cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

العدد ٦ | يوليو/تموز ٢٠١٣

خدمة تور المخفية

الهواتف الفضائية

إعداد التحقق بخطوتين في حساباتنا

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 السادس من مجلة «سايبر آرابز». كالعادة، نحاول أن نقدم إليكم أخبار ونصائح تساعدكم على حماية خصوصيتكم والتواصل بشكل أكثر أمناً عند استعمال الإنترنت.
يراودنا جميعاً قلق كبير من قيام أحد باختراق حساباتنا على الإنترنت، سواء كانت حسابات جيميل أو فيس بوك أو تويتر، أو أي حساب آخر نتواصل من خلاله مع العالم. لا تكفي كلمات المرور وحدها لتضمن أن لا أحد يتجسس على رسائلنا الخاصة.

لذا، هناك عدد متزايد من المواقع التي تقدم مستوى إضافياً من الحماية: التحقق من الهوية بعدة خطوات. يشرح فريق «سايبر آرابز» في هذا العدد ما هي هذه العملية، كيف تعمل وكيف تحميكم وتحمي حساباتكم. عند تطبيق هذه العملية، سيكون من الصعب جداً على أي أحد غيركم أن ينفذ إلى حساباتكم.

في هذا العدد أيضاً، نلقي نظرة متعمقة على الأمن (أو غيابه) عندما تستخدمون الهاتف الفضائي. في بعض الأحيان، قد لا تمتلكون خياراً آخر غير استعمال هذا النوع من الهواتف، ولكن على الأقل يجب أن تعوا المخاطر المترتبة على هذا الأمر والتدابير الواجب اتخاذها قبل الاتصال بالأقمار الصناعية الموجودة في الفضاء.

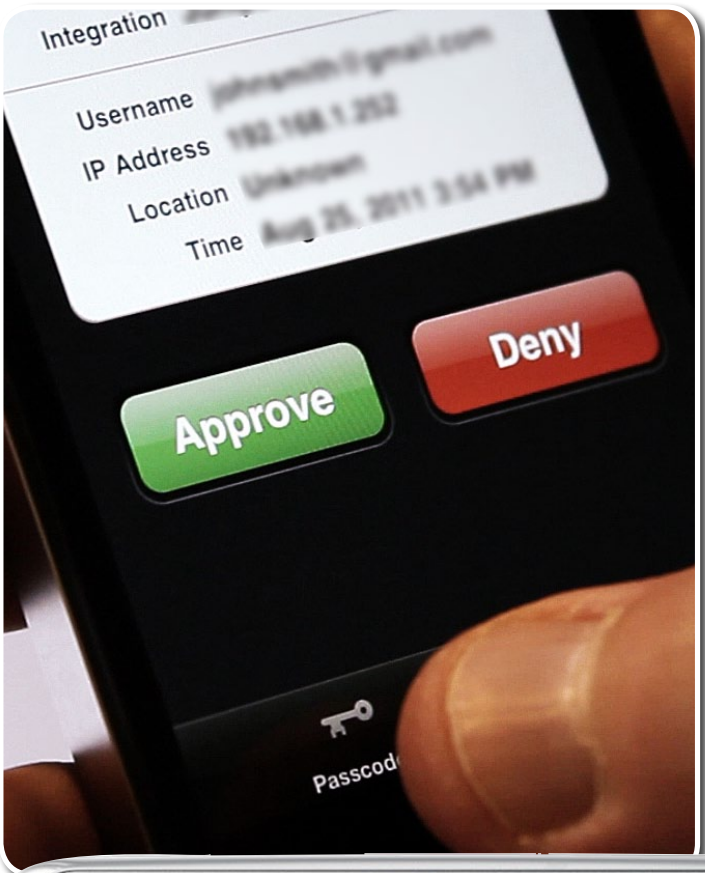
بالمناسبة، صفحة «سايبر آرابز» على فيس بوك لديها الآن أكثر من ٢٨,٠٠٠ معجب، أغلبهم من العالم العربي، وهذا الرقم يشعرنا بالسعادة والفخر أيضاً، حيث يبدو أننا على الطريق الصحيح فيما يتعلق بالخدمات التي نقدمها إلى متابعينا.

ملاحظة أخرى: ترقّبوا في الأسابيع القادمة منشورات جديدة رائعة على موقع «سايبر آرابز». ستلتقون عارف وبرهان، وهما شخصيتان فريدتان من نوعهما. سيقودكم عارف وبرهان خلال متاهة التواصل عبر الإنترنت، ونأمل أن تساهم مغامراتهما في تحسين أمنكم الرقمي، فتعرفوا عليهما وشاركوا قصتهما على نطاق واسع.

مع أفضل التمنيات من فريق «سايبر آرابز»

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

استخدام «التحقق بخطوتين» لحماية حساباتكم الشخصية من الاختراق



نقوم في «سايبر آرابز» بالتأكيد دائماً على استخدام كلمات سر طويلة وصعبة لحماية حسابات المستخدمين على فيس بوك من الاختراق. وقد مرّت علينا عدة حالات حيث تعرض المستخدمون للمتاعب جراء اختراق حساباتهم.

كلمات السر الطويلة والمعقدة ستساعد في إبعاد المخترقين عن حساباتنا (تستطيعون مراجعة مقالنا عن نصائح لكلمات سر قوية المنشور سابقاً هنا).

ولكن حتى وإن قمنا بإنشاء كلمات السر الطويلة والمعقدة، فإن إمكانية الحصول عليها أو تخمينها ليس مستحيلاً، لذا سيكون من الجيد أن نقوم بحماية حساباتنا عبر طرق أكثر أمناً من كلمات السر. لحسن الحظ، فإن العديد من المواقع توفر لنا هذه الحماية عن طريق تقنية تسمى «Two-factor Authentication» أو «عملية التحقق بخطوتين».

تستلزم هذه العملية الطلب منكم إدخال رمز إضافي بعد إدخالكم كلمة السر والتحقق منها. هذا الرمز السري سيتم إرساله إلى رقم هاتفكم الجوال في كل مرة تقومون بتسجيل الدخول من جهاز أو متصفح أو مكان جديد.

استخدام كلمة سر صعبة إضافة إلى اعتماد عملية التحقق بخطوتين يجعل قابلية اختراق حسابكم شبه مستحيلة، إلا إذا استطاع المخترق الحصول على كلمة السر الخاصة بكم بالإضافة إلى الاستحواذ على هاتفكم الجوال، وهذا نادر الحدوث. لكن أيضاً لهذه العملية مساوؤها، ففي حال ضياع هاتفكم الجوال، لن تعودوا قادرين على استعادة حسابكم، وسيتوجب عليكم أن تقومو بتسجيل الدخول من جهاز أو مكان قمتم بتسجيل الدخول منه سابقاً، فلا تضطرون إلى إدخال الرمز السري مجدداً. لذا، يجب علينا أن ننتبه إلى النقاط السابقة حين نقوم بتفعيل عملية التحقق بخطوتين.

تجدر الإشارة إلى أنه في بعض الدول – سوريا مثلاً – فإن الرسائل النصية القصيرة لا تصل دائماً، لذا يتوجب علينا أن نحاول عدة مرات حتى يتم الأمر بنجاح.

إعداد التحقق بخطوتين في «فيس بوك»

لإعداد الخدمة وتفعيلها نقوم بالنقر على رمز الدولاب في الأعلى > إعدادات الحساب ثم الذهاب إلى تبويب «أمان» من القائمة اليسرى. (أو من هنا).

تحت خانة «الموافقات على تسجيل الدخول» نقوم بتحديد «طلب رمز أمان للوصول إلى حسابي من متصفحات غير معروفة».

ستفتح نافذة جديدة، تشرح لنا ما هو الـ «تحقق بخطوتين» كما تقوم بالتأكد من أننا نريد حقاً تفعيل الخدمة، قوموا بالنقر على "الشروع في العمل".

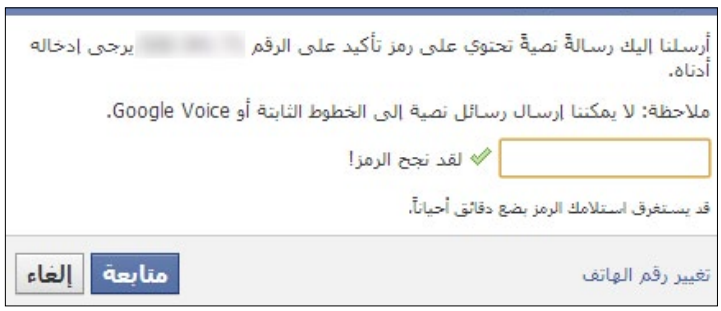
في النافذة التالية، سيقوم فيس بوك بسؤالكم عن اسم المتصفح الذين تقومون باستخدامه الآن لإضافته إلى قائمة المتصفحات الموثوقة.

في النافذة التالية سيقوم فيس بوك بسؤالكم إن كنتم تمتلكون جهاز آيفون أو أندرويد، أم تملكون نوعاً آخر من الأجهزة.

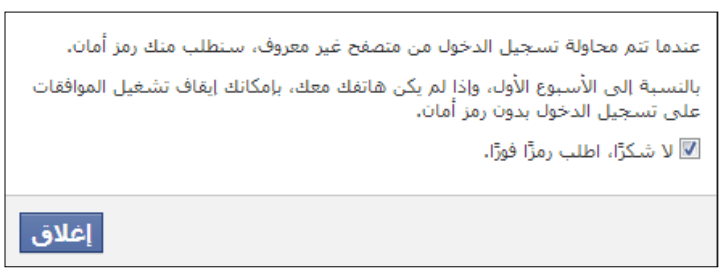
يرجى الانتباه إلى أنه في حال قمتم باختيار الخيار الأول «جهاز آيفون أو أندرويد» سيقوم فيس بوك بطلب عدة خيارات تنتهي بطلب تحميل تطبيق على جوالكم؛ هذا التطبيق، سواء كان للأندرويد أو الآيفون فإنه محجوب في بعض الدول بسبب العقوبات التجارية عليها (مثل سوريا، السودان).

أما في حال قمتم باختيار «غير ذلك» ستظهر لكم نافذة تطلب منكم تأكيد كلمة السر؛ قوموا بإدخالها ثم بالنقر على «تقديم».

بعد إعادة إدخال كلمة السر وإرسالها، سيتم طلب إدخال رقم هاتفك الجوال، قوموا باختيار الدولة من القائمة ثم أدخلوا رقم هاتفكم الجوال من دون إدخال الرمز الدولي. بعد إتمام هذه الخطوة والضغط على إرسال، إن تمت كل الخطوات بشكل صحيح، سيتم إرسال رسالة نصية قصيرة (SMS) إلى هاتفكم الجوال خلال دقيقة عادةً، تحتوي على رمز سري للتحقق من أن هذا الرقم يعود لك، قم بإدخال الرمز السري واضغط على «متابعة».



بعد النقر على «إرسال»، سيقوم فيس بوك بسؤالكم إن كنتم ترغبون بتفعيل تسجيل الدخول بدون إجباركم على استخدام التحقق بخطوتين لأول أسبوع فقط، الأفضل أن نختار «لا شكراً، اطلب الرمز فوراً».



بذلك نكون قد قمنا بتفعيل خدمة التحقق بخطوتين، مما يعني أن فيس بوك سيقوم بإرسال رسالة نصية إلى هاتفنا الجوال في كل مرة نقوم بتسجيل الدخول من جهاز أو مكان جديد، أو في حال قام أحد آخر بمحاولة الدخول إلى حسابنا.

