدام جافا، فلا داعي لتنصيبه، ولكن إذا كنتم تعتمدون على جافا، أي إذا كان جافا منصب على نظامكم (ويمكنكم التأكد من خلال البحث عنه في لائحة تحكم ويندوز، أو بإستخدام هذه الصفحة)، فعليكم ابقائه محدثاً للإستفادة من أخر تحديثاته الأمنية.
توجهوا إلى العنوان التالي: https://www.java.com
وتابعوا بالتنزيل.
أو إذا كنتم تريدون تنزيل نسخة لنظام تشغيل معين, فتوجه إلى هذا العنوان: https://www.java.com/en/download/manual.jsp
وفي حال كان الموقع محجوب لديكم يمكنكم تحميل النسخة الأخيرة من هنا.

٢- إذا قمتم بإستخدام الرابط الثاني اختاروا النسخة المناسبة لنظام التشغيل 32-bit أو 64-bit. لكي تعرفوا النظام الذي يعمل به جهازكم، أنقروا بالزر الأيمن من الفأرة على رمز «جهاز الكمبيوتر» ثم انقروا على «خصائص»

٣- بعد انتهاء التحميل أنقروا على Install وانتظروا حتى الانتهاء ثم انقروا على Finish

إيقاف عمل جافا في المتصفح

تعتبر هذه الخطوة الأهم لضمان الحماية من اي استغلال للجافا لاختراق جهازكم أو سرقة معلوماتكم كالحسابات وكلمات المرور.
معظم الاختراقات بالطرق التقليدية تكون عبر إنشاء الصفحات المزورة أو إرسال برامج يتوجب تشغيلها لتتم عملية الاختراق، لكن تكمن خطورة الاختراق عن طريق الجافا أنه لا يحتاج إلى أي تفاعل من المستخدم (الضحية) فيكفي الشخص المخترق أن يضع برنامج الجافا الذي يحتوي على برمجية خبيثة على أحد المواقع وإرسال الرابط للضحية ليعمل تلقائياً دون أي إشعار أو طلب موافقة من المستخدم. لذا نؤكد على أهمية إيقاف عمل الجافا في المتصفح.
لإيقاف الجافا من المتصفح نقوم باتباع الخطوات التالية: توجهوا إلى لوحة التحكم وابحثوا عن JAVA وافتحوه توجهوا إلى تبويب Security ثم أزيلوا التحديد من (Enable Java content in the browser) عليكم إعادة تشغيل المتصفح لكي تعمل الإعدادات الجديدة.

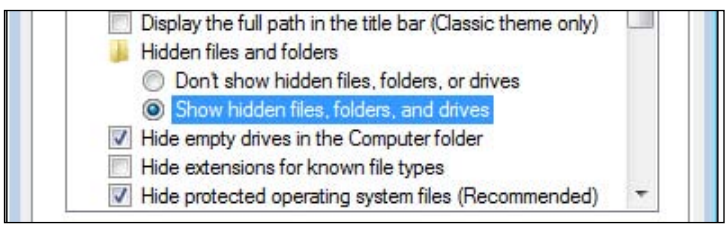
تأمين معلومات سكايب على أجهزة الحاسوب والهاتف النقال

يعتقد كثيرون أن وضع كلمة سر قوية لحسابهم على سكايب يعني أن محادثاتهم في أمان ولا يستطيع أحد الوصول إليها، إلا أن أي شخص لديه إمكانية الوصول إلى الأجهزة المستخدمة في إجراء محادثات سكايب قادر على معرفة محتوى المحادثات كاملة إذا كان يمتلك الأدوات التقنية اللازمة، وبذلك سنعرض محتوى المكالمات الحساسة للكشف في حال وقع الجهاز المستخدم في الأيدي الخاطئة.

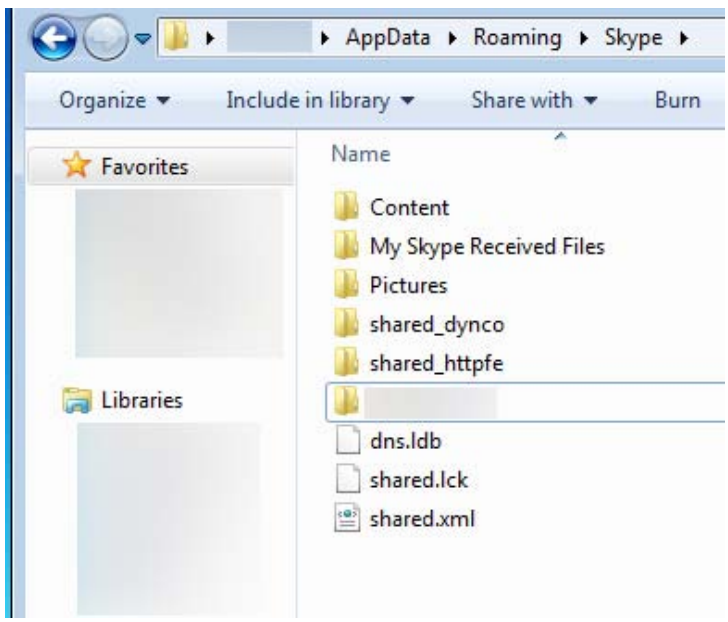
ولكثرة تلقي فريق «سايبر آرابز» تساؤلات من العديد من المستخدمين عن طريقة حذف أسماء حساباتهم التي يعملون عليها من برنامج سكايب على جهاز الحاسوب الخاص بهم، قمنا بشرح طريقة تأمين المحادثات أو حذفها وكيفية إخفاء اسم المستخدم من على أجهزة الحاسوب:

أولاً: نقوم بإغلاق برنامج سكايب نهائياً (النقر بالزر الأيمن على ايقونة البرنامج والنقر على Quit).

ثانياً: نحدد مكان حفظ أسماء الحسابات والمحادثات على جهاز الكومبيوتر عبر الذهاب إلى جهاز الكومبيوتر ثم القرص C ونفتح مجلد المستخدمون أو Users
ندخل إلى مجلد المستخدم الذي نعمل من خلاله عليه وهنا نحتاج إلى إظهار الملفات المخفية وذلك عبر أدوات > خيارات المجلد والبحث (Organize > Folder and search Option) وفي القائمة عرض (View) نفعل خيار إظهار الملفات والمجلدات المخفية (Show hidden files, folders, and drives)



بعد إظهار الملفات والمجلدات المخفية نقوم بالذهاب إلى مجلد AppData > Roaming > Skype
الطريقة الثانية والأسرع للوصول إلى المكان نفسه بسهولة، هي عبر نسخ هذه العبارة: %appdata%\skype
ووضعها في مكان البحث ضمن قائمة «إبدأ» Start > Search
سنجد هنا مجلداً يحمل أسماء الحسابات التي نستخدمها على جهازنا وكل مجلد منها يحتوي على قاعدة بيانات فيها محادثاتنا مع أصدقائنا ويمكن للخبراء فتح قاعدة البيانات بسهولة ورؤية محتواها دون الحاجة لكلمة السر الخاصة بهذه الحسابات.

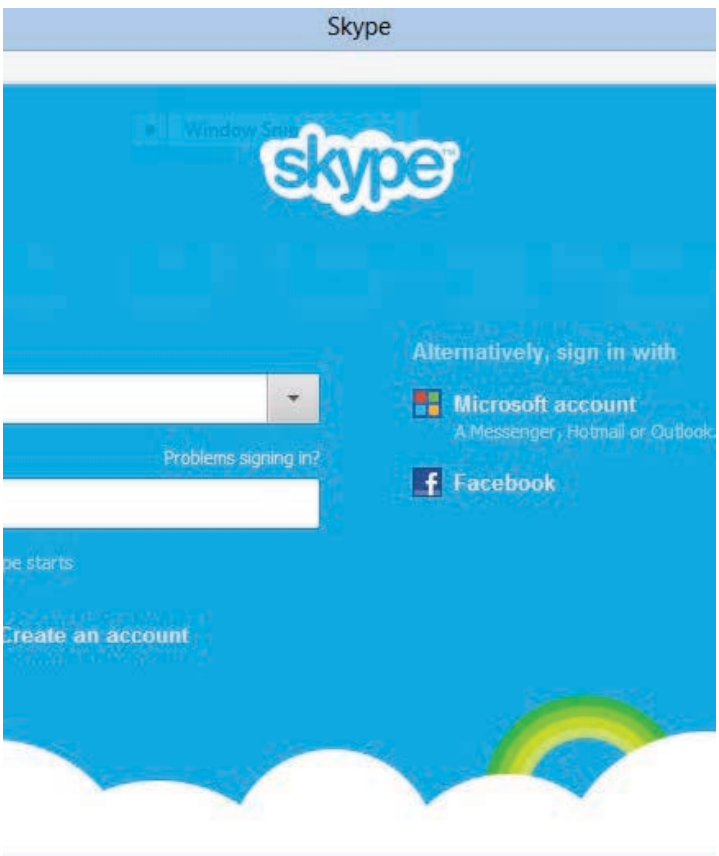


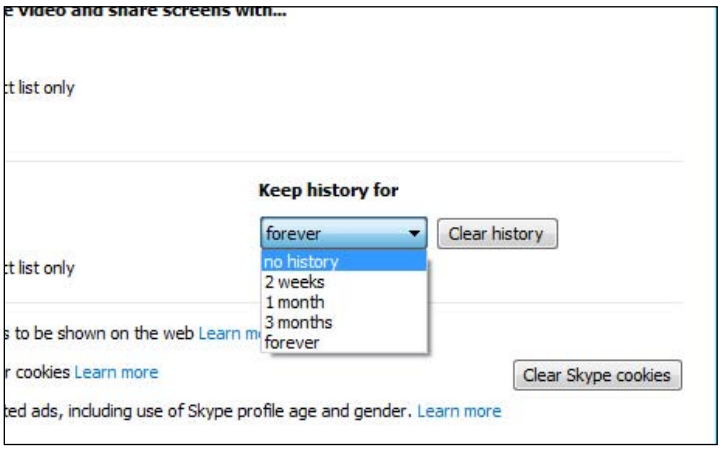
أجهزة الهاتف الجوال الحديثة تحتوي أيضاً على قاعدة البيانات نفسها وبالتالي الخطر ذاته يهددنا، في حال كنا نستخدمها

أثناء التنقّل ووقوعها بيد جهات غير مرغوبة.
يمكن أيضاً التخلص من سجل المحادثات عبر تشغيل البرنامج التالي الذي قمنا بكتابته لكم لتسهيل مهمة حذف سجل المحادثات واسم المستخدم، يقوم هذا البرنامج أولاً بإغلاق برنامج السكايب ثم حذف كل ملفات الحسابات الموجودة على الجهاز كسجل المحادثات واسم المستخدم.
وفي حال لم يتم إغلاق سكايب عند تشغيل البرنامج قوموا بإغلاقه يدوياً، وينصح فريق «سايبر آرابز» بعد تشغيل الملف بالتأكد من حذف السجل عبر الذهاب إلى مسار ملفات البرنامج الذي قمنا بشرح كيفية الوصول إليه أعلاه.

ثانياً : سنقوم الآن بتوضيح الخيارات المناسبة لتأمين حساباتنا على أجهزة الحاسوب التي نستخدمها.

١- لا تقوموا بتسجيل الدخول من أجهزة لا تملكونها، كالأجهزة في مقاهي الإنترنت أو أجهزة بعض الأصدقاء، لأنكم لا تستطيعون التأكد من أن محادثاتكم لن يراها أحد





٢- ينصح بتعطيل خيار الاحتفاظ بسجل المحادثات في سكايب عبر الذهاب إلى قائمة أدوات › إعدادات› الخصوصية› احتفظ بسجل المحادثات: اختيار عدم تخزين المحادثات عبر النقر على التالي:
Tools‹ Options › Privacy › Keep history for: no history

٣- يمكنكم حذف الملفات الموجودة في مجلد Skype وذلك بعد أن تقوموا بإغلاق البرنامج بشكل نهائي لكن هذا سيؤدي إلى إزالة كل محادثاتكم بشكل نهائي من أجهزتكم والتي ربما تحتوي على معلومات تهمكم كثيراً لذا عليكم أن تقوموا بنقل هذه المعلومات إلى مكان آمن أولاً ثم حذف هذه الملفات، وبعد حذف الملفات سيختفي من برنامج سكايب على جهازكم أسماء المستخدمين الذين قد سجلوا دخولهم سابقاً عبره؛ قد تكون هذه الأسماء هدفاً لمن يسعى إلى التجسس عليكم

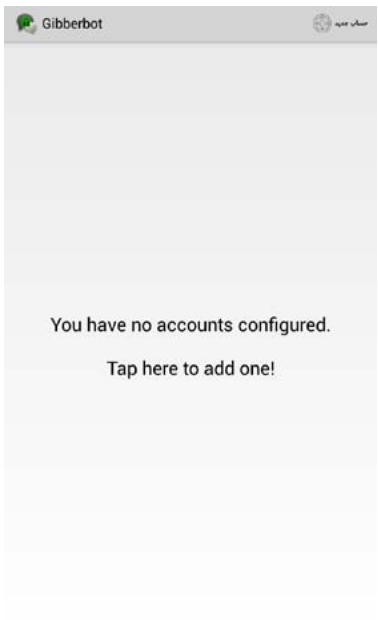
٤- يمكنكم الاحتفاظ بنسخة احتياطية عن هذه الملفات في مكان آمن ومشفر قبل حذفها لاستعادتها في وقت لاحق، وذلك عبر إعادة النسخة الاحتياطية إلى المكان نفسه وبهذا تستعيدون سجل محادثاتكم وقت الضرورة.

٥- في ما يتعلق بأجهزة الهاتف النقال، فإن أسهل وسيلة لتأمين محادثاتكم هو إزالة التطبيق نهائياً وإعادة تنصيبه عندما تكونون في أمان.

ملاحظة هامة: بعد حذف هذه الملفات لن تفقدوا أي من الأسماء لديكم وسيعيد برنامج سكايب تحميل قاعدة البيانات من جديد لكنكم ستفقدون محتوى المحادثات الأخيرة فقط .