في حال ضياع هاتفنا الجوال، علينا أن نقوم بتسجيل الدخول عبر أحد الأجهزة التي قمنا بتسجيل الدخول منها سابقاً لتغيير الإعدادات.

تستطيعون مشاهدة قائمة بالأجهزة التي تم تسجيل الدخول منها عبر النقر هنا وتأكدوا من أنه لا يوجد أي من الأجهزة التي استخدمتموها سابقاً لتسجيل الدخول في مقاهي الإنترنت والأماكن العامة.

إعداد التحقق بخطوتين في «جيميل»

١- نقوم بالذهاب إلى موقع www.gmail.com
٢- بعد تسجيل الدخول، نقوم بالنقر على الصورة في أعلى اليسار > الحساب Account
٣- نذهب إلى تبويب الأمان ثم النقر على «إعدادات» أسفل «عملية التحقق بخطوتين»، سيقوم بطلب كلمة السر منا... ندخلها ثم ننتقل إلى الصفحة التالية

٤- نقوم بالنقر على «بدء الإعداد»
٥- الخطوة الأولى: نقوم بإدخال رقم الهاتف بعد تحديد الدولة، ثم نقوم بتحديد الطريقة التي سيقوم غوغل بالتحقق منها (إرسال رسالة نصية أو اتصال هاتفي)

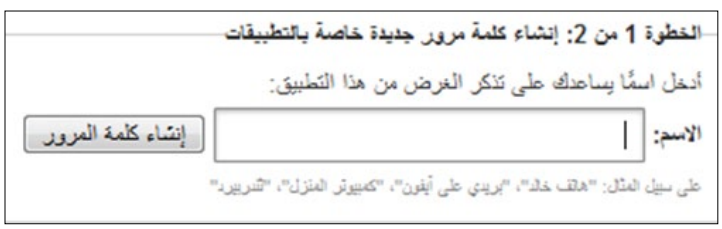
٦- الخطوة الثانية: نقوم بإدخال رمز التحقق الذي تم إرساله (أو إخبارك به عن طريق الاتصال) إلى هاتفنا ثم ننقر على «تأكيد»

٧- الخطوة الثالثة: نستطيع التأشير على «جعل هذا الكمبيوتر موثوقاً» لعدم المطالبة برمز التحقق في كلّ مرة نقوم بتسجيل الدخول من هذا الكمبيوتر. ثم ننقر على التالي
٨- الخطوة الرابعة: انتهينا، نقوم بالنقر على «تأكيد»
٩- سيقوم الموقع بإعادة طلب كلمة السر مجدداً، نقوم بإدخالها والانتقال إلى صفحة الإعدادات الخاصة بعملية التحقق من خطوتين.

> نصيحة: نستطيع إضافة رقم ثاني لشخصٍ نثق به (أهل، أصدقاء) أو رقمنا الثاني إن كنا نملك واحداً، في حال تمت سرقة هاتفنا أو ضياعه أو وقوعه في أيدٍ غير أمينة، نستطيع من خلاله الدخول إلى حسابنا.

إعداد كلمات سر للبرامج (مثل Thunderbird)

١- نقوم بالنقر على «إدارة كلمات السر الخاصة بالتطبيقات، سيطلب إدخال كلمة السر مجدداً، بعد إدخالها ننتقل إلى الصفحة التالية
٢- نقوم بإدخال اسم البرنامج (Thunderbird - الاسم فقط لنتذكره) ثم النقر على «التالي»



٣- نقوم بنسخ كلمة السر (من دون المسافات) واستخدامها في البرنامج بدلاً من كلمة السر المعتادة.

في حال لم نكن فعّلنا خيار «تذكر كلمة السر» في التطبيق المستخدم، فإننا في المرات التالية لأول استخدام، سنقوم بإدخال كلمة السر المعتادة. أي أن هذه الخطوة هي فقط لإعطاء الوثوقية للبرنامج في المرة الأولى

Gmail™

قائمة الرموز الاحتياطية

نقوم بالنقر على إظهار الرموز الاحتياطية
يتم استخدام «قائمة الرموز الاحتياطية» في حال كنا في مكان لدينا إمكانية الوصول إلى الإنترنت لكن لا تتوفر فيه تغطية شبكة الخليوي، ونحتاج الدخول إلى بريدنا الإلكتروني حيث يمنع استخدام الهواتف النقالة.

٢- نقوم بطباعة الرموز العشرة على ورقة، أو حفظها في مكان آمن.
كل رمز من هذه الرموز العشرة صالح للاستخدام لمرة واحدة فقط

٣- في حال قمنا باستخدام الرموز كلها نستطيع النقر على «إنشاء رموز جديدة» لإنشاء عشرة رموز جديدة.

التفعيل على أجهزة الموبايل

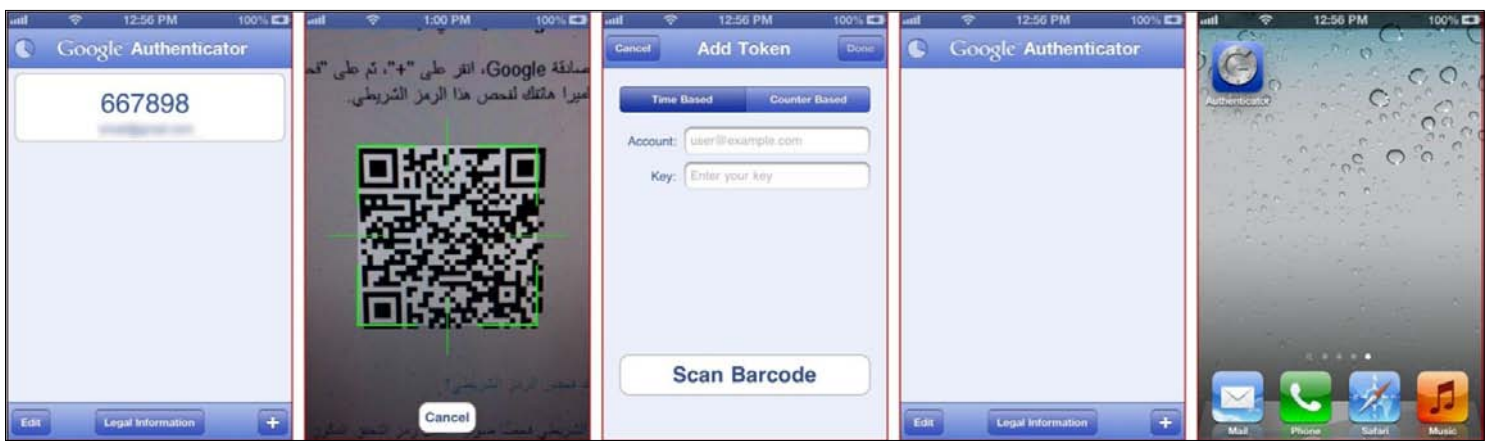
لتفعيل الرموز على أجهزة الموبايل (iPhone, Android, Blackberry)

نقوم بالنقر على نوع هاتفنا النقال ثم النقر على تحميل برنامج Google Authenticator (في حالتنا هنا نقوم بالتجربة على جهاز iPhone لذا ستظهر لدينا عبارة: «تنزيل البرنامج من App store»)

١- نبقي الصفحة مفتوحة على جهاز الكمبيوتر، بعد تحميل البرنامج على هاتفنا النقال سيكون شكله كما في الصورة رقم ١
٢- ننقر على رمز «+» (الصورة رقم ٢)
٣- ننقر على «Scan Barcode» (الصورة رقم ٣)

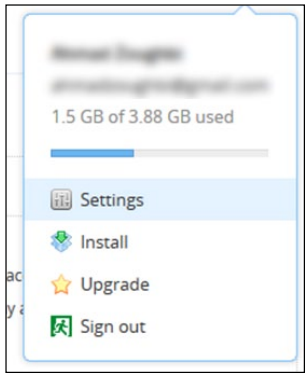
٤- نقوم بضبط وضع الكاميرا كما في الصورة رقم (٤)، ستقوم الكاميرا بأخذ الصورة تلقائياً
٥- قم بنسخ الرمز المؤلف من ستة أرقام وإدخله في الصفحة التي قمنا بتصويرها (الكمبيوتر) لإضافة هاتفنا النقال كجهاز موثوق

أخيراً، بعد إتمام هذه العملية، في كلّ مرة نقوم بتسجيل الدخول فيها إلى جهاز جديد، نستطيع الحصول على الرمز إما عن طريق برنامج Google Authenticator الذي يقوم بتوليد رمز جديد كل ٣٠ ثانية، أو بالاعتماد على وصول الرمز برسالة نصية SMS أو باتصال هاتفي.

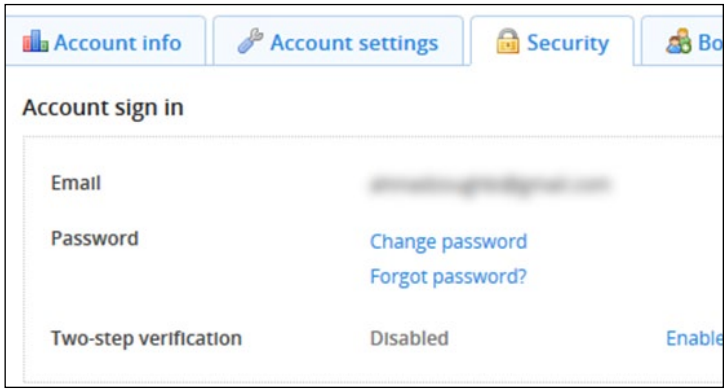


صورة رقم ١ | صورة رقم ٢ | صورة رقم ٣ | صورة رقم ٤ | صورة رقم ٥

إعداد التحقق بخطوتين في «دروب بوكس»



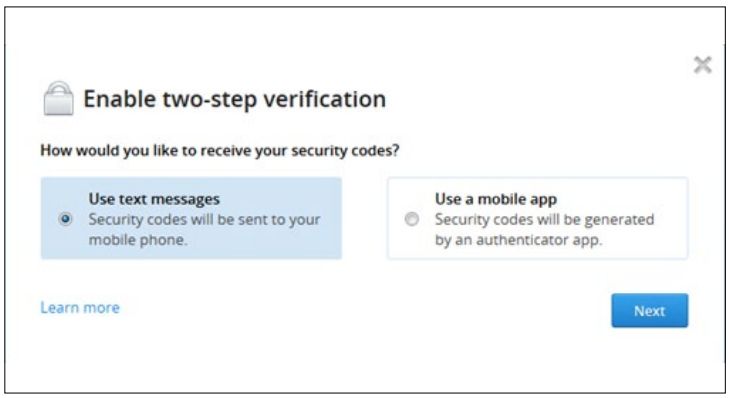
لإعداد الخدمة وتفعيلها، نقوم بتسجيل الدخول إلى موقع دروب بوكس، ثم نقوم بالنقر على السهم الموجود بجانب اسمنا في الأعلى واختيار Settings ثم النقر على تبويب Security، ثم النقر على Enable.
تظهر لنا نافذة منبثقة، نقوم بالنقر على Get started ثم نقوم بإدخال كلمة السر والنقر على Next.



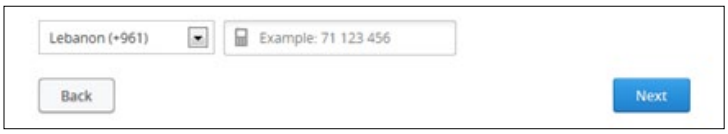
في النافذة التالية لدينا خياران:

1– Use text messages:

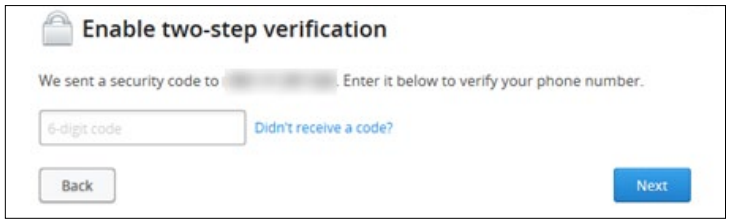
هذا الخيار سيقوم بإرسال الرمز السري إلى رقم هاتفنا النقال، ولكن تجدر الإشارة إلى أن هناك عدد من الدول ليست مدرجة ضمن القائمة المسموح بالتفعيل لها، ومنها سوريا.
للمتابعة نقوم باختيار Use text messages ثم النقر على Next



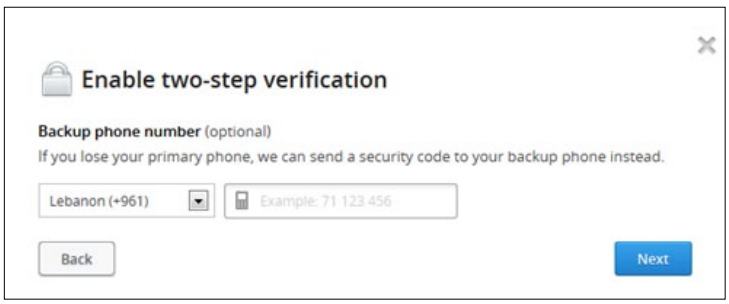
نقوم باختيار الدولة ثم نُدخِل رقم هاتفنا النقال والنقر على Next



ستصلنا رسالة نصية قصيرة SMS على هاتفنا النقال تحتوي على رمز مؤلف من ٦ أرقام، نقوم بإدخال هذا الرمز في النافذة التالية ثم نضغط على Next



في النافذة التالية، يتيح لنا موقع دروب بوكس إضافة رقم هاتف إضافي في حال قمنا بإضاعة الهاتف أو تمت سرقته، نستطيع تلقي الرمز السري على الرقم الآخر، ولكن هذا الخيار ليس إجبارياً، نستطيع إدخال رقم هاتف إضافي، أو تخطيه والنقر على Next.



سيظهر لنا في النافذة التالية رمزاً سرياً مؤلفاً من ١٦ حرفاً، نقوم بنسخه وحفظه في مكانٍ آمن، في حال فقدنا إمكانية الوصول إلى هاتفنا النقال ونريد تسجيل الدخول نستطيع استخدام هذا الرمز ولمرة واحدة فقط.

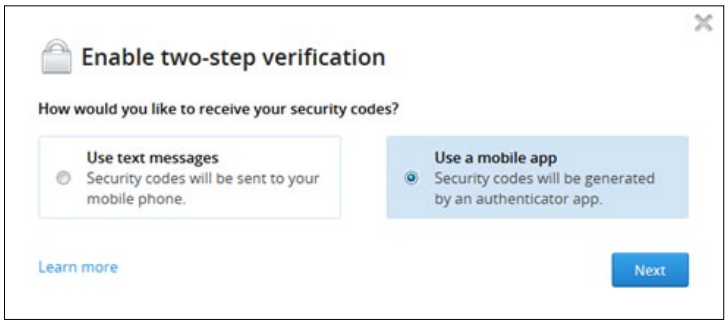
بعد التأكد من حفظ الرمز نقوم بالنقر على Enable two-step verification ثم نقوم بالنقر على done.

Dropbox

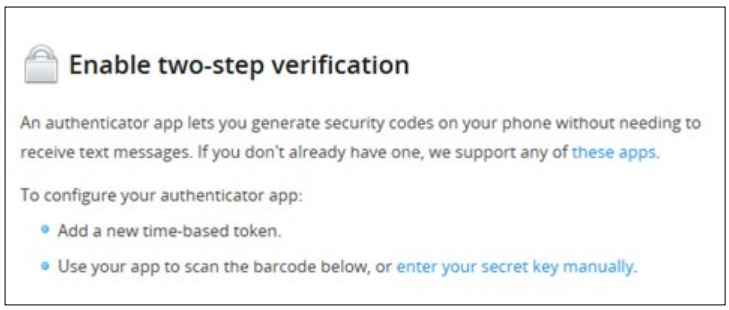
٢- Use a mobile app

هذه الطريقة لا تتطلب إدخال رقم هاتف وإنما تنصيب تطبيق يقوم بالمهمة، يستطيع المستخدمون في الدول المحظورة مثل سوريا استعمالها، وهي تعمل على كل من أجهزة آيفون وآيباد وأندرويد وبلاك بيري وويندوز فون.

للبدء نقوم باختيار Use a mobile app ثم النقر على Next



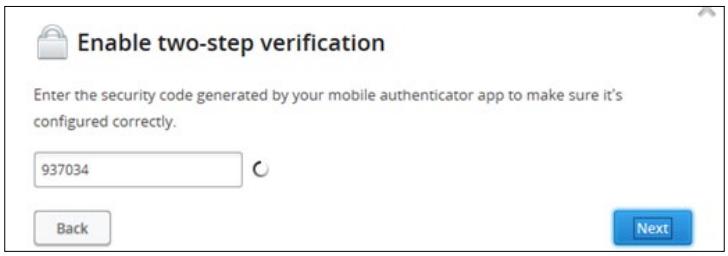
قوموا بالنقر على these apps أو من هنا لاختيار التطبيق المناسب لنظام تشغيل هاتفكم النقال وتنصيبه.



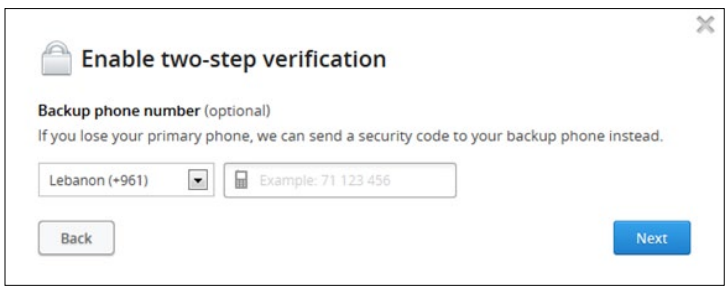
بعد إتمام عملية تنصيب التطبيق نقوم بتشغيله وجعله يقوم بتصوير المربع المشار إليه في الصورة، سيقوم التطبيق بعد إتمام العملية بتوليد رمز سري جديد كل دقيقة.

بعد إتمام عملية تصوير المربع نقوم بالضغط على Next

نقوم بفتح التطبيق الذي يولّد الرمز السري ونقوم بإدخال الرمز، ثم النقر على Next

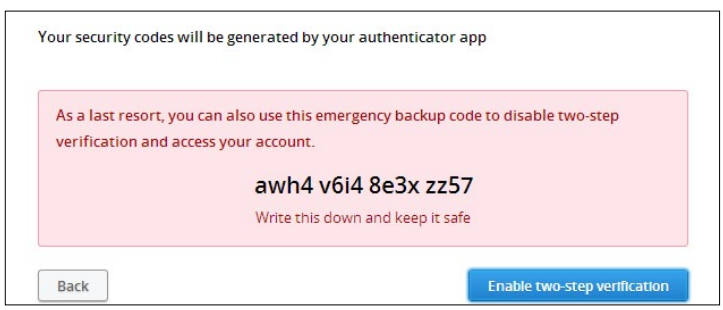


كما نستطيع في النافذة التالية إدخال رقم هاتف إضافة الى التطبيق لاستقبال الرمز السري عليه، يمكننا تخطيه عبر النقر على Next



في النافذة التالية نقوم بنسخ الرمز السري المؤلف من ١٦ حرفاً وحفظه في مكانٍ آمن، في حال فقدنا إمكانية الوصول إلى هاتفنا النقال ونريد تسجيل الدخول نستطيع استخدام هذا الرمز ولمرة واحدة فقط. ثم ننقر على Next.

في النافذة التالية نقوم بالنقر على Enable two-step verification.

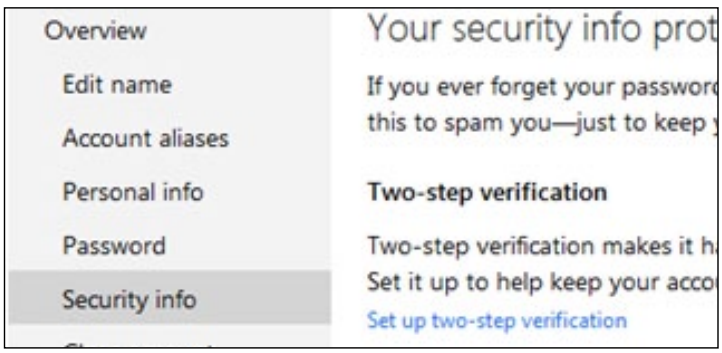


بهذه الطريقة قمنا بتفعيل التحقق بخطوتين ونستطيع تأمين ملفاتنا الموجودة على دروب بوكس من وقوعها في يد أحد مالم يستطيعوا أن يحصلو على كلمة السر والهاتف النقال الذي تستخدمه للتحقق، وهذا أمر نادر الحدوث.

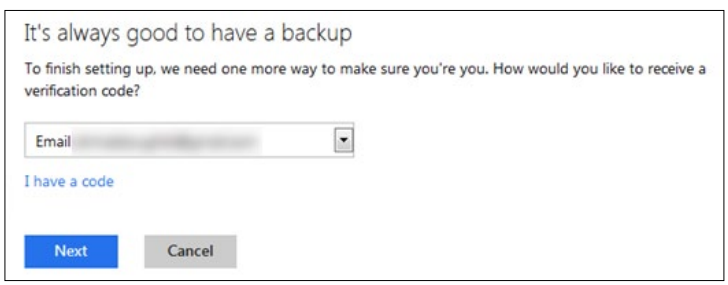
Microsoft

إعداد التحقق بخطوتين في «مايكروسوفت»

نقوم بتسجيل الدخول إلى حسابنا في مايكروسوفت (أو هوتميل كما هو متعارف عليه)، ثم الذهاب إلى تبويب Security info والنقر على Set up two-step verification.



نقوم بالنقر على Next، في الخطوة التالية سيطلب التحقق من أنه نحن من نقوم بهذه العملية، لذا سيطلب إرسال رمز سري إلى بريدنا الإلكتروني الاحتياطي، نقوم باختيار البريد الذي قمنا بإدخاله أثناء إنشائنا الحساب ثم نضغط على Next،

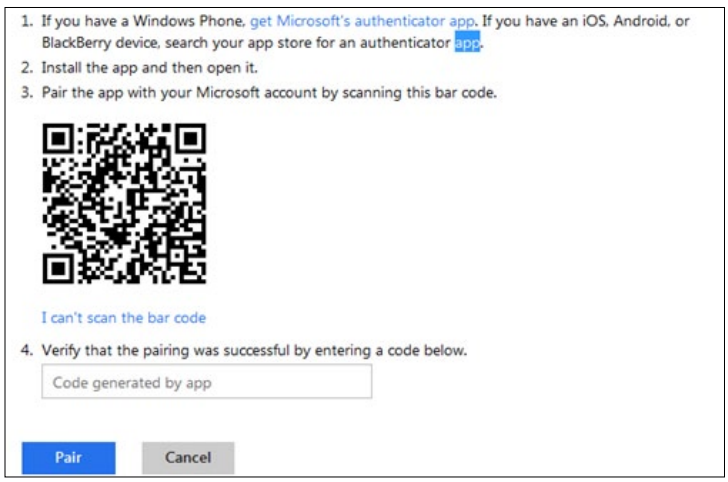


ستصلنا رسالة بريد إلكتروني خلال دقائق تحتوي على رمز مؤلف من ٤ أرقام، نقوم بنسخ الرمز وإدخاله في النافذة التالية ثم نقوم بالنقر على Next ثم Done.