«جيبربوت» + «غوغل» = دردشة آمنة

التراسل الفوري، أو كما هو معروف أكثر تحت تسمية الدردشة (Chat)، هو وسيلة تواصل عبر الهاتف المحمول تحظى بشعبية كبيرة، إلا أن معظم تطبيقات الدردشة المتوفرة غير آمنة ويمكن خرقها بسهولة. تتضمن هذه اللائحة تطبيقات معروفة وتستعمل على نطاق واسع، مثل «سكايب» و«واتس آب» و«فايبر». لحسن الحظ، ثمة طرق لتشفير الدردشة التي تجرونها عبر معيار التشفير AES 256. واحدة من أسهل الطرق لفعل ذلك هي الجمع بين تطبيق «جيبربوت أندرويد» السهل الاستعمال وحساب «غوغل». يمكن تحميل «جيبربوت» Gibberbot من «غوغل بلاي ستور» (هنا) في حال كان الموقع محجوب يمكنكم الحصول على التطبيق من هنا او من هنا، وإذا كنتم تستخدمون نظام التشغيل «اندرويد» فعلى الأرجح أنكم تمتلكون حساب «غوغل».



بعد تفعيل «جيبربوت» لأول مرة، سيُطلب منكم تأكيد صحة التفاصيل المتعلقة بحساب «غوغل» الخاص بكم. في أكثر الحالات، يقوم «جيبربوت» بشكل تلقائي بإدراج اسم المستخدم وكلمة المرور المعروفين من قبل «أندرويد». في حال أردتم استعمال حساب مختلف، إحرصوا على تغييره عند هذه النقطة. بعد تسجيل الدخول، ستصلون إلى شاشة فارغة تظهر عليها الكلمات التالية: "No conversation tap to start one" (لا محادثة، أنقر هنا لبدء المحادثة)، وسيقودكم ذلك إلى استطلاع أسماء أصدقائكم الذين يمتلكون بدورهم حسابات «غوغل». تنبّهوا إلى أنه لا يمكنكم إجراء محادثات آمنة إلا مع الأصدقاء الذين يستعملون «جيبربوت»! بعد اختيار الصديق، ستصلون إلى واجهة دردشة بسيطة في الشكل وسهلة الاستعمال.

إذا لم يتم تشفير محادثتكم بشكل تلقائي، سيظهر لكم تحذير باللون الأحمر، كما سترون رمز القفل مفتوحاً. النقر على رمز القفل سيدفع «جيبربوت» إلى إعادة تشفير اتصالكم. إذا لم تنجح هذه الخطوة، فمعنى ذلك أن ثمة مشكلة في اتصالكم بالإنترنت، أو أنّ صديقكم لا يستعمل «جيبربوت».

يعمل «جيبربوت» أيضاً مع تطبيق «أوربوت»، وهو تطبيق شبكة «تور» الخاص بنظام التشغيل «أندرويد». ولإضافة المزيد من الأمان إلى محادثتكم، يمكن تشغيل «أوربوت» قبل فتح «جيبربوت». إذا تمت تهيئة «جيبربوت» بشكل صحيح، سيتم تشغيله من خلال شبكة «تور»، فيصبح من المستحيل اختراقه من قبل أحد.

إخفاء الملفات في الملفات

في بعض الأوقات قد لا ترغبون في أن يطلع شخص ما على ملفاتكم، مثلاً عندما تشاركون مستندات سرية مع زملاء أو أصدقاء لكم. كما شرحنا في مقالات سابقة على موقع «سايبر آرابز»، من الأفضل في هذه الحالات تشفير الملفات، عبر استعمال برامج مثل «ترو كريبت» TrueCrypt أو «أي إي إس كريبت» AES-Crypt، مما يمكّنكم من جعل ملف واحد أو أكثر خارج متناول أطراف ثالثة لا تمتلك كلمة المرور.

إلا أن التشفير وحده لا يحل المشكلة، فالملف المشفّر غالباً ما يكون مثيراً للشكوك وقد يجذب انتباه أشخاص غير مرغوبين. في بلدان مثل سوريا، على سبيل المثال، أُجبر أشخاص على تسليم كلمات المرور لفك تشفير ملفات أو مجلدات بعد أن وجدت قوات الأمن أن لديهم ما يخفونه.

لمنع مثل هذا الأمر من الحدوث، يمكنكم إخفاء الملفات داخل ملف آخر، مثلاً صورة من نوع JPEG أو فيديو. لشخص غريب، سيبدو ملفكم مثل أي ملف آخر، ولن يعلم أنكم قد أخفيتم معلومات سرية داخله. ولكن بالطبع، يجب أن يكون حجم الملف المخفي منطقياً متوافقاً مع حجم الملف الظاهر. مثلاً، إخفاء ملف حجمه ثلاثة ميغابايت داخل ملف نصي (مثل وورد) قد يثير الشكوك. ملفات الفيديو ممتازة لإخفاء ملفات أخرى.

«سرّنا» Our Secret

للتمكن من إخفاء ملفات داخل ملفات أخرى، يمكنكم استعمال برنامج مجاني اسمه Our Secret (سرنا)، يمكن تحميله هنا. واجهة الاستخدام بسيطة وسهلة الاستخدام. لإخفاء ملف ما، أنقروا على الزر بجانب عبارة «Select Carrier File» (اختاروا الملف الذي سيحمل الملفات الأخرى) ثم عينوا الملف المطلوب، على سبيل المثال، ملف فيديو. بعد ذلك، أنقروا على زر «add» (الإضافة) لاختيار الملفات التي تودون إضافتها. أيضاً، سيتم منحكم القدرة على إخفاء رسالة في هذا الملف. في هذه الحالة، ما عليكم سوى طباعة الرسالة والنقر على OK للموافقة. ستظهر الملفات والرسائل المختارة في لائحة في الأسفل.

كل ما عليكم فعله هو إدخال كلمة مرور (ستتشاركونها مع الشخص الذي سيتلقى الملف) ومن ثم إعادة إدخال هذه الكلمة للتأكد من أنكم لم ترتكبوا أي خطأ. عند النقر على «hide» (إخفاء)، سيطلب منكم موقع حيث سيتم إنشاء الملف (الملف الحامل وداخله الملف المخفي) وسيكون جاهزاً للتوزيع.

فك الملف المخفي هو سهل أيضاً. هذه المرة، ستستعملون القسم الأيمن من واجهة الاستخدام. أنقروا على الزر بجانب عبارة «specify a carrier file» (حددوا الملف الذي سيحمل الملفات الأخرى) ثم اختاروا الملف المطلوب. أدخلوا كلمة المرور ثم انقروا على «unhide» (إظهار). إذا جرى كل شيء على ما يرام، ستجدون الملفات في اللائحة الأسفل. ثم انقروا مرتين على الملفات في اللائحة لتتمكنوا من حفظها في مكان محدد من حاسوبكم.

بينما يستخدم برنامج «Our Secret». كلمات المرور لإخفاء الملفات وإعادة إظهارها، يعتمد البرنامج معياراً متدنياً جداً للتشفير. لذا، ينصح موقع «سايبر آرابز» باستعمال هذا البرنامج بالتزامن مع استعمال أداة جيدة للتشفير. شفّروا ملفاتكم باستعمال «ترو كريبت» أو «أي إي إس كريبت» ثم اخفوها باستخدام «Our Secret».

نظام التشغيل لينكس (Linux)

كثيراً ما يتم سؤالنا في «سايبر آرابز» عن صحة كون نظام التشغيل «لينكس» أكثر أماناً من ويندوز.
«لينكس» (Linux) هو نواة نظام تشغيل مفتوح المصدر تم ابتكاره من قبل «لينوس تورفالدز» كهواية أثناء دراسته في جامعة فنلندية في أوائل التسعينات، ومنذ ذلك الحين، ظهرت عدة «توزيعات» (distributions) من لينكس قامت بجمع هذا النواة مع مكونات وبرامج أخرى لخلق أنظمة تشغيل كاملة، وباتت عبارة «نظام التشغيل لينكس» ترمز إلى أي نظام تشغيل مبني على نواة لينكس. وكما ويندوز ونظام التشغيل ماك، تقوم أنظمة التشغيل لينكس بتوفير البيئة لتشغيل البرامج، والوصول إلى الإنترنت، وإنشاء المستندات، ولكن على عكس الويندوز، هي مجانية، ولديها شعبية قوية عندما يتعلق الموضوع بالأمان.
لذا، السؤال هنا: هل حان الوقت للاستغناء عن ويندوز والانتقال إلى لينكس؟
سنحاول في هذا المقال تقديم فكرة أعمق عن هذا السؤال.

الاستخدام

تتعلق الإجابة عن هذا السؤال بما تحتاجونه بالضبط من جهاز الحاسوب الخاص بكم، فنظاما التشغيل ويندوز ولينكس ليسا متوافقين مع بعضهما، ما يعني أن العديد من البرامج المستخدمة على ويندوز لن تعمل على لينكس، فالبرامج الخاصة مثل «مايكروسوفت أوفيس» ومجموعة برامج «أدوبي» معروفٌ بأنها لا تعمل على لينكس، لكن على الرغم من ذلك، تتوفر العديد من البدائل المجانية لهذه البرامج على لينكس، وإن كنت تعتمد على الإنترنت في عملك، فإن خبرتك لن تختلف كثيراً.
يأتي لينكس بعدة هيئات وأنماط للتصفح. فمثلاً، إن كنتم تعتمدون على استخدام زر «إبدأ» في ويندوز، فعملية الانتقال إلى «لينكس مينت» أو النسخ الحديثة من «أوبنتو» لن تكون صعبة عليكم، ولكن

على الرغم من ذلك، فإن المظهر سيبدو مختلفاً كثيراً عن نظام التشغيل ويندوز، ولكن في كافة الأحوال، عليكم تعلم كيفية التعامل مع بيئات التشغيل وأنظمة التشغيل المختلفة، كما ينطبق الأمر على المستخدمين الذين يريدون الانتقال من نظام التشغيل ويندوز ٧ إلى النسخة الأحدث منه ويندوز ٨.

الأمان

ماذا عن كون لينكس أكثر أماناً؟

تم تصميم لينكس بحيث يتم الحد من إمكانية المستخدم لقيام بأمور خبيثة خطيرة في نظام التشغيل، وذلك يعني أيضاً أنه يصعب على الفيروسات أن تنصب نفسها على نظام التشغيل، أضيفوا إلى ذلك، أن تقريباً كل الفايروسات المكتوبة والتي تستهدف الدول العربية، تم كتابتها لتستهدف نظام التشغيل ويندوز، وهذا يعني أنه في حال قمتم بتحميل ملف يحتوي على فيروس، أو قمتم بفتح سواقة USB، فلا شيء سيحدث لجهازكم. لأنه ببساطة الفيروسات المكتوبة لتستهدف الويندوز لا تعمل على لينكس.

النقطة الإيجابية الأخرى في نظام التشغيل لينكس أنه مفتوح المصدر، وهذا لا يعني فقط أنه مجاني، بل يساهم هذا الأمر في حماية جهاز الحاسوب، وذلك بسبب أن الكود المصدري لنظام التشغيل متاح للجميع مما يعني إمكانية اكتشاف وإصلاح الأخطاء والثغرات الأمنية بسرعة كبيرة. بينما عندما يتعلق الموضوع بويندوز، فإن اكتشاف الأخطاء وإصلاحها يأخذ وقتاً أطول، وبالطبع في حال لم يتم تفعيل التحديثات التلقائية في ويندوز فإن جهاز الحاسوب سيبقى معرضاً لخطر الاختراق.

وتعد قرصنة البرمجيات في عالمنا العربي مشكلة شائعة جداً، حيث عانى العديد من قرّاء موقع «سايبر آرابز» من مشاكل تعود إلى كون نظام التشغيل ويندوز والبرامج المستخدمة مقرصنة، كما أن التحديثات التلقائية لويندوز لديهم لا تعمل بصورة دائمة على النسخ المقرصنة، ووفقاً لبحث أجرته شركة مايكروسوفت بالتعاون مع IDC، فإن ٨٠ بالمئة من البرامج المقرصنة تحتوي على برمجيات خبيثة. أما لينكس، فإنه مجاني ١٠٠ بالمئة، مما يعني أن كل النسخ المتوفرة قانونية.

بالنسبة للمستخدمين الذين يعون خطورة النسخ المقرصنة من الويندوز، قد يبدو من الصواب الانتقال إلى لينكس.

توزيعات عديدة

على عكس نظام التشغيل ويندوز، فإن نظام التشغيل لينكس ليس مملوكاً من قبل شركة معينة، ولهذا السبب، ستجدون العديد من توزيعات لينكس على الإنترنت، وكل توزيعة منها تم تصميمها وبرمجتها لتناسب احتياجاً معيناً للمستخدمين. وتعد أشهر توزيعات اللينكس «أوبنتو» (Ubuntu) وتستطيعون تحميلها من هنا (سيتم تحميلها بصيغة ISO ما يعني الحاجة لوضعها على القرص المدمج (CD) أو على الفلاشة (USB) بإستخدام برنامج مثل unetbootin أو LinuxLive USB Creator).

تم تصميم «أوبنتو» لإتاحته كنظام تشغيل سهل الاستخدام، مع مجموعة من البرمجيات الأساسية، كمتصفح الإنترنت فَيرفوكس (Firefox)، وبرامج النصوص وقراءة الصوتيات والفيديو.

تتميز واجهة المستخدم بتصميمها المثالي، على الرغم من أن مستخدمي الويندوز سيجدون صعوبة في البداية باستخدامها. وإن كنتم غير جاهزين

للانتقال بشكل كامل إلى نظام التشغيل لينكس، بإمكانكم تنصيب «أوبنتو» بجانب ويندوز، (سيتم سؤالكم أثناء عملية تنصيب «أوبنتو» إن كنتم ترغبون بتنصيبه إلى جانب ويندوز أو حذف ويندوز واستخدام أوبنتو فقط)، وعند تشغيل الحاسوب سيتم تخييركم بين ويندوز أو أوبنتو للإقلاع منه.

توجد توزيعة ثانية شائعة الاستخدام من لينكس، هي «لينكس مينت» (Linux Mint)، التي تستطيعون تحميلها من هنا.

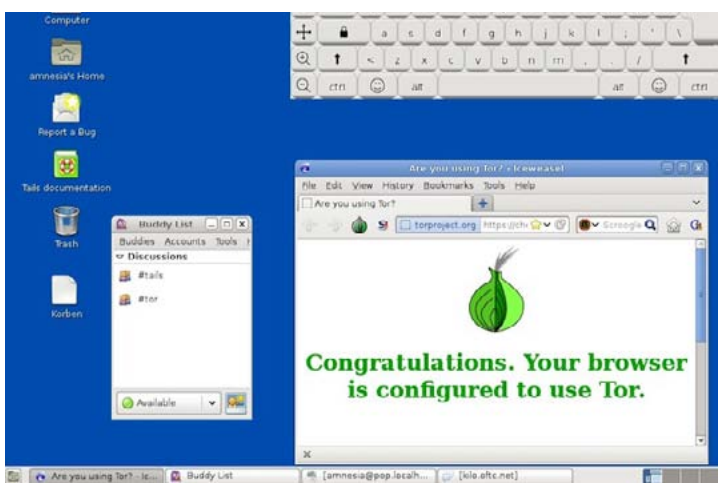
يتميز «لينكس مينت» بذات القدرات التي يتميز بها أوبنتو، ولكنه يأتي مع واجهة مستخدم أقرب إلى الويندوز، تتضمن شريط المهمات، وزر إبدأ، لذا في حال كنتم لا تملكون أي تجربة سابقة مع لينكس، بالإمكان الاعتماد على لينكس مينت كونه الطريق الأسهل للاعتياد على لينكس.

أيضاً تستطيعون تنصيب لينكس مينت إلى جانب ويندوز والاختيار بينهما عند الإقلاع.

ووفقاً للتصميم الذي بُنيَ عليه لينكس مينت، فهو يستهلك القليل من موارد الجهاز عند تخفيض إعدادات المنظر، لذا فيمكن تنصيبه على أجهزة الحاسوب التي يزيد عمرها عن العشر سنوات.

أما فيما يتعلق بتوزيعات اللينكس الأكثر أماناً، فإننا ببساطة ننصح المستخدمين باستعمال توزيعة «تيلز» التي تستطيعون تحميلها من هنا.

على عكس «أوبنتو» و«لينكس مينت»، لا يمكن تنصيب هذه التوزيعة على القرص الصلب (Hard Disk)، فنظام التشغيل



هذا تم تصميمه من قبل الأشخاص ذاتهم الذين قاموا بتطوير برنامج تور (Tor) ويهدف إلى الاستخدام في الحالات التي تتطلب بيئة آمنة في العمل.

ولأنه يقوم بالإقلاع من القرص المدمج أو الفلاشة، يمكن استخدامه في مقاهي الإنترنت، فهو نظام تشغيل محمول وسهل الاستخدام وآمن.

تيلز لينكس لا يترك أي أثر لما تقومون به على الإنترنت، لأنه يقوم بشكل افتراضي بإخضاع حركة مروركم على الإنترنت إلى العبور عبر شبكة تور. ولكن لسوء الحظ، فإن برنامج تور قد يكون بطيئاً أو قد يكون محجوباً مما يتطلب تغيير في الإعدادات لكي يعمل، ولكن من جهة أخرى فإن أحد إيجابيات تيلز، إتاحة الخيار للإقلاع بواجهة مستخدم تشبه إلى حد كبير واجهة نظام التشغيل ويندوز إكس بي (XP)، لذا فلن يجد مستخدمي الويندوز صعوبة كبيرة في استعمال نظام التشغيل تيلز.

بسبب الخطوات الأمنية القصوى التي يطبقها تيلز (وعدم إمكانية تنصيبه على القرص الصلب) فهو ليس خياراً جيداً للاستعمال اليومي، بالطبع يمكنكم استعمال هذا النظام إلى جانب نسخة ويندوز من دون الحاجة إلى تغيير جهاز الحاسوب.

ختاماً

حتى وإن كان من الحكمة الانتقال من ويندوز إلى لينكس إلا أن الانتقال يعتمد على العديد من العوامل المختلفة:

هل تملكون نسخة قانونية من ويندوز؟ هل تستخدمون برامج خاصة؟ هل تحتاجون إلى المزيد من الأمان؟

ليس هناك توصية عامة متاحة. ولكن تبقى النصيحة الأفضل للمستخدمين المهتمين بالموضوع: قوموا بالتجربة!

«أوبنتو» و«مينت» بالإمكان تنصيبهم إلى جانب ويندوز، و «تيلز» لا يحتاج إلى تنصيب، ولكن على الرغم من ذلك فإن تنصيب العديد من توزيعات لينكس سهلة للغاية، فما عليكم سوى إقلاع الجهاز من القرص المدمج أو الفلاشة – ونحن في «سايبر آرابز» ننصحكم بالاستعانة بصديق لديه الخبرة الكافية في تنصيب نظام التشغيل في حال لم يكن لديكم أي خبرة سابقة في تنصيب أنظمة التشغيل، بما في ذلك ويندوز.

بإمكانكم الإطلاع على معلومات أكثر عن لينكس وتاريخه هنا.

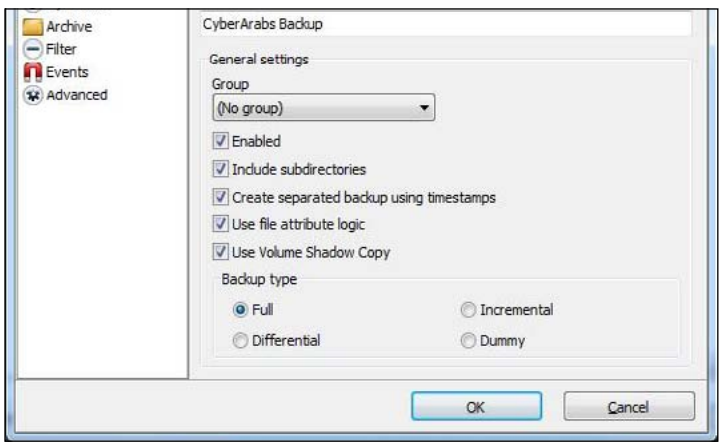
إجراء نسخة إضافية من ملفاتكم باستعمال «كوبيان»

الكثير ممن يمتلكون أجهزة حاسوب قد واجهوا الأمر مرة واحدة على الأقل: خسارة الملفات. تعود خسارة الملفات إلى أسباب عدة، فقد تكونوا قد حفظتموها في موضع خاطئ، أو أن القرص الصلب تعرض للانهيار، أو قد تكونوا قد مسحتم ملفاً ما عن طريق الخطأ. يبقى أن العديد من الناس يتساءلون بعد حادث مماثل: «لماذا لم أقم بإجراء نَسخ احتياطي؟» يتلقى موقع «سايبر آرابز» بشكل مستمر أسئلة من أشخاص يطلبون المساعدة في إعادة الملفات المفقودة. البرامج مثل «ريكوفا» (Recuva) قد تكون مفيدة في بعض الأحيان لبلوغ هذا المسعى، ولكن الاستثمار في حل جيد لمشكلة النسخ الاحتياطي يبقى أفضل بكثير. ثمة تطبيق رائع لإجراء النسخ الاحتياطي، وهو «كوبيان» (Cobian).

«كوبيان» برنامج مجاني يعمل مع «مايكروسوفت ويندوز»، يمكن استعماله لجدولة عملية النسخ الاحتياطي للملفات والمجلدات وتنفيذها، ويمكن وضع النسخة في موضع جديد (مجلد أو قرص) على حاسوبكم أو على حاسوب آخر في الشبكة. يمكنكم تحميل «كوبيان» هنا. يتمتع التطبيق بعدة خيارات يمكنكم تغييرها، ولكن الالتزام بالوظائف الأساسية يمنحكم خياراً رائعاً لتنفيذ النسخ بشكل تلقائي. سنعرض في هذا المقال كيف يمكنكم أن تُعدوا البرنامج.

عملية التنصيب تتطلب إجراءات إعداد بسيطة، مثل الموافقة على شروط الاستخدام وإنشاء الاختصارات، (اضافة) ولكنها في الوقت نفسه تتضمن خطوات أكثر تقدماً، وهي تتطلب بعض النصائح، يمكن الإطلاع عليها من خلال وضع مؤشر الفأرة فوق لائحة النصائح، أو في قائمة المساعدة. ننصح بإبقاء جميع الخيارات على صورتها القياسية .(Standard) عند تنصيب البرنامج، سيتم وضعه بجانب الساعة على الجهة اليمنى. افتحوه لإكمال عملية الإعداد.

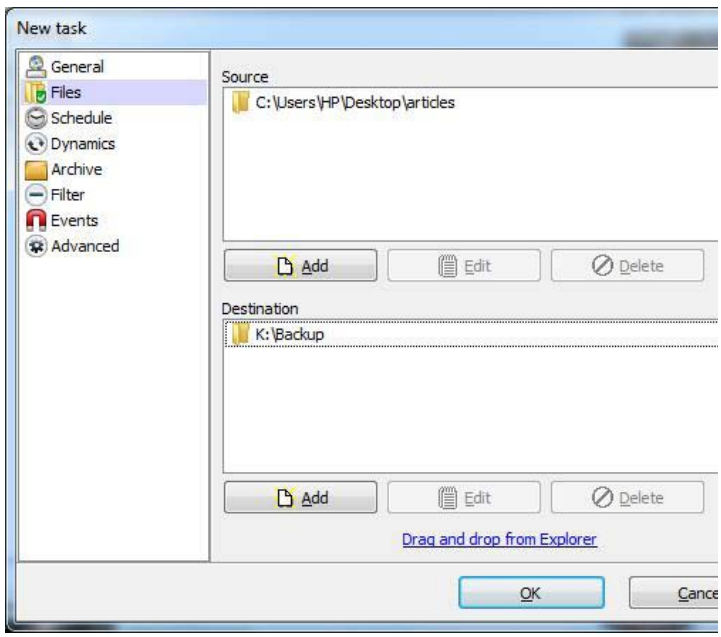
يقدم «كوبيان» العديد من الميزات المتقدمة، إلا أن مطوري البرنامج قاموا بجمعها في واجهة بسيطة وسهلة الاستخدام. لإنشاء مهمة جديدة للنسخ الاحتياطي، أنقروا على الرمز «+» الكبير في أعلى نافذة التطبيق، أو في القائمة (Task > New Task) سيأخذكم ذلك إلى نافذة جديدة حيث يمكنكم أن تقوموا بإعداد مهمة النسخ. ثمة ثمانية تصنيفات على القائمة اليسرى، ويمكن انتقاء الخيارات في النافذة الأساسية إلى جهة اليمين. المستخدمون العاديون سيقومون على الأرجح بانتقاء الخيارات تحت «عام» «General» (اسم المهمة؟)، «ملفات» «files» (أي ملفات، ونقلها إلى أين؟) و«الجدول» «schedule» (متى؟).



تحت خانة «General» يمكنكم تحديد اسم المهمة واختيار نوع النسخ الاحتياطي. اختاروا «Full» (كامل) إن أردتم أن تنسخوا كل ملف موجود، في كل مرة. اختاروا «Incremental» (متزايد) إذا أردتم إجراء نسخ احتياطي عن الملفات الأحدث أولاً. اختاروا «Differential» (تفاضلي) إذا كنتم تودّون البرنامج أن يقوم بنسخ ما تغيّر عن النُسخ السابقة فقط. لن نستعمل خيار «Dummy». ننصح باختيار إما «Full» أو «Differential».

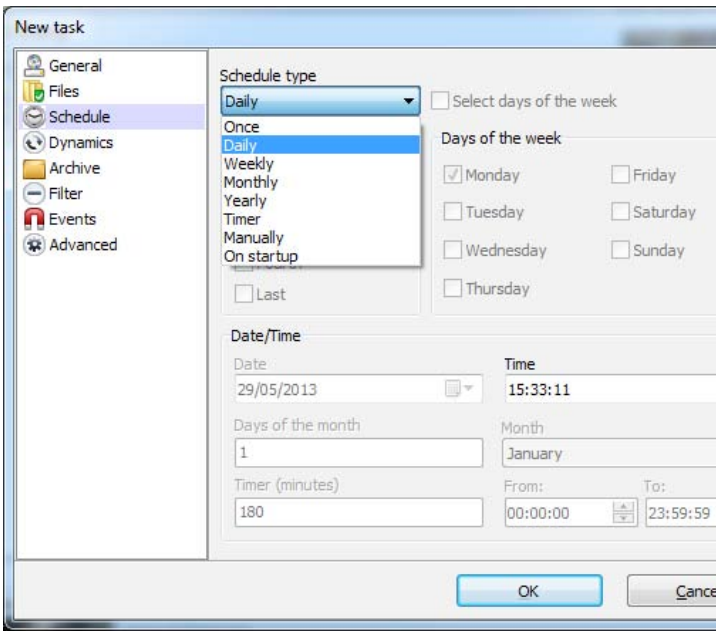
يتم اختيار المصدر والوجهة تحت Files. عند النقر على زر Add تحت Source يمكنكم أن تختاروا الملفات والمجلدات التي تحتاجون إلى إخضاعها للنسخ الاحتياطي بشكل

دوري. تحت Destination، يمكنكم أن تختاروا الوجهة التي تودون حفظ النسخة الاحتياطية من الملفات فيها. من الممكن أيضاً أن تقوموا بوضع النسخ الاحتياطية في مكانين مختلفين. على سبيل المثال، يمكن حفظ نسخة محلية على القرص الصلب، ونسخة أخرى على الشبكة أو على قرص خارجي. بالطبع، يمكنكم أن تختاروا أيضاً القيام بنسخ احتياطي عن مجلد «تروكربت» أو داخله.

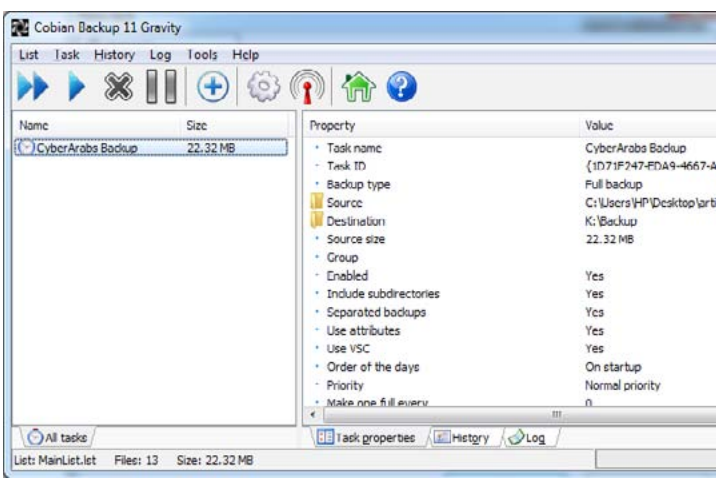


استعمال جدولة المهام (Schedule) أمر اختياري، ولكنه بالطبع أساسي للحصول على عملية نسخ احتياطي جيدة. وضع النَسخ الاحتياطي في جدول تلقائي سيضمن أنكم لن تحتاجوا إلى التفكير بالأمر. في الجدول، يمكنكم تحديد مجموعة من الخيارات؛ وضع تواريخ محددة للنسخ؛ ضبط النسخ بشكل أسبوعي؛ أو اختيار أن يتم النسخ عند إقلاع الحاسوب. الخيار الذي نوصي به هو النسخ عند الإقلاع، إلا أنه ليس دائماً عملياً لأنه يبطئ نظام التشغيل.