بهذه العملية قمنا بتفعيل التحقق بخطوتين لبريدنا الإلكتروني على مايكروسوفت، ولكن في بعض الأحيان قد لا تتوفر شبكة خليوي ونريد تسجيل الدخول إلى بريدنا الإلكتروني، لذا نستطيع عبر الرجوع إلى صفحة Security info النقر على Set up تحت العنوان Authenticator app.

تفتح لنا نافذة فيها مربع، نقوم بتحميل تطبيق Authenticator لنظام التشغيل ويندوز فون من هنا أما بالنسبة لأجهزة آيفون وأندرويد وبلاك بيري نستطيع الدخول إلى متجر التطبيقات الخاص بكلّ واحد فيهم والبحث عن Authenticator وتنصيبه.

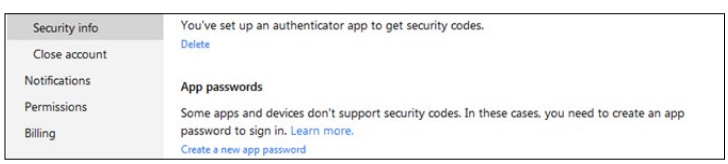
بعد إتمام عملية التنصيب نقوم بفتح التطبيق وجعله يقوم بتصوير المربع الظاهر في الصورة:



سيولّد التطبيق رمزاً سرياً كل دقيقة، نقوم بنسخ الرمز ووضعه في الحقل المخصص له ثم النقر على Pair.

بهذه العملية عندما نقوم بتسجيل الدخول ويطلب الرمز السري، بينما لا تتوفر شبكة في الهواتف النقالة، ولكن يوجد انترنت، نستطيع الحصول على الرمز السري عبر التطبيق وإدخاله.

في حال كنا نريد استخدام بريدنا الإلكتروني عبر برنامج معيّن مثل Thunderbird، يجب علينا إعداد كلمة سر خاصة بالبرنامج، وذلك عبر الذهاب إلى App passwords والنقر على Create a new app password من صفحة Security info.



في الصفحة التالية سيقوم الموقع بتوليد كلمة سر عشوائية، نقوم بنسخها وإدخالها في البرنامج الذي نريد استخدامه، إذا كنا نريد استعمال أكثر من برنامج، يجب علينا توليد كلمة سر عشوائية لكل برنامج، أي أننا لا نستطيع استخدام كلمة السر ذاتها لعدة برامج، كما أنه لا يمكننا استعراضها، لذا يجب علينا تذكر هذه الكلمة من الصفحة، أو أننا سنضطر إلى إلغائها وتوليد كلمة جديدة.

ويندوز إكس بي... وداعاً!

أعلنت شركة مايكروسوفت أنها ستتوقف عن دعم ويندوز إكس بي. عملياً، تعني هذه الخطوة أنه اعتباراً من تاريخ ٨ أيار / مايو ٢٠١٤، لن تقوم مايكروسوفت بتزويد مستخدمي ويندوز إكس بي بأية تحديثات أمنية.

لا يعتبر هذا الإعلان مفاجئاً، خاصة أن نظام التشغيل المذكور قد ناهز عمره االأحد عشر عاماً، ومستخدمي هذا النظام قد فوتوا على أنفسهم ثلاث نسخ أحدث وهي ويندوز فيستا، وويندوز ٧ وويندوز ٨، لكن المفاجئ أن أكثر من ٣٨٪ من مستخدمي أجهزة الحاسوب لا زالوا يعتمدون على ويندوز إكس بي! وربما تكون النسبة أكثر من ٣٨٪ من المستخدمين في الدول العربية.

تعدّ التحديثات الأمنية جزءاً مهما بل ومصيرياً لاستمرار استخدام أي نظام تشغيل، وبدون وجود التحديثات الأمنية ستعرضون أنفسكم لخطر الاختراق بسهولة كبيرة، لأن المخترقين سيكونون قادرين على استغلال الثغرات الأمنية التي لم يتم إصلاحها.

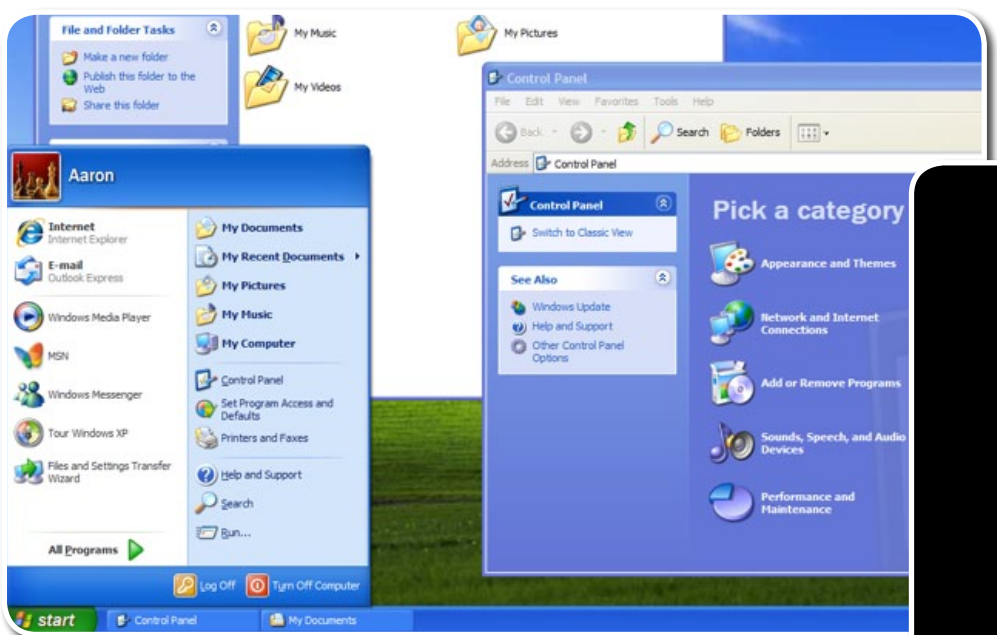
لهذا السبب، نصيحتنا لمستخدمي ويندوز إكس بي واضحة جداً: التحديث!، وإن لم يكن ويندوز ٧ أو ويندوز ٨ محبباً لكم، بإمكانكم استعمال لينوكس، فهو مجاني وآمن، وإن كانت هي المرة الأولى لكم في استخدام لينوكس، بإمكانكم البدء باستخدام Mint Linux أو للأشخاص المهتمين بالأمان يستطيعون استخدام TAILS، على كل حال، ضعوا في الحسبان دائماً أن البرامج التي كانت تعمل على ويندوز إكس بي لن تعمل على البيئة الجديدة لينوكس في حال قررتم الانتقال إليه.

ولكن تجدر الإشارة إلى أن المخاطر الأمنية ليست حكراً على ويندوز إكس بي فقط، فمالكو النسخ المقرصنة من بقية نسخ ويندوز هم معرضون لذات المخاطر، لأن تحديثات ويندوز غالباً لا تعمل بشكل صحيح.

إذا كنتم ترغبون بالتأكد من عمل هذه التحديثات بشكل صحيح أنقروا على:

إبدأ > لوحة التحكم > النظام والأمان > تحديثات ويندوز

ومن هناك تأكدوا من أن تحديثات ويندوز تم تفعيلها.



إعداد خدمة تور المخفية لمشاركة الملفات

يصلنا في سايبر «آرابز» العديد من الأسئلة حول كيفية إعداد موقع انترنت آمن ومجهول الهوية لمشاركة المستندات والملفات، أو لاستضافة صفحة للمعلومات. قمنا مؤخراً بكتابة مقال عن مزودي خدمة استضافة المواقع المجانية هنا. لكن هناك طريقة أخرى لإنشاء موقع لكم على الانترنت يكون آمناً ومجهول الهوية، وهي Tor hidden service أو «خدمة تور الخفية»، وهي تعمل مباشرة من على جهازكم. خدمة Tor hidden service تم إنشاؤها بمساعدة الأداة المعروفة في التخفي والتصفح الآمن «تور».

ماذا تفعل هذه الخدمة؟

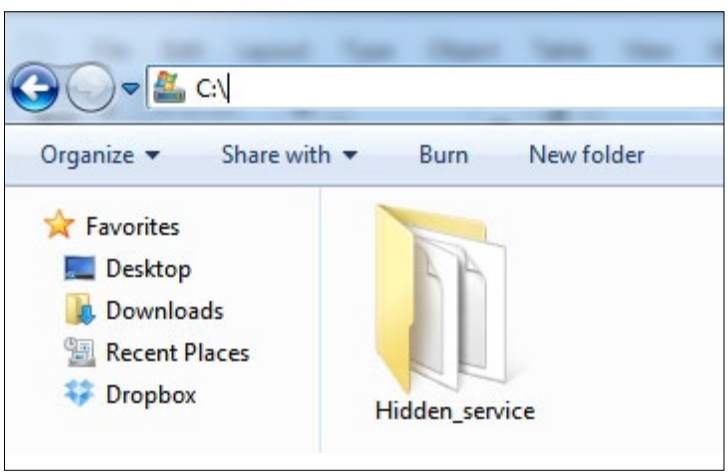
تقوم هذه الخدمة بإنشاء خادم (سيرفر) على الانترنت يعمل مباشرةً على جهازكم ويتم الوصول إليه عبر شبكة تور، ما يعني أن مكان تواجد حاسوبكم سيكون مجهولاً ١٠٠ بالمئة، وإمكانية الوصول للملفات التي تودون مشاركتها ستكون متاحة فقط لمن يستخدم برنامج تور. بإمكان خادم الإنترنت المحلي الموجود على جهازكم أن يشير إلى أي مجلد حيث تحتفظون بملفات مخزنة يمكن مشاركتها، أو حيث وضعتم ملف من نوع index.htm يحتوي على صفحة إنترنت.