ننصحكم أن تضعوا دائماً جدولاً للنسخ، لكي تتم العملية بشكل تلقائي، إلا أنه يمكنكم أن تفعّلوا عملية النسخ الاحتياطي يدوياً في أي وقت. أنقروا على زر التشغيل (رمز السهم الأزرق المنفرد المتجه إلى اليمين) من أجل تشغيل وظائف محددة، إما وظيفة واحدة أو عدة وظائف. أنقروا على زر السهم المزدوج إلى أقصى اليسار لتشغيل جميع



الوظائف (إذا كان هناك أكثر من واحدة). عند التأكيد على الاختيارات، يمكن ضبط الحاسوب ليتم إطفائه بعد أن تنتهي جميع الوظائف. بالطبع، يجب أن تستعملوا هذا الخيار فقط إذا لم يكن لديكم أي مستندات غير محفوظة مفتوحة.



بعد إعداد عملية النسخ، يمكنكم إغلاق البرنامج. يقوم «كوبيان» بالعمل في الخلفية، يهتم بكل شيء بشكل تلقائي. إذا خسرتم بياناتكم، توجهوا ببساطة إلى المجلد الهدف، وانسخوا الملفات الضائعة ثم ألصقوها في أماكنها الأصلية.

تطبيق «أوبسكيوراكام» لإخفاء الوجوه في نظام «أندرويد»

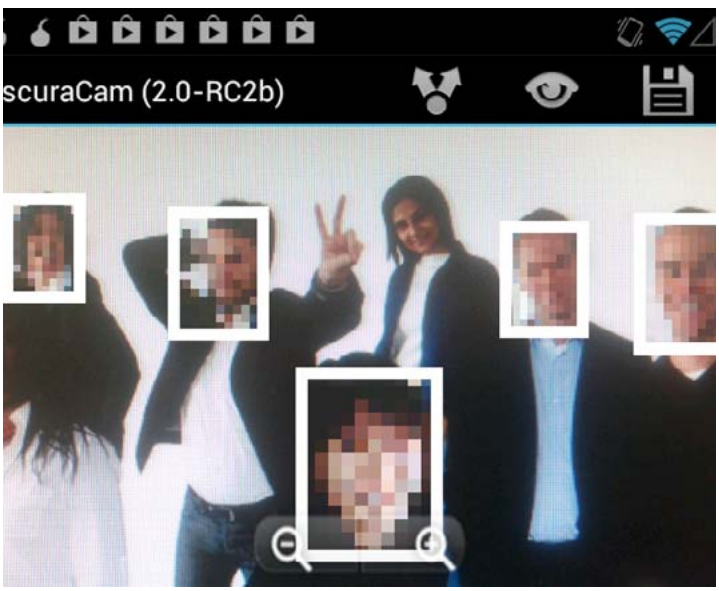
يقوم العديد من قراء «سايبر آرابز» بأخذ صور فوتوغرافية وتسجيل مقاطع فيديو، في ظروف غالباً ما تكون صعبة، مثل المظاهرات. مع أنّ الصور والفيديو قد تكون مفيدة في نشر معلومات عن قضيتكم أو الدفاع عن وجهة نظر معينة، إلا أنها قد تشكل خطراً على من يظهر فيها. على سبيل المثال، علمنا بحالات عديدة أجبر فيها أشخاص على تسليم آلات التصوير إلى السلطات. نتيجة لذلك، تم توقيف الأشخاص الذين ظهروا في الصور.

لحسن الحظ، ثمة حل لهذه المشكلة، وهو تطبيق «أوبسكيوراكام» Obscuracam الذي يعمل في نظام التشغيل «أندرويد». يضيف «أوبسكيوراكام» بعض الوظائف إلى كاميرا الهاتف، تتيح تعتيم وجوه الأشخاص الذين يظهرون في الصور أو مقاطع الفيديو. يعمل التطبيق بشكل بسيط للغاية، ويمكن تحميله مجاناً من «غوغل بلاي ستور» هنا. ومن 1mobile هنا. بعد تشغيل التطبيق على هاتفكم، سترون شاشة مع ثلاثة خيارات: «صورة جديدة» New picture ؛ «تعتيم صورة» Obscure photo؛ و«تعتيم فيديو» Obscure video.

إذا نقرتم على الخيار الأول، ستصلون إلى واجهة الكاميرا التي اعتدتم عليها، ولكن بعد إنشاء الصورة، سيقوم التطبيق بوضع موزاييك على الوجوه بشكل تلقائي، بشكل يجعلها غير معروفة. في بعض الأحيان، لا يقوم التطبيق بالتعرف على الوجوه بشكل صحيح. في هذه الحالة، يمكنكم النقر على الوجه وستتم تغشيته. بعد إخفاء كل الوجوه، أنقروا على «save» أو «share». قبل ذلك، سيُطرح عليكم السؤال حول عما إذا كنتم تريدون حذف الصورة الأساسية. ننصحكم بتطبيق هذه الخطوة، لأن الأشخاص الظاهرين في الصورة سيتعرضون للخطر إذا انكشفت هويتهم.

إذا عدتم إلى قائمة «أوبسكيوراكام»، يسمح لكم خيار «obscure photo» (تعتيم الصورة) بإخفاء الوجوه في صورة أنشئت خارج التطبيق. توجهوا إلى الصورة ودعوا «أوبسكيوراكام» يتعرف على الوجوه ومن ثم إحفظوا الصورة من جديد. الخيار الثالث، «obscure video» سيسمح لكم فعل الأمر نفسه مع مقاطع فيديو قمتم بإنشائها مسبقاً.

بعد اختيار الفيديو، ستُسألون إذا كنتم تريدون أن يتم التعرف على الوجوه بشكل تلقائي، وهي وظيفة يمكنكم أن تفعّلوها عبر النقر على «Yes». وقد تأخذ بعض الوقت. يمكنكم أيضاً أن تختاروا الوجوه في الفيديو يدوياً. في الفيديو، كما في الصور، ما عليكم سوى النقر على الوجه لإخفائه، ويقوم التطبيق بتتبع الوجه خلال تتابع المشاهد. ولكن يجب أن تتنبّهوا إلى أنّ وظيفة الإخفاء الخاصة بالفيديو لا زالت قيد التطوير، مما يعني أنها تعمل بدقة أقل مما تعمل في الصور، لذا تحقّقوا من مقاطع الفيديو قبل نشرها.



مخاطر استعمال الإنترنت في بلدان الخليج

حتى الآن، تفادت دول الخليج العربي الاضطراب الذي نتج عن الربيع العربي، وطال تونس ومصر واليمن وسوريا. وحدها البحرين شهدت مظاهرات واسعة، تسبّبت في تشديد الرقابة على الإنترنت واعتقال المدوّنين، والصحافيين ومستخدمي وسائل الإعلام الاجتماعي. لسوء الحظ، يبدو أن هذه الخطوات تعكس نمطاً من تزايد القمع والرقابة على الأصوات الرقمية في بلدان الخليج.

في المملكة العربية السعودية، تم احتجاز العديد من الأشخاص بسبب نشر ما اعتبر أنه تصريحات متمردة في حساباتهم على «تويتر» و «فيس بوك»، كما تم تمرير تشريع لفرض الرقابة على الاتصالات عبر تطبيقات مثل «فايبر» و «سكايب». في البلد الجار الإمارات العربية المتحدة، تتجه الحكومة نحو اتخاذ إجراءات جذرية مماثلة، وينص قانون الجرائم الإلكترونية الجديد على عقوبة السجن ١٥ عاماً في حال استعمال الإنترنت لنشر رسائل تهين قادة الإمارات أو «تهدد أمن الدولة». أول شخص تمت إدانته بحسب هذا القانون هو عبد اللّه الحديدي، وتم الحكم عليه بالسجن عشر سنوات بعد نشر تغريدة عن والده ناشط حقوق الإنسان الذي يقبع في السجن.

وبموجب تشريع مماثل مثير للجدل، حكم على حامد الخالدي البالغ من العمر ٢٧ عاماً، وهو من الكويت، بالسجن لمدة سنتين، وقد وجد الخالدي مذنباً لكتابته تعليقات على «تويتر» اعتبرت مهينة للأمير الشيخ صباح أحمد الصباح. وفي قطر أيضاً، حكم على محمد العجمي البالغ من العمر ٣٧ عاماً بالسجن مدى الحياة، بسبب قصيدة ينتقد فيها عجمي النظام القطري، نشرها صديقه على الإنترنت.

في عُمان، وهو بلد ليبرالي إلى حد ما، أدى استعمال وسائل الإعلام الرقمية إلى أحكام بالسجن. بعد مظاهرات تبعتها اعتقالات في العام ٢٠١٢، أصدر مكتب الإدعاء العام في عُمان تصريحات تتضمّن تهديداً باتخاذ إجراءات قانونية ضد أي شخص ينشر ما وصفته التصريحات بأنها كتابات مسيئة أو تحرض على الاحتجاجات عبر «فيس بوك» أو «تويتر» أو المدوّنات الشخصية. ومع أن السلطان قابوس بن سعيد أصدر عفواً سلطانياً عن أي شخص أدين بارتكاب «جرائم تكنولجيا المعلومات»، إلا أنه من الواضح أن حرية التعبير لا زال أمامها طريق طويل لتقطعه.

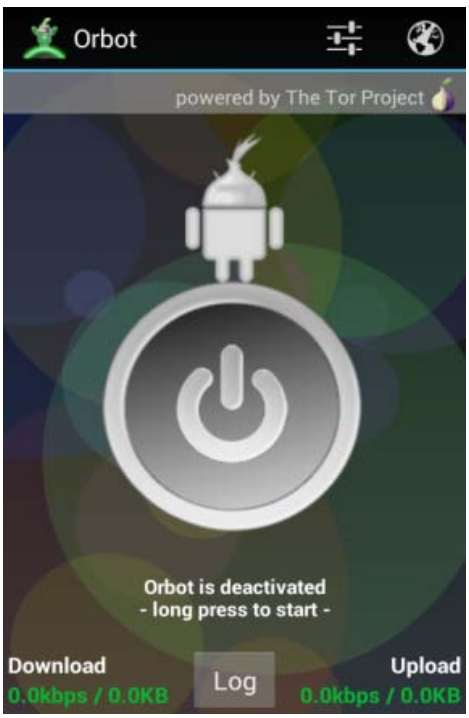
يساعد فريق «سايبر آرابز» الناس على حماية أصواتهم على الإنترنت. وبسبب وجود أجهزة أمن متطورة في بلدان الخليج، ننصح الناس في هذه البلدان باتخاذ أقصى حذرهم خلال التعبير عن آرائهم النقدية وأن يتنبّهوا دائماً إلى النتائج التي يمكن أن تحدث.

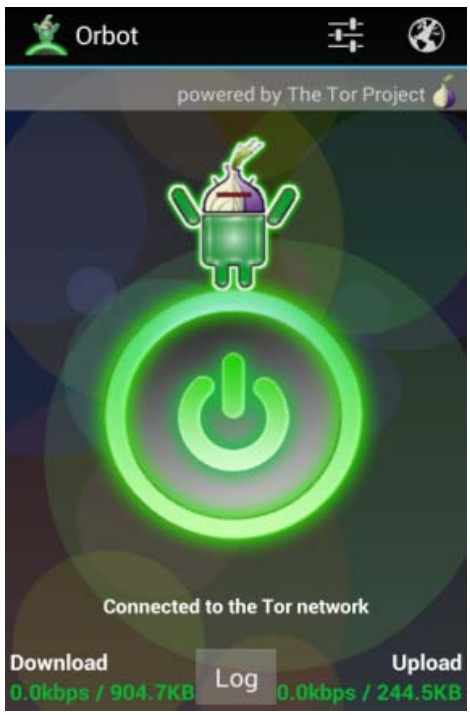
يمكنكم إخفاء موقعكم الجغرافي وتخطي الرقابة والتنصت من قبل السلطات، عبر استخدام الشبكات الافتراضية الخاصة VPN أو «تور»، وإذا أمكن، حاولوا أن تعبرّوا عن انتقاداتكم من دون الكشف عن هويتكم. اقرؤوا كتيّب «سايبر آرابز» حول استخدام «فيس بوك» بشكل آمن.

«أوربوت» و«أورويب» لاستعمال شبكة «تور» في نظام «أندرويد»

تطبيق «تور» هو واحد من أكثر الوسائل شعبية وأمناً التي تستعمل لتخطي حجب المواقع على الإنترنت، وحماية اتصالاتكم الرقمية من المراقبة. التكنولوجيا المستعملة في «تور» تقوم بتشفير بياناتكم عدة مرات عند ارسالها من خلال سلسلة من أجهزة الحاسوب الوسيطة والمجهولة الهوية، الموزعة حول العالم. نشرنا على موقع «سايبر آرابز» في السابق مقالين حول استعمال تطبيق «تور» مع جهاز الحاسوب الشخصي. ستجدونهما هنا وهنا. إلا أن قلة من المستخدمين يعرفون أن ثمة نسخة مفيدة جداً من «تور» تستخدم مع هواتف «أندرويد»، وهي «أوربوت» (Orbot)، التطبيق المطور من قبل «مشروع غارديان».

يسمح تطبيق «أوربوت» لمستخدمي الهواتف المحمولة بالدخول إلى شبكة الإنترنت من دون التعرض للمراقبة أو الحجب من قبل مزود خدمة الإنترنت للهاتف المحمول، وهو سهل الاستخدام، ويمكن تحميله من «غوغل بلاي ستور» مجاناً هنا أو من هنا في حال كان الموقع محجوباً. عند استعمال هاتف خاضع لل «روتنغ»، (Rooting)، وهي عملية تتيح للمستخدمين التحكم بنظام التشغيل، سيقوم «أوربوت» بتمرير نشاط الإنترنت من خلال قناة «تور». في الهواتف العادية، غير الخاضعة لل «روتنغ»، ستضطرون إلى استعمال متصفح «أورويب» Orweb، وهو آمن ومجاني، ويمكن تحميله من «غوغل بلاي ستور» هنا أو من هنا في حال كان الموقع محجوباً.

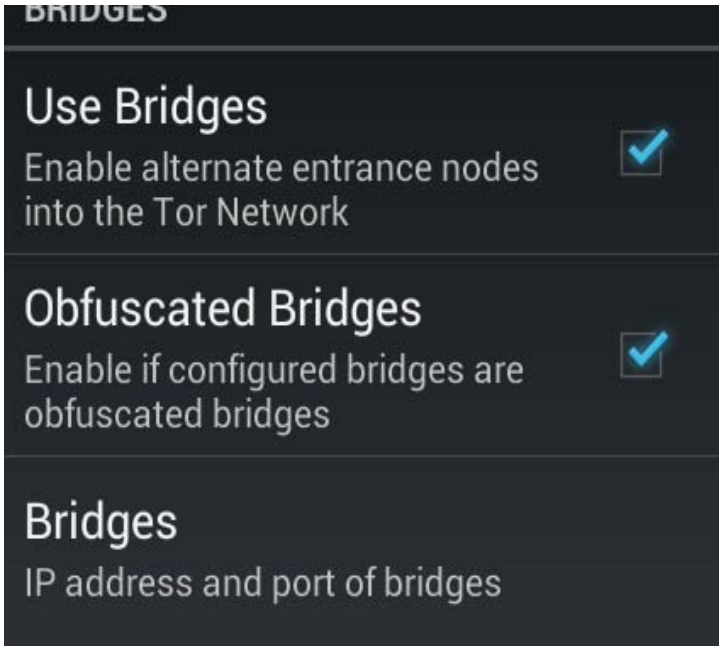




بعد تنصيب «أوربوت»، سيكون استعماله سهلاً للغاية. ستجدون زراً كبيراً على الشاشة، وإذا تم إعداد كل شيء بشكل صحيح، كل ما عليكم فعله هو النقر على الزر لبضع ثوانٍ. سيتغير لون الزر من الرمادي (إذا لم يكن الاتصال مفعّلاً) إلى الأصفر (خلال القيام بالاتصال) إلى الأخضر (متصل). عندما تكونون متصلين بـ «أوربوت»، وفي حال استعمال هاتف خاضع لـ «روتنغ» أو يكون متصفح «أورويب» منصّب، يمكنكم النقر على رمز الكرة في الزاوية اليمنى العليا لتفعيل المتصفح، الذي سيوضح لكم إذا ما كان الاتصال يعمل بشكل جيد.

عند تفعيل الاتصال، سيعمل «أوربوت» في الخلفية وسيقوم متصفحكم العادي (في الهواتف الخاضعة لـ «روتنغ») أومتصفح «أورويب» (في الهواتف غير الخاضعة لـ «روتنغ») باستعمال اتصال «تور» للدخول إلى الإنترنت. في بعض الحالات، قد يعطي «أوربوت» علامة خطأ، يشير فيها إلى عدم القدرة على الاتصال بشبكة «تور». إذا حصل ذلك، فإنه يعني أن مزود خدمة الإنترنت يحجب الاتصال من خلال «تور». لحسن الحظ، يمكن تخطي هذا الأمر بسهولة عبر إعداد ما يسمى بالجسر.

الجسر هو جهاز حاسوب مجهول الهوية، تتصلون من خلاله بشبكة «تور». ثمة نوعان من الجسور، الجسر العادي والجسر المموه. عليكم اختبار هذين النوعين لمعرفة أي واحد منهما يعمل بشكل أفضل، ولكن الجسر المموه يعمل تقريباً بشكل شبه دائم. يقوم هذا الجسر بتحويل النشاط عبر



«تور» إلى نشاط يبدو عادياً، (نشاط يشابه التصفح العادي للانترنت) مما يجعل من الصعب اكتشاف أنكم تستعملون «تور». يمكنكم الحصول على جسر عادي هنا وجسر مموه هنا. بشكل عام، يبدو عنوان بروتوكول الإنترنت الخاص بالجسر كالتالي: 50.112.85.82:52176

إذا نقرتم على زر الإعدادات، ستصلون إلى قائمة حيث يمكنكم أن تعدّوا الجسر. كما سترون، ثمة ثلاثة أبواب. عليكم اختيار الباب الأول «Use Bridges» (استعمال الجسور) للحرص على أن «أوربوت» يستعمل الجسر الذي اعددتموه، والباب الثاني «Obfuscated Bridges» (الجسور المموهة) إذا كنتم تستعملون جسراً مموهاً. يمكنكم إدخال عنوان بروتوكول الإنترنت (الآي بي IP) بعد النقر على «Bridges» (جسور).

بعد الإعداد، عليكم إغلاق اتصال «أوربوت» وإعادة تفعيله لكي تتمكنوا من تسجيل الدخول إلى شبكة «تور» من خلال هذا الجسر. إحرصوا على التحقق مما إذا كنتم لا تزالون تتصفحون الإنترنت بشكل مجهول وذلك عبر زيارة موقع التالي:
https://check.torproject.org

استعادة الملفات المحذوفة باستخدام برنامج Recuva

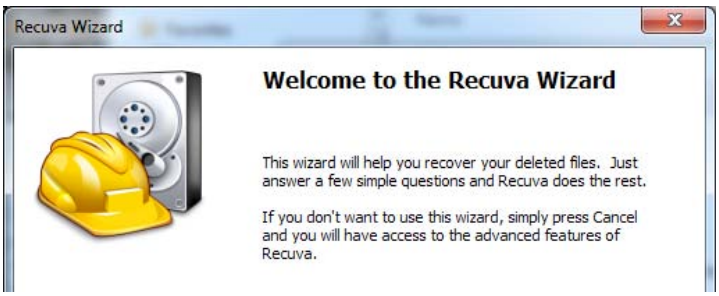
لا بدّ أن يمرّ كل شخص منّا بهذه الحادثة: حذف ملف لا يجدر بنا حذفه.
في معظم الحالات، يكون الناس محظوظين بمافيه الكفاية للعثور على ملفاتهم المحذوفة في سلة المحذوفات في نظام التشغيل «ويندوز»، ومن السهل جداً إعادتها إلى موقعها الأصلي. ولكن رغم ذلك، هناك أيضاً أشخاص كثيرون قليلو الحظ، ممن يلاحظون حذف ملفاتهم بعد إفراغ سلة المحذوفات، مما يعني فقدان هذه الملفات إلى الأبد، أو على الأقل هذا ما يظنه العديدون.
بالنسبة إلى الأشخاص غير المحظوظين الذين يخسرون ملفاتهم بهذه الطريقة، هناك أخبار جيدة: لا زلتم تستطيعون استعادة ملفاتكم! بالطبع، يستعمل هذا الأمر جهات ليست نيتها جيدة بما فيه الكفاية. على سبيل المثال: أجهزة الأمن التي تود قراءة مستند سري معين ظننتم أنكم قد محوتموه نهائياً.
في هذه الحالة، ألقوا نظرة على مقالنا السابق عن برنامج Eraser.
أما بالنسبة للأشخاص الذين يريدون استعادة ملفاتهم، بإمكانهم استخدام برنامج Recuva.

كيف يعمل؟

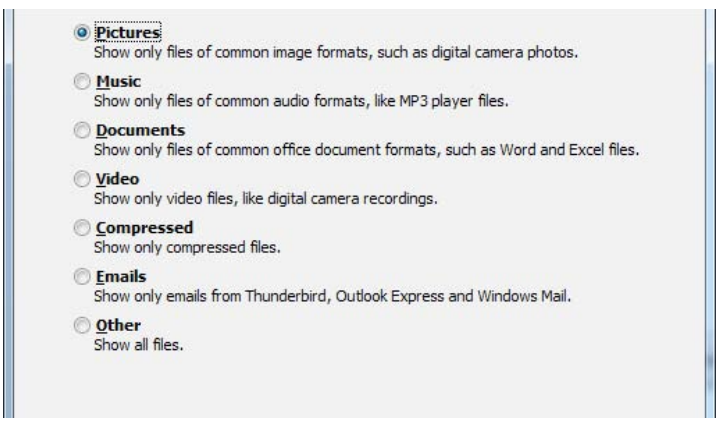
لماذا لا يزال بإمكانك استعادة ملفاتكم مرة أخرى بينما يقوم «ويندوز» بإخباركم بأنها قد ذهبت للأبد؟
يرتبط هذا بكيفية عمل الأقراص الصلبة وأنظمة التشغيل. ببساطة، يقوم نظام التشغيل بتقسيم القرص الصلب إلى جزئين، في الأول يتم تخزين البيانات، حيث يوجد البايتات الفعلية، بينما الجزء الثاني أصغر بكثير، ويحتوي على جدول للبحث بأسماء الملفات ومواقعها على جهاز الحاسوب. جدول البحث هذا هو ما يقوم نظام التشغيل «ويندوز» –وأنظمة التشغيل الأخرى– بالعمل عليه. فهو يعطي نظرة عامّة عمّا هو متوفر على القرص الصلب. تماماً كدليل أرقام الهاتف، فعندما تقومون بحذف رقم من الدليل، ذلك لا يعني أن خط الهاتف الذي يحمل ذلك الرقم سيختفي فجأة. كذلك الأمر بالنسبة إلى الملفات: عندما تقومون بحذف ملف من جهاز الحاسوب (عبر إفراغ سلة المحذوفات) كل ما يقوم به الحاسوب هو إزالة الإدخال من «دليل الهاتف» أو في مصطلحات الحاسوب «جدول توزيع الملفات». البيانات تبقى حيث هي، إلى أن نقوم بالكتابة فوقها بملفات جديدة.

Recuva

Recuva هو برنامج يمكّنكم من استعادة ملفاتكم المحذوفة، ووضعها مجدداً في جدول توزيع الملفات، حيث يقوم بإجراء عملية بحث عن الملفات غير المذكورة في الجدول وسؤالكم عمّا تريدون فعله بها. ستتمكّنون بهذه الطريقة بسهولة من استعادة هذه الملفات.
Recuva برنامج مجاني وبإمكانكم تحميله من هنا. بعد إتمام



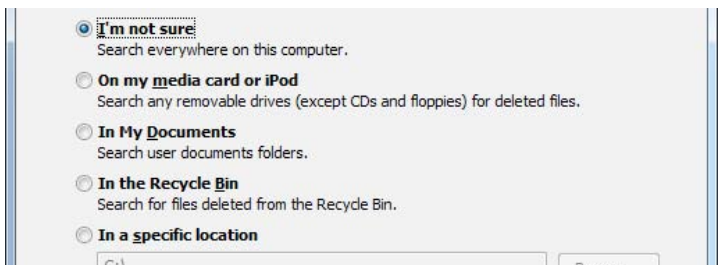
عملية التنصيب وتشغيل البرنامج، سيتم عرض شاشة ترحيب ودليل يقودكم إلى عدد من الخطوات السهلة.
بعد ظهور شاشة الترحيب أنقروا على Next.
في الشاشة التالية ستظهر لكم نافذة تسأل عن نوع الملفات التي تبحثون عنها. تحديد النوع بشكل محدد سيوفر على برنامج Recuva الوقت، حيث سيبحث عن أنماط معيّنة من الملفات، حددوا خياركم ثم انقروا على Next. إذا كنتم تريدون البحث عن أنواع



مختلفة من الملفات، بإمكانكم اختيار Other؛ سيقوم هذا الخيار بإبطاء عملية البحث، ولكن سيتيح لكم إمكانية إلقاء نظرة على كافة أنواع الملفات المحذوفة.

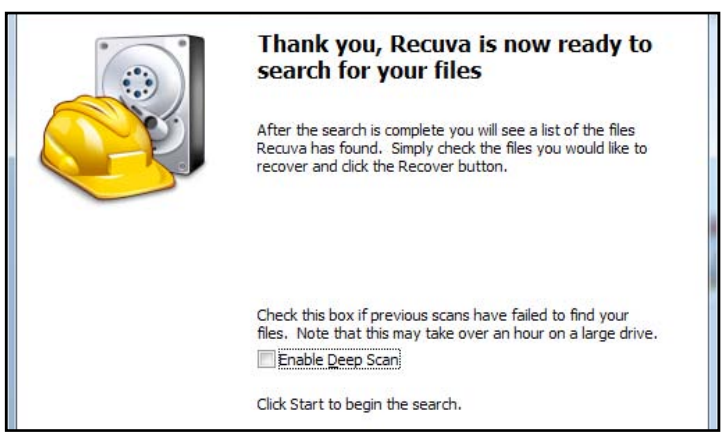
في الشاشة التالية سيتم سؤالكم في أي مسار يجب على برنامج Recuva أن يبحث.

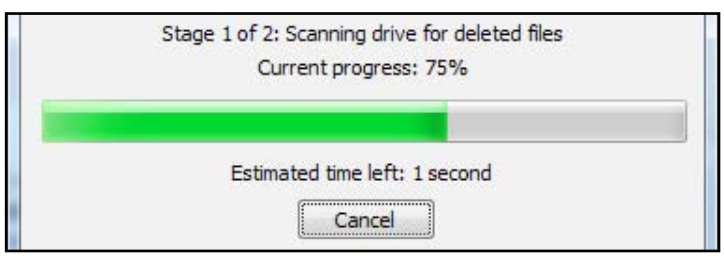
هذا الخيار هدفه توفير الوقت عبر البحث في أماكن محددة. إن كنتم تعرفون أين كان يوجد بالتحديد الملف المحذوف قومو بتحديد مساره، أما في حال لا تتذكرون أين كان الملف اختاروا «I'm not sure»وانقروا على «Next».



في الشاشة التالية سيتم إعلامكم بأن Recuva جاهز للبدء بعملية البحث، كما أنه يوفر خياراً يدعى فحص عميق أو Deep-Scan يتيح هذا الخيار البحث بعمق، إلا أنه قلما يتيح العثور على ملفات يمكن استرجاعها.

إلجؤوا إلى هذا الخيار فقط في حال لم تتمكنوا من العثور على ملفاتكم عبر الخيارات السابقة.