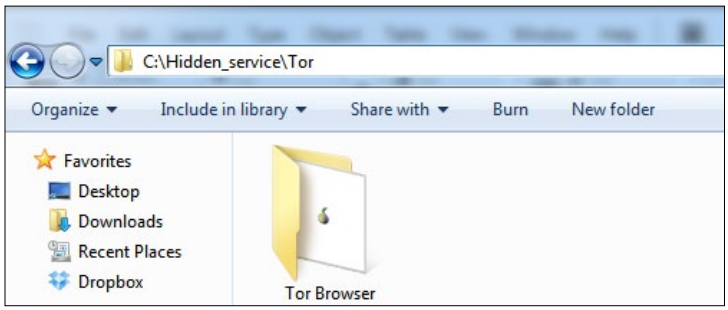
لجعل الموقع متاحاً عليكم اتباع الخطوات التالية:

١- إنشاء المجلد Hidden_service على القرص C

٢- تحميل نسخة Tor browser bundle من هنا ثم تنصيبها في المسار التالي: C:\Hidden_service\Tor

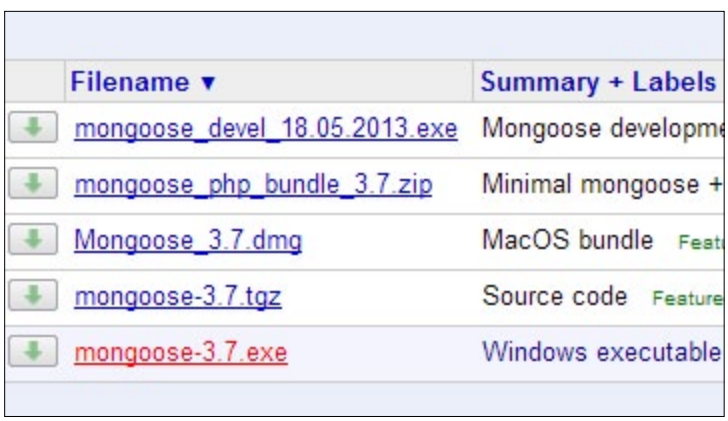
بعد إتمام هذه الخطوة، يمكنكم إنشاء خادمكم الشخصي، وتستطيعون استخدام أي نوع من الخوادم، مثل استضافة موقع يستخدم لغة البرمجة PHP ونظام قواعد البيانات MYSQL.





إذا وجدتم هذه الطريقة معقدة تستطيعون استخدام Mongoose webserver، ولكن قبل تنصيبه أنشئوا مجلداً اسمه index داخل المجلد hidden_service، هذا المجلد سيحتوي على ملفاتكم التي ستكون متاحة على الانترنت.

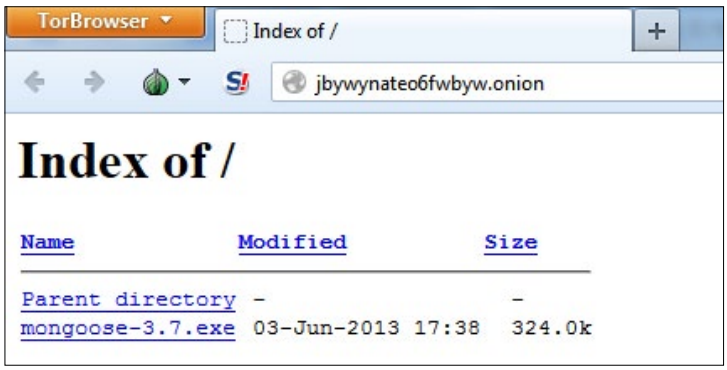
٣- قوموا بتحميل Mongoose webserver من هنا (أثناء التحميل اختاروا Windows executable إذا كنتم تستخدمون نظام التشغيل ويندوز) ثم قوموا بنقله إلى المجلد index



٤- أنقروا مرتين على الملف الذي قمتم بتحميله؛ ستظهر أيقونة ضفدع في شريط المهام حيث توجد الساعة

تشير هذه الأيقونة إلى أن برنامج Mongoose يعمل، إذا قمتم بفتح المتصفح والذهاب إلى العنوان التالي:
http://localhost:8080 ستظهر محتويات المجلد الذي أنشأتموه C:\Hidden_service\index

هذا المجلد متاح حالياً فقط من خلال جهاز حاسوبكم، ويجب إجراء بعض التعديلات لجعله متاحاً عبر شبكة تور.



٥- إبحثوا عن الملف "torrc" الموجود في المجلد الفرعي Data\ Tor في المجلد الذي قمتم بتنصيب تور فيه، في المثال الذي اتبعناه سيكون:

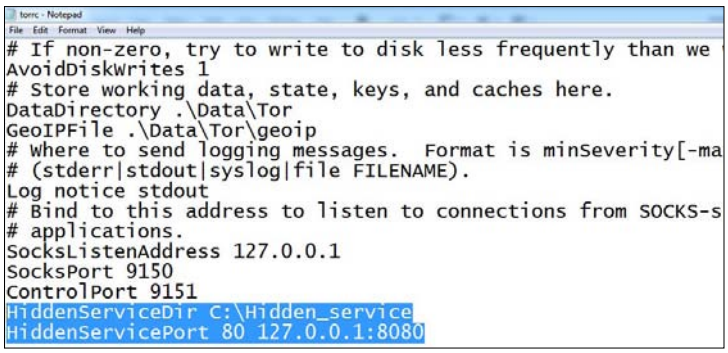
C:\Hidden_service\Tor\Tor Browser\Data\Tor

٦- افتحوا الملف باستخدام أي برنامج محرر للنصوص (المفكرة أو notepad)

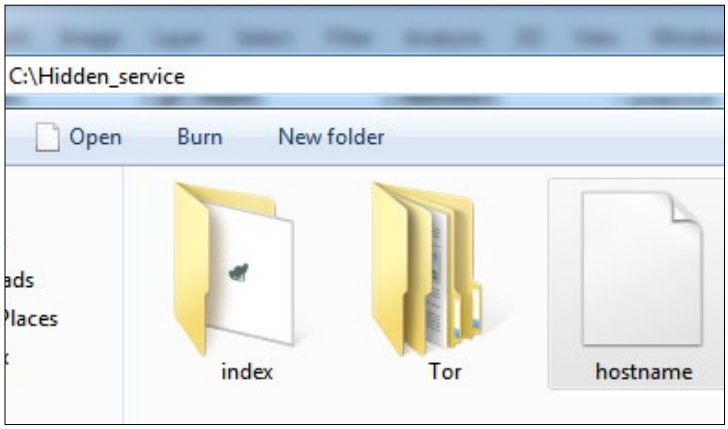
٧- أضيفواالسطرين التاليين

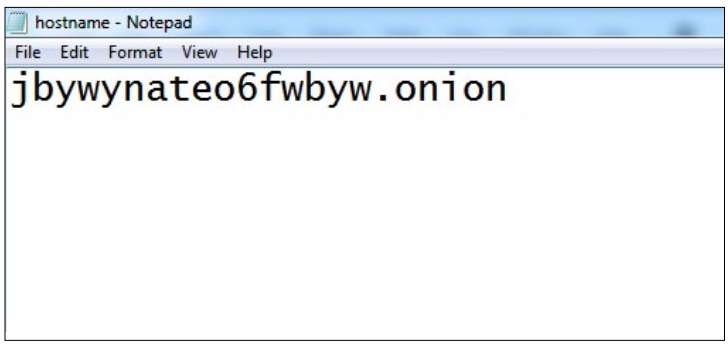
HiddenServiceDir C:\Hidden_service
HiddenServicePort 80 127.0.0.1:8080

عدلوا الاسم في حال كنتم قد اخترتم مكاناً آخر لتخزين المجلد Hidden_service



٨- الآن شغّلوا تور؛ ستلاحظون وجود ملفين جديدين في المجلد Hidden_service... افتحوا الملف hostname باستخدام محرر النصوص وستجدون سطراً مؤلفاً من مجموعة من الحروف والأرقام وتنتهي بـ onion.





هذا هو عنوان موقعكم على شبكة تور، وبإمكان أي شخص يستخدم تور ولديه هذا العنوان زيارته واستعراض الموقع أو الملفات التي قمتم بوضعها، فيمكنكم أن تتشاركوا هذا الموقع مع أصدقائكم. كل الملفات التي تضعونها داخل المجلد index ستكون متاحة عبر هذا العنوان الذي ينتهي بلاحقة .onion

٩- إذا أردتم أن تحصلوا على صفحة إنترنت بسيطة عوضاً عن الترتيب الذي يحتوي على مجلدات تستطيعون إنشاء صفحة انترنت عبر إنشاء ملف وورد Open Office أو Libre Office أو Microsoft Word وحفظ الملف باسم index.html حيث سيظهر للزائر محتويات هذا الملف تلقائياً حين زيارة رابط موقعكم الذي ينتهي بـ onion.

يمكنكم أن تغلقوا mongoose webserver أو tor أو كلاهما وتعيدوا تشغيلهما بقدر ما تريدون وسيبقى العنوان ثابتاً ولن يتغير.

بالطبع يجب أن يكون الحاسوب مشغلاً لإتاحة الوصول للآخرين إلى الملفات والمحتويات التي تريدون مشاركتها.

البرمجيات مفتوحة المصدر

ما هي البرمجيات المفتوحة المصدر؟

كثيراً ما نقوم في «سايبر آرابز» بدعم استعمال البرمجيات مفتوحة المصدر. في الحقيقة، نحن نفضّل استخدام البرمجيات مفتوحة المصدر على ما يسمى بالبرمجيات الاحتكارية، أي تلك التي تملكها جهة بعينها.

لكن السؤال: ماذا يعني أن تكون البرمجية مفتوحة المصدر؟

معظم الأشخاص يأتون على ذكر ميزة واحدة فقط: كونها مجّانية! وعلى الرغم من كون هذه نقطة إيجابية من دون شك، إلا أنها جزء بسيط وصغير جداً من ميّزات البرامج مفتوحة المصدر.

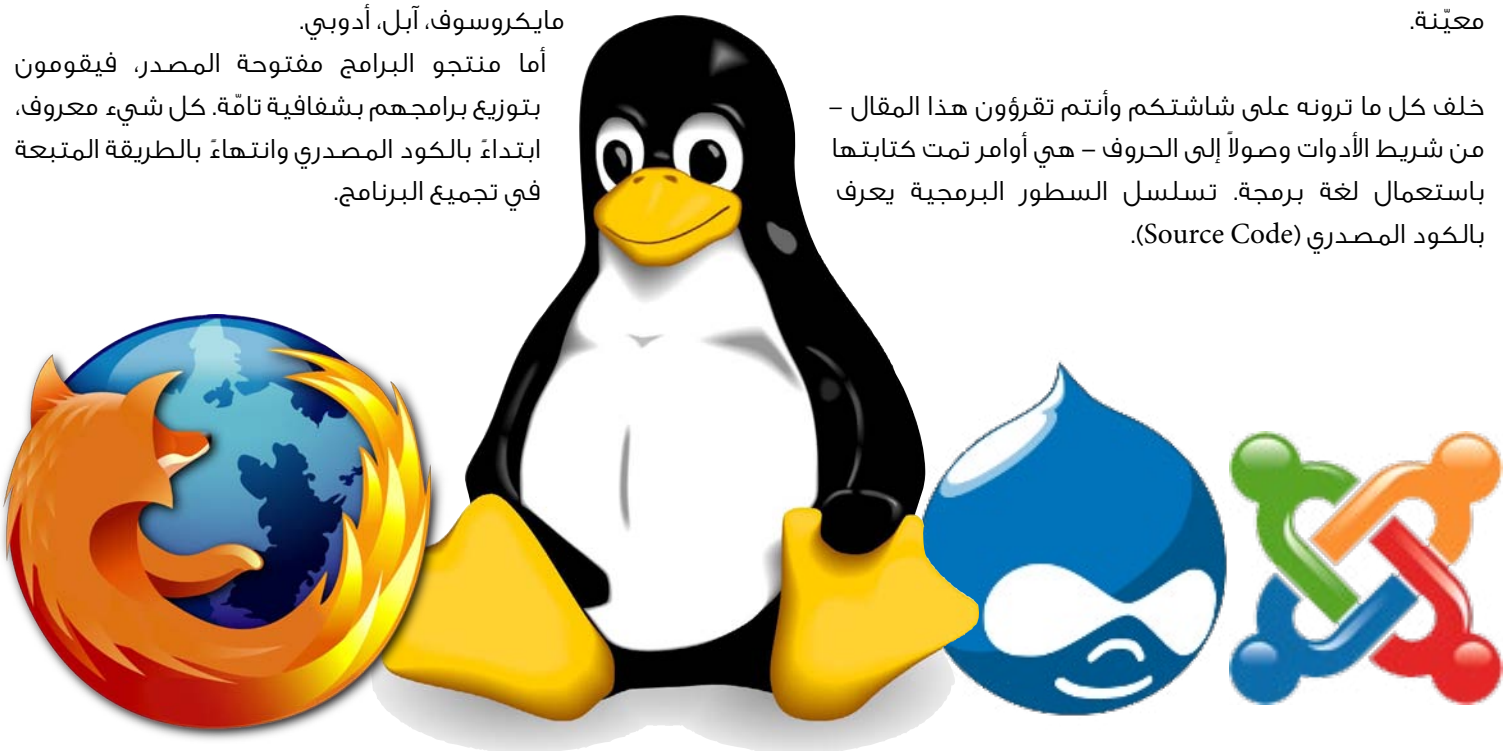
كل برنامج يعمل على الحاسوب، ابتداءً بنظام التشغيل ويندوز ومروراً بالمتصفح، تمت كتابته بلغة برمجة. يقوم صانعو البرمجيات بكتابة لغة برمجة لجعل الحاسوب أو نظام التشغيل يقوم بمهمة معيّنة.