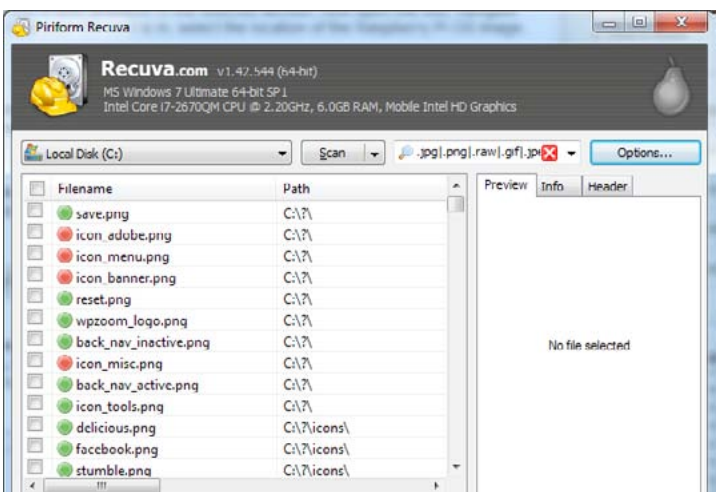
سيقوم البرنامج الآن بالبحث في القرص الصلب عن الملفات المحددة. واعتماداً على حجم القرص الصلب وعدد الملفات، قد تستغرق هذه العملية دقيقة، أو نصف ساعة، أو ربما أكثر. لذا تحلّوا بالصبر.

بعد انتهاء عملية البحث، تحين اللحظة الكبرى؛ سيقوم برنامج Recuva بعرض الملفات التي قام بإيجادها. سيكون من الأسهل عليكم إن قمتم بالنقر على "Switch to advance mode"، حيث سيقوم بتزويدكم بنظرة عامة أكثر فائدة عن هذه الملفات. العديد من الملفات التي سترونها ربّما لن تكونوا رأيتموها من قبل. يقوم نظام التشغيل «ويندوز» بحذف هذه الملفات تلقائياً، وبإمكانكم تجاهلها.

ستلاحظون أيضاً أن هناك عدد من الملفات سيتم تحديدها بنقطة خضراء، والبقية بنقطة حمراء.

تدل النقطة الخضراء أن برنامج Recuva استطاع استعادة هذه الملفات، بينما النقطة الحمراء تدل على أن هذا الملف معطوب، أو تمت الكتابة فوقه بشكل جزئي من قبل ملف آخر. النقطة الحمراء غالباً ما تعني أن تم فقدانها جزئياً إلى الأبد.

حدّدوا الملفات التي تريدون استعادتها ثم انقروا على زر «Recover» سيقوم البرنامج بسؤالكم عن المكان الذي تريدون تخزين ملفاتكم فيه. ننصحكم باختيار مجلد غير المجلد الأصلي للملفات لتفادي إعادة الكتابة فوق الملفات التي لم تقوموا باستعادتها بعد.



الآن تمت استعادة ملفاتكم! تحقّقوا من المجلد حيث خزنتم الملفات فيه، ومن أنها تعمل أيضاً، ففي بعض الأحيان لا تفتح هذه الملفات، في هذه الحالة عليكم اللجوء إلى مختصّ وطلب استعادة ملفاتكم.

إزالة الملفات الخبيثة Malware

البرمجيات الخبيثة Malware هي برامج صغيرة مؤذية تنتقل إلى حاسوبكم بعد زيارة موقع إنترنت مصاب أو استخدام USB (فلاشة) تحتوي على ضيوف غير مرغوب فيهم.

البرمجيات الخبيثة هي كابوس للعديد من مستخدمي الحاسوب، تستطيع أن تبطئ نظام التشغيل، أو تزعجكم بالنوافذ المنبثقة، أو تغيّر بعض الأمور على حاسوبكم، ممّا يحرمكم من الحصول على تجربة ممتعة.

على الرغم من أنّ معظم البرمجيات الخبيثة تثير الإزعاج، إلا أن البعض منها يمكنه أيضاً أن يدمر ملفاتكم، أو يتجسس على جهازكم، وهذه البرمجيات تعرف ببرامج التجسس.

لسوء الحظ هناك الكثير من البرمجيات الخبيثة، والعديد منها لا يتم الكشف عنه باستخدام برامج مكافحة الفيروس العادية، خاصة عندما تكون برمجية ما جديدةً جداً. لهذا السبب، غالباً لا توجد طريقة عامة لإزالة البرمجيات الخبيثة من الحاسوب، وفي بعض الحالات الخطيرة، لا يمكن إزالتها سوى بإعادة تنصيب نظام التشغيل. على الرغم من أن حالاتٍ مشابهة يمكن أن تحدث بسبب مشاكل في قطع الحاسوب، إلا أنه من الجيد التحقق دائماً من وجود البرمجيات الخبيثة إذا كان حاسوبكم يتصرف بشكل غريب. في هذه المقالة سنقدم شرحاً عاماً لكيفية القيام بذلك.

مسح الفيروسات وإعادة تشغيل الحاسوب

إذا كنتم تظنون أن حاسوبكم مصاب ببرمجيات خبيثة، فالخطوة الأولى التي يجب اتخاذها هي فحصه بأحد برامج مكافحة الفيروسات. إذا لم يكن لديكم واحد، تأكدوا من تثبيت واحد فوراً واستخدامه باستمرار. يوصي فريق «سايبر آرابز» المستخدمين بالنسخة المجانية من برنامج مكافحة الفيروسات «أفيرا» الذي يتم تحديثه باستمرار ويعمل بشكل جيد. تأكدوا من أنكم تستخدمون النسخ الأصلية من برامج مكافحة الفيروسات، فمن المعروف أن النسخ المقرصنة منها تحتوي فيروسات ويجب تجنّب استخدامها.

إذا استمر حاسوبكم بالتصرف بشكل غريب بعد إتمام عملية مسح الفيروسات، عليكم اللجوء إلى عملية أكثر جذرية. لبدء هذه العملية من الأفضل إعادة تشغيل الحاسوب في مايسمى «الوضع الآمن».

في هذا الوضع، يعمل الحاسوب بتحميل الحد الأدنى من البرامج والخدمات. إذا تم إعداد أي من البرمجيات الخبيثة للعمل عند إقلاع نظام التشغيل، فإن العمل في الوضع الآمن سوف يمنع البرمجية الخبيثة من ذلك.

للدخول إلى «الوضع الآمن» أعيدوا إقلاع نظام التشغيل «ويندوز»، في المرحلة التي تسبق ظهور شعار «ويندوز»، إضغطوا على زر F8؛ ستظهر لكم قائمة الخيارات المتقدمة للإقلاع. اختاروا Safe mode with Networking ثم اضغطوا على Enter.

ستلاحظون أن بيئة العمل ستختلف عليكم قليلاً، وذلك لأن «ويندوز» يقوم بتحميل الإعدادات الأساسية فقط في الوضع الآمن. أما البرامج التي تعمل مع بدء تشغيل «ويندوز»، مثل «سكايب» أو برامج مكافحة الفيروسات، فلن يتم تحميلها.

الوضع الآمن ليس بيئة مناسبة للعمل، فنحن نلجأ إلى هذا الوضع فقط لحل المشاكل كما نفعل الآن.

برامج مكافحة البرمجيات الخبيثة

الآن وبعد أن قمتم بتشغيل الحاسوب في الوضع الآمن، حان الوقت لتحديد برنامج لمسح الفيروسات في حاسوبكم. إذا كنتم قد استعملتم برنامج لمكافحة الفيروسات على جهازكم، عليكم استخدام واحداً من نوعٍ آخر لإتمام عملية الفحص هذه، طالما أن مكافح الفيروسات الحالي لم يستطع اكتشاف البرمجية الخبيثة. تذكروا: لا يوجد أي برنامج لمكافحة الفيروسات أو البرمجيات الخبيثة يستطيع أن يضمن لكم اكتشاف الملايين من أنواع البرمجيات الخبيثة بنسبة ١٠٠٪. بعض البرمجيات الخبيثة، خاصة تلك التي تستهدف مجموعات صغيرة من المستخدمين، قد لا يمكن اكتشافها أبداً، في هذه الحالة عليكم التواصل معنا عبر صفحتنا على فيس بوك لتلقي المساعدة.

من بين البرامج المجانية المتاحة لمسح الملفات الخبيثة هناك:

Microsoft Malware Remover
BitDefender Free Edition
Kaspersky Virus Removal Tool
Malwarebytes
Norman Malware Cleaner
SuperAntiSpyware
Spybot

وأما المستخدمون في سوريا، فننصحهم بشدة باستخدام Dark Comet Remover بالإضافة إلى البرامج المذكورة أعلاه. حيث يستهدف برمجية خبيثة معينة. فبينما في الغالب لا تقوم هذه البرمجية بالتسبب بعطب في الحاسوب، فإنها تسمح لأطراف ثالثة (موجودة في سوريا) بالتحكم بجهاز الحاسوب، وقراءة الملفات، وتشغيل الكاميرا، أو التجسس على المحادثات. وبما أن ليست كافة برامج المسح تقوم باكتشاف البرمجية الخبيثة نفسها، فمن الأفضل تجربة أي البرامج تعمل بشكل أفضل بالنسبة إليكم. وكافة البرامج المذكورة أعلاه مستقلة، أي أنها لا تعمل في الخلفية كبرامج مكافحة الفيروسات. بعد إتمام عملية الفحص والتخلص من البرمجيات الخبيثة على حاسوبكم، بإمكانكم إزالة هذه البرامج وإعادة تشغيل حاسوبكم.

تشغيل برنامج مكافحة البرمجيات الخبيثة

بسبب العدد الهائل من برامج مكافحة البرمجيات الخبيثة، لن نناقش كل برنامج منها على حدة في هذا المقال. معظم هذه البرامج تعمل بشكل بديهي، حيث تقومون بتنصيبها ثم تشغيلها والقيام بعملية فحص، وهي تستهلك في بعض الأحيان وقتاً طويلاً (قد يصل إلى بضع ساعات). سيقوم البرنامج بعدها بإزالة البرمجيات الخبيثة التي يجدها، وبعض الأحيان يقوم بسؤالكم قبل الإزالة، وحالما يزيل البرنامج البرمجيات الخبيثة تستطيعون إعادة تشغيل جهاز الحاسوب.

لكون برنامج MalwareBytes من أفضل البرامج المتوفرة، سوف نناقش باختصار هذا البرنامج هنا بهدف الإيضاح.

يبدأ استخدام برنامج MalwareBytes طبعاً بتحميله من الإنترنت؛ تستطيعون تحميله هنا. إذا كنتم لا تملكون اتصالا بالإنترنت أو لا تستطيعون تحميله على الجهاز المصاب، حمّلوه على حاسوب آخر ثم انسخوه إلى الحاسوب المصاب باستخدام قرص USB.

بعد إتمام عملية التحميل، شغّلوا ملف التنصيب واتّبعوا الإرشادات لتنصيبه، بعد انتهاء العملية سيتحقق برنامج MalwareBytes من وجود تحديثات

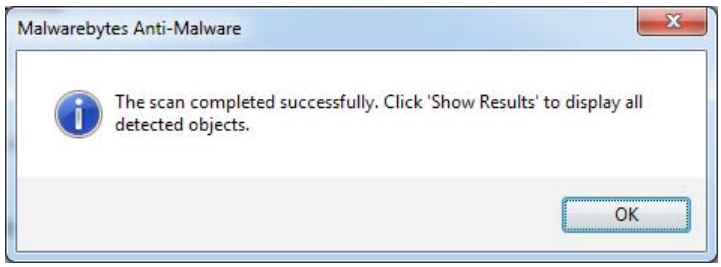
وبعد إتمام تحميلها سيعمل تلقائياً. إذا ظهرت لكم رسالة تخبركم بأن قاعدة البيانات لديكم منتهية الصلاحية، أنقروا على «Yes» لتحميل التحديثات ثم على OK عندما تظهر للتأكيد أنه تم تنصيب التحديثات بنجاح.

بعد تحديث MalwareBytes، ستشاهدون القائمة الرئيسية للبرنامج. في التبويب الأول هناك ثلاثة خيارات: Perform quick scan،perform full scan وperform flash scan. الفرق بين هذه العمليات الثلاث هو الكثافة في الفحص، فعملية flash scan ستقوم بفحص الذاكرة وبعض الأماكن التي تصاب غالباً بالبرمجيات الخبيثة. في النسخة المجانية هذا الخيار غير متاح، ونحن لا ننصح باستخدامه.

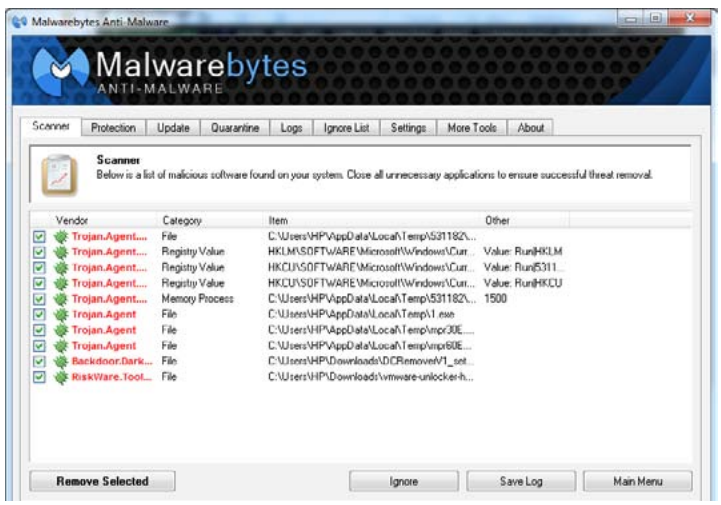
أما خياري quick scan و full scan فالفرق بينهما هو كمية مسارات الملفات التي يقوم بفحصها؛ قد يقوم quick scan بالكشف عن أغلب البرمجيات الخبيثة، إلا أن عملية full scan قد تكون ضرورية لإيجاد البرمجيات الخبيثة المخفية جيداً. لذلك فإن الخيار الأخير قد يستغرق وقتاً قد يصل إلى ساعات، بينما quick scan لن يستغرق أكثر من نصف ساعة. حددوا الخيار المناسب لكم ثم انقروا على زر "scan".