خلف كل ما ترونه على شاشتكم وأنتم تقرؤون هذا المقال – من شريط الأدوات وصولاً إلى الحروف – هي أوامر تمت كتابتها باستعمال لغة برمجة. تسلسل السطور البرمجية يعرف بالكود المصدري (Source Code).

عندما ينتهي المبرمج من كتابة برنامجه، يقوم بتحويل لغة البرمجة المستخدمة – القابلة للقراءة والفهم من قبل الأشخاص – إلى لغة قابلة للقراءة من قبل الحاسوب. عملية التحويل هذه تسمّى بالتجميع أو Compilation، ونتيجة عملية التجميع تكون البرامج المتواجدة على جهازكم.

مالكو البرامج الاحتكارية ينشرون برامجهم فقط بعد انتهاء عملية التجميع، ما يعني أنه لا يمكن لأي أحد أن يعرف كيف تم إنشاء البرنامج، وما هي الأخطاء التي تم ارتكابها أثناء عملية البرمجة، أو حتى ما هي لغة البرمجة المستخدمة في كتابته. وغالباً ما يكون هناك سبب مادّي لعدم نشر الكود المصدري للبرنامج، والفكرة من وراء ذلك أنه إن أُتيح لأي شخص الوصول إلى هذا الكود المصدري، سيكون من المستحيل بيع البرنامج من قبل الشركات المعروفة في برمجياتها غير مفتوحة المصدر: مايكروسوف، آبل، أدوبي.

أما منتجو البرامج مفتوحة المصدر، فيقومون بتوزيع برامجهم بشفافية تامّة. كل شيء معروف، ابتداءً بالكود المصدري وانتهاءً بالطريقة المتبعة في تجميع البرنامج.



معظم البرامج مفتوحة المصدر لا يتم إنشاؤها عبر شركات، بل عبر مجموعة كبيرة من مبرمجي الحاسوب المتحمّسين حول العالم، الذين يقدمون وقتهم وخبرتهم لإنشاء البرامج بالتعاون فيما بينهم.

كل هذا لا يعني أن البرامج مفتوحة المصدر غير ربحية، فشركات مثل كانونيكال التي قامت بتطوير نظام التشغيل «أوبنتو» وغوغل التي قامت بتطوير نظام تشغيل الهواتف النقالة أندرويد، إضافة إلى المتصفح غوغل كروم، استطاعتا جني ملايين الدولارات عبر بيع البرامج مفتوحة المصدر وتسويقها ودعمها. هناك أيضاً برامج أخرى معروفة مثل المتصفح الأكثر انتشاراً فَيرفوكس، وبرنامجي الاتصال الآمن سايفون Psiphon وتور Tor، بالإضافة إلى ليبر أوفيس LiberOffice بديل مايكروسوفت أوفيس Microsoft Office.

من ميّزات البرمجيات مفتوحة المصدر أن آلية عملها شفافة تماماً، لذا إن قام المبرمج بارتكاب خطأ خلال كتابت برنامجه، فإن أي شخص يستطيع ملاحظة هذا الخطأ وإصلاحه، لأن غالباً ما يكون هناك آلاف الأشخاص يعملون على تطوير هذه البرامج، فالأخطاء تتم ملاحظتها وإصلاحها بسرعة. أما البرمجيات الاحتكارية، فغالباً ما يكون مطوروها قليلي العدد مما لا يسمح لهم بملاحظة جميع الأخطاء وإصلاحها بسرعة.

في أغلب الأحيان، يكون من الضروري وقوع خلل ما قبل أن تكون هناك إمكانية فعل شيء ما.

لهذا السبب، نلاحظ انتشار متصفحات مثل غوغل كروم وفَيرفوكس فيما يبتعد الكثيرون عن استخدام متصفح مثل إنترنت اكسبلورر، ببساطة لأن الأخير فيه العديد من الأخطاء التي لم يتم تحديدها مما يجعله غير آمنٍ للاستعمال.

أيضاً يمكن اعتبار الفرق بين البرامج مفتوحة المصدر وتلك الاحتكارية، كالفرق بين سيارة لا يمكن لأحد فتح غطاء محركها إلا عبر أخذها إلى الشركة المصنعة، وبين سيارة يمكن لأي أحد لديه الخبرة الكافية أن يفتح الغطاء.

لهذه الأسباب يوصي فريق «سايبر آرابز» باستخدام البرامج مفتوحة المصدر قدر الإمكان، خاصة البرامج التي تتعلق بأمان المستخدمين.

كما ننصح كافة المستخدمين عند رغبتهم بتحميل أي برنامج قراءة آراء المستخدمين (Reviews)، التي تتوفر كتعليقات على معظم مواقع التحميل مثل CNET وهذه النصيحة تنطبق على كافة البرامج سواء كانت مفتوحة المصدر أم احتكارية.

استعمال («راوتر») وشبكة الاتصال اللاسلكي («واي فاي») بأمان

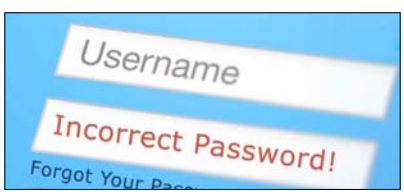
يقوم معظم مستخدمي الإنترنت في المنزل بالإتصال مع الشبكة عبر (الراوتر) أو ما يعرف بـ«نقطة وصول». الراوتر جهاز يتم تقديمه عادة من قبل مزود خدمة الإنترنت الذي تشتركون لديه، وهو صندوق بلاستيك مع هوائي واحد أو أكثر موصول به. الراوتر –هو في جوهره حاسوب مصغّر – يقوم بالاهتمام بعملية توجيه الحركة عبر الإنترنت بين أجهزة الحاسوب لديكم (أو الهاتف النقال) وبين اتصال الانترنت الذي يقدمه مزود الخدمة. إضافة إلى قيامه بوصلكم بشبكة الإنترنت، يقوم الراوتر بإنشاء شبكة صغيرة تربط جميع الأجهزة المتصلة ببعضها البعض، وعبر هذه الشبكة، تكون الأجهزة قادرة على الوصول إلى الأجهزة الأخرى المتصلة بذات الراوتر، ويمكن أن يكون ذلك مفيداً للقيام بنشاطات مثل الألعاب المشتركة أو تبادل الملفات.

يقوم العديد من الأشخاص بضبط الراوتر لإعداد الشبكة المنزلية مندفعين للحصول على الاتصال في أسرع وقت ممكن، بينما لا يتم إيلاء ضبط إعدادات الأمان إلا الاهتمام القليل أو لا يتم إيلاؤها أي اهتمام على الإطلاق. يمكن تفهّم هذا الأمر، إلا أنه يجعل اتصالاتكم أقل أمناً. إضافة إلى ذلك، فإن مهمة الراوتر ليست فقط تأمين الاتصال بالانترنت، بل هو مرتبط أيضاً بحاسوبكم وكافة الملفات الموجودة فيه.

ينصح فريق «سايبر آرابز» المستخدمين أثناء ضبطهم الراوتر قراءة دليل المستخدم الذي يأتي معه وضبط الإعدادات بطريقة تزيد الأمان قدر الإمكان. لسوء الحظ، تختلف آلية العمل بين راوتر وآخر، ولا يوجد آلية موحّدة تشرح ضبط الإعدادات لكل الراوترات دفعة واحدة، ولكن معظم الراوترات تأتي بواجهة مستخدم بسيطة يتم الوصول إليها عبر عنوان (مخفي) من خلال متصفح الانترنت.

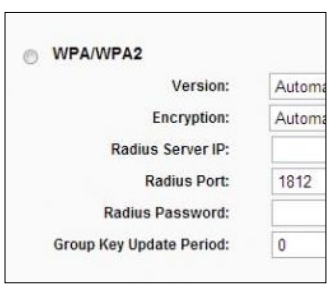
تستطيعون معرفة هذا العنوان من خلال «دليل المستخدم» المرفق مع الراوتر، إذا لم تتمكنوا من إيجاد العنوان تستطيعون البحث عنه على الإنترنت عبر كتابة اسم الراوتر وإصداره عبر هذا الموقع.
سنقوم بتوضيح بعض التوجيهات العامة للإعدادات المثلى لأمان الراوتر.

غيّروا اسم المستخدم وكلمة السر الافتراضيين للراوتر



تتم حماية قائمة الإعدادات في الراوتر عبر اسم المستخدم وكلمة السر، لكي يتمكن المالك الشرعي للجهاز فقط من تغيير الإعدادات. ولكن كافة أجهزة الراوتر تأتي مصحوبة باسم مستخدم وكلمة سر افتراضيّين بسيطين جداً، ومعروفين لدى المخترقين، ومعظم هذه الأجهزة يكون فيها اسم المستخدم وكلمة السر نفسها: admin/admin، مما يجعل إمكانية الوصول إلى إعدادات الراوتر سهلة جداً، لذا ننصح بتغيير اسم المستخدم وكلمة السر واستخدام كلمات سر طويلة ومعقدة.

فعّلوا تشفير WPA



تدعم كافة راوترات الواي فاي نوعاً من التشفير مقروناً باستعمال كلمة السر ، لكن لا يزال كثير من المستخدمين يضبطون إعدادات الراوتر دون استخدام تشفير أو كلمة السر، وبذلك يستطيع أيّ كان الوصول إلى الشبكة وأجهزة الحاسوب المتصلة بالراوتر .

يوجد نوعان من التشفير في أجهزة الراوتر: WEP وWPA (أتت بعدها WPA2). استعملوا تشفير WPA دائماً مع التأكد من وضع كلمة سر قوية.
مع أن استعمال تشفير WEP أفضل من أن لا يكون هناك أي تشفير على الإطلاق، لكنه صار قديماً وقابلاً للاختراق خلال ثوانٍ باستخدام مجموعة من الأدوات والخبرة اللازمة.
إذا استخدمتم تشفير WPA مع كلمة سر معقدة سيكون من الصعب جداً للأطراف الخارجية الوصول إلى الشبكة.

المخاطر الأمنية

غيّروا الاسم الافتراضي للشبكة (SSID)

نقاط الوصول وأجهزة الراوتر تستخدم اسماً شبكياً يسمى SSID. هذا الاسم تستطيعون ملاحظته عند البحث عن الشبكة اللاسلكية للاتصال بها من خلال الحاسوب أو الهاتف المحمول، وتقوم الشركات المصنعة للراوتر بتوزيع كافة أجهزتها مصحوبة باسم SSID افتراضي يدل على نوع الراوتر (مثلاً شركة Linksys تقوم بوضع اسم Linksys كعنوان افتراضي للشبكة) ومشاركة هذه المعلومات مع بقية العالم ليس خياراً ذكياً، فكما هو معروف، لكل جهاز من هذه الأجهزة نقاط ضعف يتم استغلالها من قبل المخترقين للوصول إلى الشبكة، وإذا قمتم بكشف نوع الراوتر لهم، فإنكم تمهّدون لهم الطريق للوصول إلى الشبكة.

بعض مزودي خدمة الإنترنت أيضاً يقومون بتوزيع أجهزة راوتر بأسماء معدة مسبقاً؛ هذه الأسماء هي الأخرى غير آمنة. قد تجدون مثلاً الراوتر باسم Thomson_563B67 أو Blink_567876 أو أية أسماء أخرى. من المعروف بين «الهاكرز» أو قراصنة الحاسوب أن هذه الأسماء المتبوعة برقم، تدل عادة على كلمة السر المستخدمة في تشفير WPA، وعبر معرفة هذه الأرقام من الممكن إجراء عملية حسابية لمعرفة كلمة السر خلال ثواني، وعدم تغيير هذا الاسم وكلمة سر WPA سيجعل اختراق شبكتكم سهلاً جداً.

تفادوا الاتصال التلقائي بالشبكات اللاسلكية المفتوحة (واي فاي)

إذا قمتم بالاتصال بشبكة لاسلكية مفتوحة لا تستخدم كلمة سر، مثلاً شبكة لجيرانكم أو نقطة اتصال مجانية، عليكم الانتباه لكونكم تعرضون أنفسكم للخطر، لأن أي شخص متصل بالشبكة ذاتها يستطيع الوصول إلى جهازكم بقليل من الجهد. بالطبع، حتى لو كانت الشبكة محمية بالتشفير وكلمة السر، سيستطيع أي شخص متصل بالشبكة نفسها أن يصل إلى محتوى نشاطكم، لذا عليكم دائماً التأكد من الأشخاص المتصلين بهذه الشبكة وأنهم موثوقون، للتقليل قدر الإمكان من المخاطر الأمنية على أجهزتكم.

فعلوا جدار الحماية («الجدار الناري»)

يتم تزويد أجهزة الراوتر الحديثة بجدار حماية (أو ما يشار إليه بـ«الجدار الناري» أو الـ firewall) مدمج معها، عليكم تفعيله.

جدار الحماية هو برمجية متطورة، تقوم بتحليل وفحص النشاط عبر الشبكة ومنع العمليات المشتبه بأنها قد تشكل خطراً.

تستطيعون أيضاً استخدام جدار حماية منفصل عن الذي يأتي مع الراوتر، ونحن في «سايبر آرابز» ننصح المستخدمين بتفعيل كل من جدار الحماية المدمج مع الراوتر (إن وجد) وجدار الحماية الخاص بنظام التشغيل ويندوز.

للوصول إلى إعدادات جدار الحماية في ويندوز نقوم باتباع الخطوات التالية:

نقوم بالنقر على إبدأ > لوحة التحكم > النظام والأمان > جدار الحماية أو

Start > Control panel > System & Security > Windows Firewall

تستطيعون أيضاً اللجوء إلى بعض برامج جدار الحماية المنفصلة؛ في «سايبر آرابز» ننصح باعتماد Commodo أو ZoneAlarm.

ضعوا الراوتر في مكان آمن

تصل إشارة الشبكة اللاسلكية بطبيعة حالها إلى خارج المنزل. تسرب كمية قليلة من الإشارة إلى الخارج ليس بمشكلة، لكن إن كانت الإشارة تصل إلى مدى بعيد في الخارج فهذا سيجعل من الأسهل استغلالها من قبل الجيران وسكان الشارع، لذلك، عند ضبط الشبكة اللاسلكية في المنزل، يحدد مكان توضع الراوتر أو نقطة الوصول إلى أين تصل الإشارة، لذا حاولوا دائماً أن يكون مكان الراوتر في منتصف المنزل تماماً، وحاولوا الابتعاد عن النوافذ للتقليل من تسرب الإشارة إلى الخارج.

أوقفوا تشغيل الراوتر عندما لا يتم استخدامه

الخطوة القصوى في تأمين الشبكات اللاسلكية، هي إيقاف تشغيلها عندما لا تقومون باستخدامها، وهذا يحدّ من إمكانية الاتصال بالشبكة أو اختراقها، كون معظم الاختراقات للشبكات تتم أثناء غياب الأشخاص عن منازلهم، أو في العطلة أو في الليل. لذا تأكدوا دائماً، عندما لا تكونون تستخدمون الشبكة، من إيقاف تشغيل الراوتر وفصل جهازكم عنه، ففي حال اتصالكم بالشبكة (التي قد تكون غير آمنة)، فإنكم تتيحون للمخترقين الوصول إلى أجهزتكم.

تطبيق سوفوس Sophos لأمن الهاتف النقال

تبدو الأوقات التي كان يتم فيها استخدام الهواتف النقالة لمجرد إجراء المكالمات الصوتية قد ولّت منذ زمن، وحلّت مكانها أجهزة الهواتف الذكية، التي تحوّلت إلى أجهزة حاسوب صغيرة خلال السنوات القليلة الماضية، وبالنسبة إلى العديد من الأشخاص أصبحت هذه الأجهزة هي بوابة الوصول الأساسية إلى شبكة الإنترنت. لكن المفاجئ أنه رغم هذا التطور، فإن موضوع أمان هذه الأجهزة لا يتم أخذه على محمل الجد بالقدر نفسه الذي يتم تناول أمن أجهزة الحاسوب العادية والمحمولة.

يبدو هذا غريباً، خاصة أننا لا نقوم فقط بتخزين صورنا الشخصية ومستنداتنا ومعلومات جهات الاتصال، بل نقوم أيضاً باستخدامها للاتصال بشبكة الهاتف والإنترنت!

تصلنا العديد من القصص في «سايبر آرابز» حول أشخاص وقعت بيانات هواتفهم النقالة في الأيادي الخطأ، وفي بعض الدول قد تقود هذه البيانات إلى مشاكل خطيرة كالتعرض للاعتقال أو التنكيل. لهذه الأسباب نقوم في «سايبر آرابز» دائماً بنشر مقالات تدور حول أمن الهواتف النقالة (تستطيعون قراءة آخرها هنا).

هناك العديد من التطبيقات المتاحة التي تساعد في حماية أجهزة هاتفكم النقالة، تماماً كالبرامج الموجودة لحماية أجهزة الحاسوب، لكن لا يوجد برنامج يستطيع إغلاق كافة الثغرات والتهديدات على هذه الهواتف.

إن كنتم حديثي العهد باستخدام أجهزة الهواتف النقالة، تستطيعون البدء باستخدام تطبيق سوفوس Sophos المجاني والمتاح للهواتف التي تعمل بنظام التشغيل أندرويد. هذا التطبيق يحتوي على عدد من الأدوات التي تقوم بحماية المعلومات في الهاتف، كفحص الفيروسات والملفات الخبيثة، وأدوات تقوم بإعطاء النصائح حول كيفية حماية بياناتكم وخصوصيتكم.

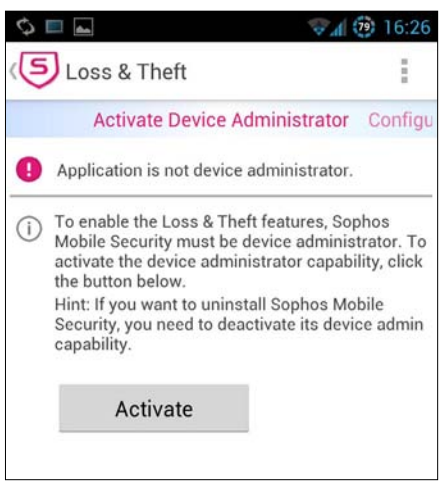
بعد تحميل هذا التطبيق وتنصيبه عبر متجر غوغل للتطبيقات (غوغل بلاي ستور) أو في حال كان الموقع محجوباً نستطيع تحميل التطبيق من هنا. بعد تشغيل التطبيق ستظهر على الشاشة أربع خيارات سنقوم بشرحها كلّ على حدة.

ماسح الفيروسات والبيرمجيات الخبيثة Scanner

عند النقر على «Scanner» سيقوم التطبيق بتحويلكم إلى أداته لفحص وتنظيف الهاتف من الفيروسات والملفات الخبيثة، كل ما عليكم فعله هو الضغط على Scan ليبدأ التطبيق بإجراء عملية فحص كاملة للهاتف، وإذا تم إيجاد شيء، سيخيركم التطبيق بين حذف الملف المصاب أو تعطيل عمله.

وفي حال كنا على اتصال بالانترنت سيقوم التطبيق بشكل دوري بتحديث قاعدة بياناته عن الفيروسات والمخاطر الأمنية، ويقوم التطبيق أيضاًبالعمل في الخلفية أي أنكم لستم مضطرين لإبقائه مفتوحاً حتى انتهاء الفحص، حتى وإن كان يعمل في الخلفية ووجد شيئاً سيقوم بتحذيركم. إلا أنه من المستحسن أن تقوموا بإجراءالفحص عبر قائمة التطبيق.

Loss & Theft للتحكم بالهاتف عن بعد من خلال الرسائل النصية

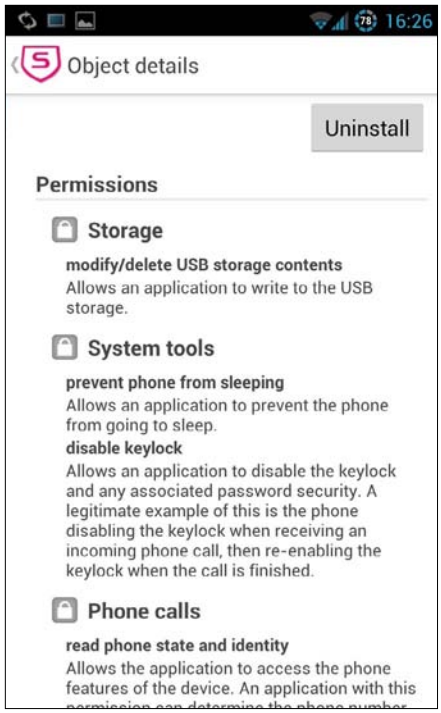


عند اختيار loss&theft من القائمة الرئيسية للتطبيق، سيتم تحويلكم إلى قائمة حيث تستطيعون ضبط التطبيق للقيام بعمليات معينة عند إرسال رسالة نصية إلى الهاتف تحتوي على نص معد مسبقاً ترسلونه من رقم تثقون به.

هذا الخيار مفيد في حال فقدان الهاتف أو سرقته أو حتى إذا تمت مصادرته من قبل السلطات.

على سبيل المثال، إذا تم مصادرة هاتفكم من قبل عناصر الأمن، وكنتم لا تريدون لبياناتكم ودليل الهاتف والصور أن تقع بيدهم، تستطيعون أن تطلبوا من صديق موثوق بأن يقوم بإرسال النص من رقمه المحدد من خلال التطبيق مسبقاً.