سيقوم برنامج MalwarreBytes بمسح البرمجيات الخبيثة في حاسوبكم، إذا وجد شيئاً مثيراً للشك سيقوم بإظهار الملف باللون الأحمر، وكما قلنا سابقاً فإن عملية الفحص قد تستغرق ساعات. وفي حال – لسبب ما – أردتم القيام بإيقاف عملية الفحص، يمكنكم دائماً النقر على زر "Abort" للعودة إلى القائمة الرئيسية للبرنامج.

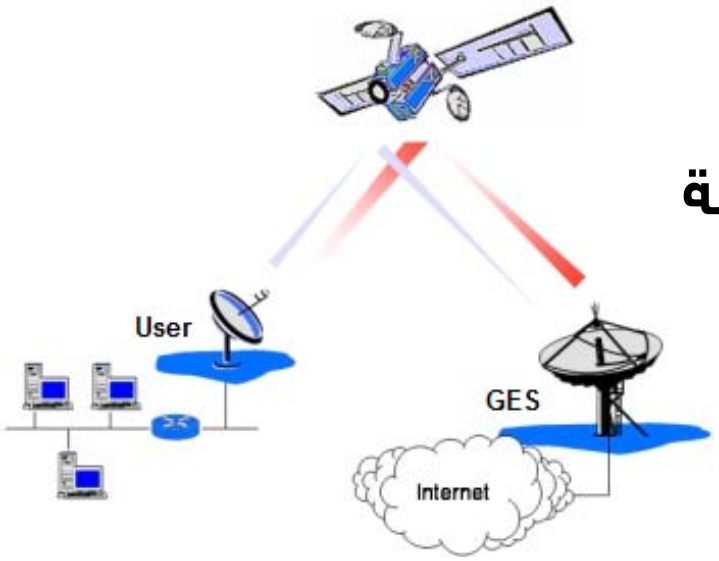
بعد انتهاء عملية الفحص بنجاح، ستظهر لكم رسالة على الشاشة تخبركم بأن عملية الفحص تمت بنجاح، وبإمكانكم مشاهدة نتائجها.



بعد النقر على "Show Results" سيتم عرض كل شيء كشفه البرنامج. في بعض الأحيان يقوم برنامج مكافحة البرمجيات الخبيثة بإظهار برنامج ما على أنه برمجية خبيثة، بينما هو في الحقيقة برنامج أصلي. لهذا السبب من المهم التأكد من قائمة الملفات التي وجدها البرنامج وإزالة التحديد عن البرامج التي تتأكدون من أنها لا تحتوي على برمجيات خبيثة. بعد إتمام ذلك انقروا على "Remove selected" ما سيجعل برنامج MalwareBytes يحذف هذه البرمجيات الخبيثة من حاسوبكم.



بعد قيام البرنامج بحذف كافة البرمجيات الخبيثة، سيطلب منكم إعادة تشغيل الحاسوب. بعد إتمام هذه العملية من الأفضل إعادة تشغيل برنامج MalwareBytes وإجراء عملية الفحص مرة أخرى للتأكد من أنه قام بحذف كافة الملفات المصابة. إذا كنتم لا تزالون تواجهون مشاكل مع حاسوبكم، من الجيد تجربة برامج مكافحة البرمجيات الخبيثة المذكورة أعلاه. لا تستطيع كافة البرامج هذه الكشف عن البرمجية الخبيثة ذاتها، لذا ربما يكون حاسوبكم لا يزال مصاباً بإحدى البرمجيات الخبيثة بعد أن يخبركم البرنامج أن جهازكم قد أصبح سليماً.



الإنترنت عبر الأقمار الصناعية (أو الإنترنت الفضائي)

ازداد استخدام الإنترنت الفضائي انتشاراً في العالم العربي كثيراً، خاصة في المناطق النائية حيث لا توجد بنية تحتيّة قويّة للإنترنت، كسوريا، ومناطق الريف في اليمن، وصحراء الجزائر والسعودية.

يوفّر الإنترنت الفضائي إمكانية الاتصال بالإنترنت خارج نطاق السلطة القضائية للدول، وكمستخدمين للإنترنت الفضائي فأنتم تشغّلون مزود الإنترنت الخاص بكم.
يعمل الإنترنت الفضائي عبر أقمار صناعية ثابتة بالنسبة إلى الأرض، وعلى ارتفاع ٣٥ كيلومتر عن سطحها. وكما ترون في الصورة (١) فالقمر الصناعي هو نقطة الاتصال بين المستخدم وما يسمى «المحطة الأرضية» عبر اتصال إنترنت سريع، وعادةً ما تكون المحطة الأرضية متواجدة في أوروبا أو الولايات المتحدة و لا تخضع للتجسس.

تتوفّر العديد من الشركات المزودة لخدمة الإنترنت الفضائي في العالم العربي. وأكثرها شهرة هي:

SES Broadband (المعروفة بـ Astra2Connect سابقاً) و HughesNet وEutelsa التي تبيع حزم انترنت باسم "TooWay".
ولكن ينبغي أن نأخذ في عين الاعتبار أن ليس بالضرورة أن تكون جميع الحزم توفر تغطية شاملة، ما يدفعنا إلى التحقق عبر موقع الشركة على الإنترنت من المناطق التي تقوم بتغطيتها وبناءً عليه نحدد فيما إذا كانت هذه الشركة مفيدة لنا أم لا. أيضاً، من الجيّد معرفة حقيقة أن العديد من الحكومات تحظر استخدام أجهزة الإنترنت الفضائي.

تتألف معدّات الإنترنت الفضائي عادة من:
١. مودم/راوتر
٢. طبق لاقط
٣. إبرة تغذية
٤. كابلات
٥. اشتراك وبطاقات إعادة شحن (يتم عادة شراؤها باستخدام بطاقة الإئتمان)

تختلف تكاليف الاشتراك وحجم التحميل بشكل كبير بين مزوّدي الخدمة والموزعين، حيث تبدأ أسعار الاشتراكات تقريباً بـ ٥٠ دولاراً شهرياً مع حجم تحميل محدود، وتصل إلى عدة مئات من الدولارات للحزم غير المحدودة. أما اختيار الاشتراك الأفضل فيعتمد على ما تريدونه.

عندما تتجاوزون حجم التحميل المسموح به شهرياً، تنخفض السرعة إلى حد كبير حيث تصبح غير عمليّة، بإمكانكم شراء بطاقات زيادة الرصيد على الإنترنت لزيادة حدّ التحميل، ولكن لا تتم عملية شراء هذه البطاقات من الشركات المالكة (مثلاً: EutelSat أو Astra) بل يتم شراؤها عبر الشركات الوسيطة التي قمتم بشراء المعدات منها. اسألوا الموزّع عن أماكن بيع هذه البطاقات.

التركيب

تركيب الإنترنت الفضائي ليس صعباً جداً، على الرغم من ذلك نوصي بتركيب المعدات من قبل المختصّين، إلا أننا لاحظنا أن معظم قرّاء «سايبر آرابز» ليسوا في أماكن تتيح لهم الوصول إلى المختصين لتركيب المعدات، ويعود ذلك غالباً إلى صعوبة الوصول إلى المكان كسوريا مثلاً. لذا، سوف نتطرق إلى طريقة

التركيب في هذه المقالة بشكل موجز، ولكن يرجى الأخذ بعين الاعتبار أنه من الضروري اتباع الإرشادات التي أتت مع المعدات بعناية، فوصل كابل خطأ قد يؤدي إلى تدمير المعدات بكاملها. لكي تحصلوا على المعلومات، قام فريق «سايبر آرابز» بكتابة دليل إعداد نظام أسترا/SES، تستطيعون قراءته هنا.

إن كنتم حديثي العهد باستعمال الصحون اللاقطة، من الجيد معرفة أن رزمة الصحن اللاقط تتألف – على الأقل– من الأجزاء التالية:

١. الصحن اللاقط
٢. إبرة التغذية (القطعة التي تقوم باستقبال الإشارة)
٣. الذراع المعدني (تقوم بحمل إبرة التغذية)
عملية تجميع هذه الأجزاء مع بعضها ليست صعبة، وننصح باتباع الإرشادات التي أتت مع الحزمة عند شرائها.

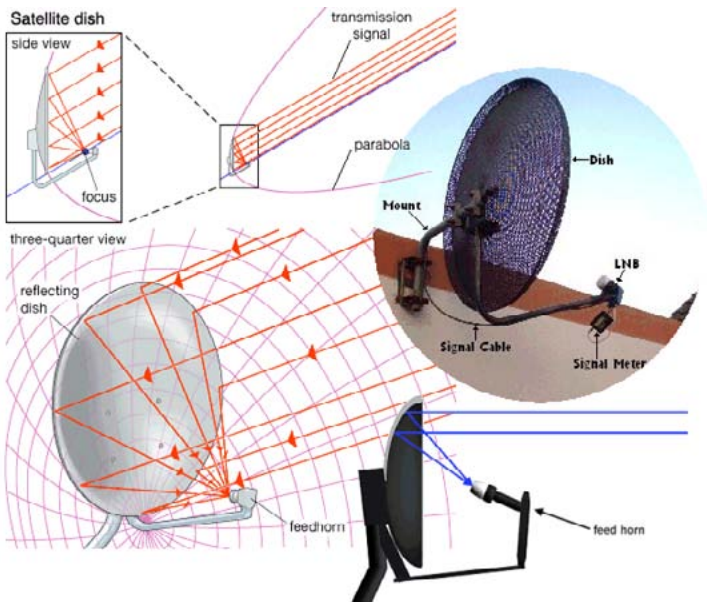
يعمل الصحن اللاقط على استقبال الإشارة على الصحن نفسه ثم تركيز هذه الإشارة على إبرة التغذية، وتقوم الإبرة بدورها بنقل الإشارة إلى موزّع الإنترنت (راوتر).

الجزء الأهم في إعداد اتصال الإنترنت الفضائي هو مكان الصحن اللاقط، فالصحن (أو بشكل أدق الذراع المعدني الحامل للإبرة) يجب أن يشير بالضبط إلى القمر الصناعي، وتوجيه الإبرة في الاتجاه الصحيح مهمة يقوم بها عادة أشخاص ذوو خبرة في هذا المجال. إلا أننا تمكنّا من تحقيق نتائج جيدة أثناء تركيز الإبرة عبر استعمال أدوات بسيطة وتطبيق هاتف ذكي.

لبدء تحديد موقع الصحن اللاقط ستحتاجون إلى اسم وموقع القمر الصناعي في السماء. تستخدم حزم الإنترنت الأكثر شيوعاً إما KA-SAT (Eutelsat, Astra-3B (Astra2Connect, SES broadband أو Echostar XVII (HughesNet (TooWay)..

المعلومة الثانية التي تحتاجون إليها هي الإحداثيات الجغرافية لتموضعكم على الكرة الأرضية، باستخدام خطوط العرض والطول.

بمعرفة هذه المعلومات، من الممكن حساب زاوية السمت وميل الصحن. السمت هو الزاوية بين اتجاه الشمال ومحور الصحن. ويشير ميل الصحن إلى مدى ارتفاع الطبق بالنسبة إلى الأفق (٠–٩٠ درجة). وتختلف هذه المعايير بناءً على موقعكم على الأرض.



لحسن الحظ، هناك تطبيق على نظام «أندرويد» يقوم بكافة عمليات الحساب اللازمة اعتماداً على إشارة الـ GPS (نظام التموضع العالمي) للهاتف وتطبيق البوصلة اسمه «Satellite Director». حملوا التطبيق، من «غوغل بلاي ستور»، أو من هنا في حال كان المتجر محجوباً. تأكدوا من تحميله قبل الانتقال إلى الميدان (حيث لاتوجد شبكة إنترنت). التطبيق لا يحتاج إلى اتصال بشبكة إنترنت ليعمل، ولكن من الجيد التأكد من أن هاتفكم النقال فيه بوصلة مدمجة. بعض الهواتف الذكية رخيصة الثمن لا توجد فيها ميزة البوصلة وبالتالي لن تعمل بشكل صحيح.
يستخدم تطبيق Satellite Director كاميرا الهاتف للتوجيه، بهذه الطريقة تستطيعون النظر إلى تموضع

الذراع المعدني الحامل لإبرة التغذية وضبطه ليطابق الإعدادات المثالية التي قام التطبيق بتحديدها.

قبل البدء باستعمال تطبيق Satellite Director قوموا دائماً بمعايرة البوصلة عبر تحريك الهاتف افقياً في رسم الشكل ٨.

أيضاً، يرجى الإنتباه إلى أن الصحن اللاقط الحديدي أو المنصة أو قطب مغناطيسي ، ستؤثر على البوصلة عندما تقربوها منها. لدى الجهوز لتحديد موضع الصحن اللاقط، اتبعوا الخطوات التالية:

١. فعّلوا نظام التموضع العالمي (GPS)

٢. أنقروا على تبويب Satellites ثم اختاروا القمر الصناعي المطلوب (KA-SAT أو Astra-3B أو Echostar XVII... إلخ)

٣. قوموا بالنقر على تبويب Director، ثم قوموا بمحاذاة الجزء العلوي من الهاتف الخاص بكم مع ارتفاع القمر الصناعي عن طريق تدوير الهاتف في المستوى الأفقي (Roll) والمستوى العمودي (Pitch) إلى أن تصبح الكرة البيضاء داخل الدائرة البيضاء.

٤. في التبويب Director: قوموا بمحاذاة الجزء العلوي من الهاتف الخاص بكم مع زاوية سمت القمر الصناعي عبر تدوير الهاتف باتجاه أو بعكس اتجاه عقارب الساعة إلى أن تصبح الكرة الزرقاء داخل الدائرة الزرقاء .

٥. في التبويب Director: حين تصبح الكرة البيضاء في الدائرة البيضاء والكرة الزرقاء في الدائرة الزرقاء، إذاً فالجزء العلوي من هاتفكم (السهم الأزرق على الشاشة) يشير إلى القمر الصناعي الذي اخترتموه.

٦. قوموا بمحاذاة الذراع التي تحمل الصحن اللاقط مع زاوية السمت، مع مراعاة أن تبقى الطابة البيضاء داخل الدائرة البيضاء والطابة الزرقاء داخل الدائرة الزرقاء. يشير الصحن اللاقط الآن إلى زاوية السمت الصحيحة التي يقع عليها القمر الصناعي. عدّلوا ارتفاع الصحن ثم أميلوه قليلاً لتحسين

الإشارة.

بعد إتمام عملية محاذاة الصحن اللاقط، ثبتوه بقوة للتأكد من أنه لن يتحرك. يمكنكم الآن تجربة ما إذا كان الاتصال بالإنترنت يعمل؛ لتجميع بقية المعدات معاً، يرجى اتباع الإرشادات المرفقة مع حزمة المعدات الخاصة بكم.

إذا كان اتصال الإنترنت بطيئاً، فذلك قد يكون مؤشراً إلى خطأ في محاذاة الصحن اللاقط، في هذه الحالة يرجى إعادة الخطوات المذكورة أعلاه.

المخاطر

يمكن بسهولة الكشف عن مكان معدات الأقمار الصناعية عن طريق التثليث (وهي عملية حسابية تتيح تحديد المسافة بين المراقب والهدف عبر استعمال المسافة بين المراقب ونقطة مرجعية والزاوية بين المراقب والهدف والنقطة المرجعية) ما يعني أن مكانكم ليس آمناً مئة بالمئة، والأشخاص السيؤون سيكونون قادرون على تحديد موضعكم.

تلقينا معلومات تفيد بأنه في سوريا، على سبيل المثال، تم استخدام هذه المعلومات من قبل الحكومة لاستهداف المراكز الإعلامية. على الرغم من أن خطر الكشف عن الإنترنت الفضائي أقل بكثير من خطر الكشف عن الهاتف الفضائي، إلا أنه من الجيد أخذ هذا الخطر الممكن بعين الاعتبار عند تجهيز مركز إعلامي.

كيف تؤمنون حياتكم الرقمية؟

غالباً ما نتلقى من قراء «سايبر آرابز» طلبات لتقديم ملخص حول البرامج التي يتوجب تنصيبها من أجل جعل حياتهم الرقمية أكثر أمناً. إلا أنه، وكما يعرف قرّاؤنا المعتادون، ليس هناك من حل سحري أو حتى لائحة تدقيق تشمل أشياء يمكن، بعد تأديتها، أن تؤمّنوا أنفسكم من أي شر. الأمن الرقمي يتعلق بشكل أساسي بسلوككم. يمكنكم أن تنصبوا عدة أدوات، ولكن إذا استخدمتوموها دون إبداء الحرص اللازم، ستجعلون أنفسكم ضحية لأعمال الأشخاص ذوي النوايا السيئة، فأبقوا هذا الأمر في بالكم. سنقوم في ما يلي بتلخيص أبرز الممارسات الأساسية التي يمكنكم أن تتبعوها لتكونوا في أمان.

إحدى أكثر الطرق شيوعاً للوقوع في المتاعب هي استعمال مقاهي الإنترنت العامة. إن العديد الحكومات في العالم العربي تراقب سلوك مستخدمي الإنترنت من خلال مقاهي الإنترنت، لذا ينصح بتفادي ارتياد هذه المقاهي في الأساس. إذا كنتم فعلاً في حاجة إلى استعمال خدمة الانترت من مقهى إنترنت عمومي (أو نقطة واي فاي عمومية)، إحرصوا على إحضار حاسوبكم المحمول الخاص أو حاسوب شخص تثقون به. من أجل الاتصال بالانترنت بشكل آمن، قد يكون أيضاً من المستحسن أن تنصبوا خدمة شبكة افتراضية خاصة **VPN** أو خدمة **SSH**. تقوم هذه الخدمات بتشفير نشاطكم على الإنترنت بشكل يمنع أي أحد آخر من النفاذ إلى محتواه. التطبيقات الأكثر شعبية التي تشفّر محتوى النشاط على الإنترنت هي **Tor** و**Hotspot Shield** ، ولكن تتوفر أيضاً عدة تطبيقات موثوقة أخرى. إن لم تكونوا متأكدين من أمان استعمال تطبيق معين، نرجو منكم الاتصال بنا عبر صفحة فيس بوك الخاصة بنا.

المتصفح الذي تستعملونه هو التطبيق الذي تنفذون من خلاله إلى الإنترنت، ولذا فمن المهم أن تبقوا هذا التطبيق آمناً. بسبب المشاكل الأمنية التي تعرض لها متصفح إنترنت إكسبلورر في الماضي، فإننا لا ننصح باستعماله. عوضاً عنه، ننصح باستعمال غوغل كروم، أو فايرفوكس مصحوباً بإضافات الأمان. من المستحسن أيضاً أن تتفحصوا إعدادات الأمان بشكل دوري في متصفحكم. إن لم تكونوا قادرين على استعمال أي من الأدوات المذكورة أعلاه لتشفير نشاطكم على الإنترنت، إحرصوا على الأقل على إجراء اتصالاتكم (البريد

الإلكتروني، إلخ.) من خلال مواقع تستعمل تشفير **HTTPS** أو **SSL**. إن أردتم التأكد من أنكم تستعملون النسخة المشفرة ببروتوكول **HTTPS/SSL** لولوج موقع معين، استخدموا إضافة **HTTPS Everywhere** مع متصفحكم.

متى ما أصبحتم على الإنترنت، إنتبهوا إلى ما تقومون بمشاركته مع الآخرين. تفادوا دائماً مشاركة التفاصيل الشخصية وانتبهوا إلى أنكم إذا قمتم برفع صور أو مشاركتها، فقد يعلم المتلقي بموقعكم الجغرافي. إن كنتم من مستخدمي فيس بوك، فمن المستحسن أن تقرؤوا كيف تستعملون فيس بوك بأمان. بالطبع، عليكم دائماً أن تستعملوا كلمات مرور آمنة، بما أن الكلمات البسيطة يمكنها اكتشافها بسهولة باستعمال برامج متخصصة. يمكنكم أن تخزّنوا كلمات المرور الخاصة بكم في قاعدة البيانات التي يوفرها برنامج كيباس. لدى استعمال فيس بوك، من الأفضل استعمال خيار التحقق بخطوتين.

غالباً ما تكون الهجمات عبر الفيروسات (والبرمجيات الخبيثة بشكل عام) وراء المشاكل الرقمية. ونقوم بشكل دوري بالكتابة عبر موقعنا عن فيروسات تنتشر في بلدان الشرق الأوسط ولذا فمن المستحسن أن تبقواعلى اطلاع على آخر

التهديدات المماثلة عبر صفحتنا على فيس بوك. لتفادي إصابة أجهزتكم بالفيروسات، ننصح باستخدام ماسح فيروسات مثل أفيرا المجاني. لا تشتروا أي نسخة مقرصنة من البرامج المضادة للفيروسات.

حتى وإن كان لديكم أفضل برنامج مضاد للفيروسات، فإن جهاز الحاسوب الخاص بكم قد يتعرض للسرقة أو المصادرة، مما يسهّل على الجهة التي تستحوذ عليه أن تحصل على ملفاتكم الحساسة. لذا، ننصحكم بتشفير الملفات على القرص الصلب على جهازكم عبر استخدام برامج مثل **Truecrypt** أو **AES Crypt**. إذا قمتم بتشفير مستنداتكم، تأكدوا من أنكم قد أزلتم النسخ غير المشفرة. للتأكد من أنكم قد أزلتم مستنداً ما بشكل نهائي، دون السماح لأحد استرجاعه، يمكنكم أن تستعملوا برنامج **Eraser**. إن كنتم تتعاملون مع معلومات مهمة، قوموا بإعداد نسخ احتياطية عنها؛ إحدى الأدوات الجيدة للقيام بهذه المهمة هي **SyncToy**.

وأخيراً، زوروا موقعنا للحصول على آخر الأخبار، والنصائح، والتحذيرات، أو تسّجلوا على صفحة فيس بوك الخاصة بنا لتلقي هذه التحديثات بشكل تلقائي.

"جيتسي" لإجراء مكالمات ومحادثات آمنة ومشفرة

جيتسي برنامج مجاني ومفتوح المصدر وآمن، يتيح إجراء محادثات عبر الصوت والفيديو، وإجراء المحادثات النصية. يعمل جيتسي على أنظمة التشغيل ويندوز وماك ولينكس، كما يجري حالياً تطوير النسخة التجريبية منه لنظام تشغيل الهواتف الذكية أندرويد.

يدعم جيتسي العديد من بروتوكولات خدمات الدردشة مثل حسابات غوغل أو ياهو أو فيس بوك إضافة إلى بروتوكول SIP و XMPP وشبكة جيتسي نفسها، حيث تمكّنكم الأخيرة من إجراء مكالمات فيديو مشفّرة.

كما يدعم جيتسي تشفير OTR للمحادثات النصية من دون الحاجة إلى أي إضافة، ويقوم بتشفير المكالمات الصوتية بتقنية ZRTP.

– للبدء باستخدام جيتسي نقوم أولاً بالذهاب إلى موقع البرنامج

– ثم النقر على Download

– نقوم الآن بتحديد نظام التشغيل وما إذا كانت نسخة النظام هي 32 أو 64 بت إذا كان نظام التشغيل هو ويندوز

– بإمكانكم معرفة نظام التشغيل الخاص بكم عبر النقر على قائمة ابدأ، ثم النقر بالزر الأيمن على الكمبيوتر واختيار خصائص أو Properties

– في خانة System Type ستلاحظون نسخة نظام التشغيل الموجودة على جهازكم

– بعد اختيار النسخة المطلوبة وانتهاء التحميل نقوم بفتح ملف التنصيب وإتمام عملية التنصيب كما تشاهدون

– الآن بعد انتهاء عملية التنصيب نقوم بفتح جيتسي. عند الفتح للمرة الأولى ستظهر نافذة تحتوي على الشبكات التي يدعمها البرنامج. بإمكانكم إدخال أكثر من حساب، لكن في درسنا هذا سنقوم بإضافة حساب جيميل.

– بعد إضافة الحساب نقوم بالنقر على Sign in

– نقوم الآن بإضافة جهة اتصال لبدء المحادثة معها عبر النقر على file ثم add contact

– نقوم بإدخال البريد الالكتروني ثم النقر على Add

– لبدء اي محادثة مشفرة علينا أولاً إنشاء المفتاح الخاص بنا. نقوم بالذهاب إلى Tools ثم Options ثم نذهب إلى تبويب Security، نختار الحساب الذي نريد توليد المفتاح الخاص به ثم ننقر على Generate.

– لتشفير المحادثة النصية بين الطرفين نفتح المحادثة مع الشخص ثم ننقر على Secure chat ثم Start private conversation

– يجب ملاحظة أنه في حال كان الشخص لم يكن يستخدم جيتسي أو أحد البرامج التي تدعم تشفير OTR مثل بدجن فإن هذا الخيار لن يعمل، حيث ستظهر للمستخدم رسالة تخبره بأن يقوم بتحميل أحد برامج الدردشة التي تدعم OTR.

– الآن بعد أن قمنا باختيار تشفير المحادثة، سنلاحظ أن رمز القفل تغيّر ولكن مع إشارة تعجب. هذه الإشارة تعني أن المحادثة مشفرة ولكن لم يتم التأكد من هوية الشخص

– للتأكد من هوية الشخص ننقر على Secure Chat ثم نختار Authenticate buddy ستظهر لنا نافذة فيها البصمة الخاصة بنا وتحتها البصمة الخاصة بالشخص الذي نريد محادثته، نستطيع الاتصال بهذا الشخص والتأكد من أن هذه هي البصمة الخاصة به

– بعد التأكد قوموا بتعديل الخيار إلى I have والنقر على Authenticate buddy . تستطيعون أيضاً، للتأكد، كتابة البصمة الخاصة بالشخص الآخر مجدداً في مكانها ثم النقر على Authenticate buddy

– ستلاحظون أن إشارة التعجب قد زالت. بإمكانكم الآن بدء المحادثة المشفرة، حيث لن يراها أحد، ولن يتم تخزينها على الجهاز أيضاً.

بالنسبة لتشفير المحادثات الصوتية والفيديو لا يختلف الأمر كثيراً. للبدء بمحادثة صوت او فيديو أو حتى مشاركة الشاشة، نقوم بالنقر على الزر المخصص لها في قائمة جهات الاتصال او من نافذة المحادثة عبر النقر على الرمز، يتأخر عادةً جيتسي عدة ثوانٍ للبدء، بعد أن تفتح النافذة سيظهر لكم رمز تشفير المحادثة. أنقروا عليه وتأكدوا من هوية الشخص الذي تتصلون به عبر رؤية الرمز مطابقاً لدى كليكما، بعد التأكد أنقروا على confirm وسيتم تشفير الاتصال سواء كان صوتياً فقط أو فيديو أو لمشاركة الشاشة.

بإمكانكم أيضاً استخدام شبكة جيتسي لإجراء جميع أنواع المحادثات المشفرة المتوفرة في الشبكات الأخرى. لإنشاء حساب على شبكة جيتسي، توجهوا إلى موقع jit.si وسجلوا حساباً خاصاً بكم.

بعد الانتهاء من إدخال البيانات، اذهبوا إلى برنامج جيتسي وانقروا على file ثم add new account
قوموا باختيار بروتوكول XMPP وأدخلوا بياناتكم، لا تنسوا أن تضعوا بعد اسم المستخدم عنوان سيرفر جيتسي @jit.si

الآن بإمكانكم إضافة عناوين جهات الاتصال الخاصة بأصدقائكم على شبكة جيتسي وإجراء محادثات نصية وصوتية وفيديو ومشاركة الشاشة بشكل آمن ومشفر.

لإزالة أحد الحسابات أو تعطيله مؤقتاً توجهوا إلى قائمة Tools ثم Options
توجهوا إلى تبويب Accounts
لإزالة الحساب نهائياً من البرنامج وحذفه قوموا بالنقر على الحساب ثم اختيار Delete
أو لإيقاف الحساب مؤقتاً (تسجيل الخروج) قومو بإزالة التحديد عنه وأغلقوا النافذة

يرجى الانتباه أيضاً إلى أنه عليكم ألا تسمحوا لجيتسي بتذكر كلمة المرور، حتى ولو كان يقوم بتشفيرها، فربما استطاع أحدهم الوصول إلى جهازكم وسرقة ملف الإعدادات الذي يحتوي كلمة المرور المشفرة، بالتالي يستطيع تسجيل الدخول إلى حسابكم من دون الحاجة إلى معرفة كلمة المرور.

بإمكانكم مشاهدة الفيديو التالي الذي يشرح طريقة تنصيب وإعداد جيتسي