حال وصول هذه الرسالة إلى الهاتف سيقرأها التطبيق ويقوم بإجراء العملية التي قمتم بتحديدها، قد تكون مثلاً إزالة كافة البيانات والصور وجهات الاتصال والرسائل – وبالطبع الرسالة التي أرسلها الصديق ستتم إزالتها أيضاً.



إضافة إلى عملية المسح، يستطيع التطبيق إجراء العمليات التالية:

– قفل الهاتف
– إرسال أمر يجعله يرن بصوتٍ عالٍ
– إظهار رسالة معدة مسبقاً للشخص الذي لديه الهاتف بيده (الشخص الذي سرقه أو صادره أو وجده)
– تفعيل واستخدام نظام تتبع لتحديد مكان الهاتف
– إعلامكم في حال تم تغيير الشريحة الهاتفية

لاستخدام هذه الوظائف عليكم الموافقة على إعطاء الصلاحية للتطبيق لإجراء عدد من العمليات، مثل قفل الشاشة أو الحصول على صلاحية «مدير» أو Administrator. هذه الشروط تستطيعون رؤيتها والموافقة عليها بعد أول مرة تقومون بالنقر فيها على loss&theft. بعد الانتهاء من تحديد الوظائف التي تريدون أن تتم تأديتها، سيتم تحويلكم إلى قائمة حيث تستطيعون تغيير الإعدادات المطلوبة.

عليكم أيضاً تحديد رقم هاتفي واحد على الأقل يمكنكم الوثوق به (رقم الهاتف بالإضافة إلى رمز الدولة)، كما عليكم تحديد نص الرسالة التي سيتم استعمالها ككلمة سر لتفعيل العملية المعينة.

إذا حرّكتم الشاشة إلى اليمين، سيعرض لكم خيار يتيح إمكانية تفعيل أو تعطيل خدمة أو أكثر.

بعد الانتهاء من ضبط هذه الخدمة في التطبيق ستتمكنون من تجربتها إن كانت تعمل، فإذا قمتم، باستعمال الهاتف الآخر الموثوق، بإرسال الرسالة «locate password» مع استبدال password بكلمة السر الخاصة، سيتلقى هذا الهاتف إحداثيات مكان جهازكم.

الأوامر الأخرى التي تستطيعون استخدامها هي:

Alarm: تقوم بتفعيل الرنين بصوت عالي

Locate: تقوم بتحديد مكان الجهاز

Lock: تقوم بقفل الجهاز

Wipe: تقوم بإزالة كافة البيانات والمعلومات الموجودة على الهاتف (تحذير: لا تقوموا باختيار هذا الخيار!)

خيار Security advisor يبيّن إعدادات الأمن

عند اختيار «Security advisor» من القائمة الرئيسية سيتم تحويلكم إلى قائمة تستطيعون أن تعاينوا فيها إعدادات الأمان في جهازكم، ويقوم التطبيق بإخباركم إن كان أحد خيارات الأمان آمناً أم لا عبر مقياس: أخضر= آمن، أحمر= غير مفعّل (لذا فهو غير آمن).

سينصحكم هذا الخيار بتفعيل الخدمات التي يظهر بجانبها اللون الأحمر.

عند الضغط على العنصر الأحمر ستظهر رسالة تشرح أهمية هذا الخيار. أيضاً سيتم تزويدكم بمسار هذا الضبط للقيام بالتعديل المطلوب.

خيار Privacy Advisor لإدارة التطبيقات

عند النقر على Privacy advisor من القائمة الرئيسية، سيتم تحويلكم إلى قائمة تحتوي على كافة التطبيقات المنصّبة على الهاتف، وعند النقر على أحد هذه التطبيقات، ستعرض لكم قائمة بالصلاحيات التي منحتموها لهذا التطبيق عند تنصيبه، وتتراوح الصلاحيات بين إمكانية تعديل الملفات على بطاقة الذاكرة، والوصول إلى دليل الهاتف أو تفعيل وتعطيل البلوتوث من دون إعلامكم.

يعتبر Privacy advisor أداة للتنبيه، أكثر من كونه أداة تحسّن أمان الهاتف.

إذا كنتم لا تثقون بتطبيق ما أو قمتم بتحميل تطبيق مصدره غير موثوق، يستحق الأمر إلقاء النظرة على التطبيق عبر هذه الأداة والتحقق من الصلاحيات التي قمتم بمنحها إياه أثناء تنصيبه.

BoxCryptor لتشفير المعلومات

إنّ تشفير الملفات مهم جداً إن لم تريدوا أن يصل أحد إلى محتواها. وهي عملية تجعل محتوياتها غير مقروئة أو مفهومة في حال وقوعها في يد أشخاص آخرين ما لم يحصلوا على كلمة السر لفك تشفيرها.

هناك العديد من الطرق لتشفير البيانات، والعديد من البرامج التي تقوم بهذه المهمة. وقمنا سابقاً في «سايبر آرابز» بشرح طريقة عمل كل من TrueCrypt وAES Crypt وتشفير هواتف الأندرويد.

برنامج BoxCryptor هو برنامج جديد نسبياً في عالم تشفير الملفات ويتميز ببساطة تصميمه وسهولة استخدامه، وقد أثبت أنه مناسب بالنسبة إلى العديد من مستخدمي الحاسوب ذوي الخبرة البسيطة. ويوجد للبرنامج نسخ لنظام التشغيل ويندوز وماكنتوش ولينوكس، إضافة إلى نظام التشغيل iOS الخاص بأجهزة الآيفون والآيباد ونظام التشغيل أندرويد، كما يتميز البرنامج أيضاً بإمكانية ربطه مع العديد من خدمات التخزين السحابي مثل Dropbox وSkyDrive وGoogleDrive وSugarSync.

ولا يقتصر عمل البرنامج على تشفير المستندات فقط، بل يمكنه تشفير كافة الملفات والمجلدات، تماماً كالبرنامج المنافس TrueCrypt. آلية التشفير المستخدمة في برنامج BoxCryptor هي AES-٢٥٦، التي استطاعت إثبات فاعليتها وعدم إمكانية اختراقها.

ومن مساوئ النسخة المجانية للبرنامج هي أنها لا تقوم بتشفير أسماء الملفات والمجلدات أو إخفائها، إلا أن الوصول لمحتوياتها لا يمكن إلا في حال الحصول على كلمة السر، لذا، في حال أردتم استخدام النسخة المجانية، ينصح فريق «سايبر آرابز» بعدم تضمين معلومات مهمة في أسماء الملفات والمجلدات، أما بالنسبة إلى النسخة المدفوعة فإنها تقوم بتشفير أسماء الملفات والمجلدات.

يقوم BoxCryptor بتشفير الملفات كل واحد على حدة دون القيام بتغيير بنية المجلدات التي تحويها، وهي صفة تجعله يمتاز على تطبيقات مثل TrueCrypt، حيث يتوجب على المستخدم أن يحدد حجم المجلد قبل البدء بعملية التشفير. وينتج عن هذه الميزة التي يتمتع بها BoxCryptor، لا سيما لدى استخدام التشفير مقروناً بإحدى خدمات التخزين السحابي، تحسيناً في الأداء، لأن ليس هناك حاجة إلى مزامنة جميع الملفات في كل مرة تودون فيها إجراء تغيير ما.

تنصيب BoxCryptor على كل أنظمة التشغيل سهل جداً، وبالنسبة إلى الهواتف النقالة، ما عليكم سوى تنصيب التطبيق من خلال غوغل بلاي ستور لأجهزة أندرويد أو آب ستور لأجهزة الآيفون والآيباد. أما بالنسبة لأنظمة التشغيل ويندوز ولينوكس وماك بإمكانكم تحميل نسخة البرنامج من هنا.

بعد تنصيب البرنامج عليكم تحديد نوع خدمة التخزين السحابي حيث ستضعون البرنامج أو بإمكانكم انتقاء خيار «مخصص» أو Custom في حال كنتم ستهيئون البرنامج على السواقة في جهازكم (القرص الصلب C مثلاً). بعد اختيار السواقة، ينبغي إنشاء المجلد حيث ستضعون الملفات التي ترغبون بتشفيرها. بعد إتمام هذه الخطوة، نقوم باختيار كلمة سر قوية وطويلة (بإمكانكم استخدام برنامج مثل Keepass لتخزين كلمة السر).

في أنظمة التشغيل ويندوز ولينوكس وماك سيقوم البرنامج بإنشاء سواقة افتراضية تحتوي على الملفات المشفّرة. وطالما برنامج BoxCryptor يعمل فإن كافة الملفات الموجودة في هذا المجلد الذي قمتم باختياره سابقاً ستكون مشفرة.

في حال اخترتم إحدى خدمات التخزين السحابي، لن يستطيع أي أحد الوصول إلى المعلومات في هذه الملفات. وإن كنتم تستخدمون البرنامج على الملفات والمجلدات المتواجدة على جهاز الحاسوب الخاص بكم، من المستحسن إغلاق BoxCryptor بعد الانتهاء من كل جلسة، أو تعطيل التشغيل التلقائي للبرنامج عبر انتقاء خيار «start application with Windows/OSX» الموجود في قائمة الإعدادات.

الاستخدام الآمن للرسائل النصية القصيرة (SMS)

الرسائل النصية القصيرة أو «SMS»، هي واحدة من أكثر الخدمات استخداماً في أجهزة الهاتف المحمول، ولكن، كما الاتصال الصوتي، فإنها وسيلة غير آمنة للتواصل، فكل الرسائل القصيرة التي يتم إرسالها واستقبالها غير مشفرة، وتبقى نسخة من رسائلكم مخزّنة في عدة مواضع عبر شبكة الاتصالات.

لذا، فمن السهل جداً على سيّئي النية، من الأشخاص والمجموعات السياسية والحكومات، أن يروا ما هي الرسائل التي ترسلونها وتتلقونها. لهذه الأسباب، يوصي فريق «سايبر آرابز» بتوخي الحذر الشديد عند استخدام الرسائل النصية، لكن على الرغم من ذلك، من الممكن تشفير الرسائل النصية، خاصةً إذا كنتم تستخدمون جهاز هاتف يعمل بنظام «أندرويد».

من الممكن إتمام تشفير الرسائل عبر الطريقة التي سنقترحها حتى دون الحاجة إلى وجود اتصال بالانترنت، وبعد عملية التشفير تبقى الرسائل قابلة للاعتراض من قبل طرف ثالث (غيركم أنتم والشخص الآخر الذي تتواصلون معه)، إلا أن محتواها سيكون مشفراً وغير مقروء.

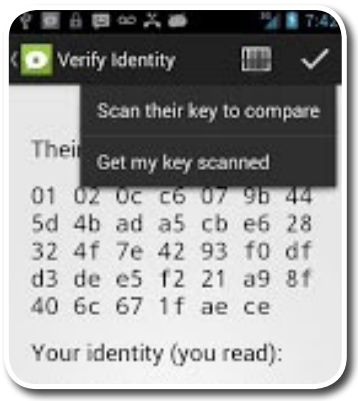
لتشفير الرسائل يتوجب تحميل تطبيق يدعى TextSecure، تستطيعون تحميله من متجر غوغل (أو من هنا في حال كان محجوباً). لدى استخدام تطبيق TextSecure يبقى بإمكانكم أن تبعثوا الرسائل غير مشفرة، مثلاً للأشخاص الذين لم يقوموا بتنصيب هذا التطبيق.

عند تشغيل التطبيق للمرة الأولى، سيُطلب منكم إدخال كلمة سر. عليكم تذكر هذه الكلمة جيداً لأنكم قد تحتاجون إليها لاحقاً للوصول إلى الرسائل المشفرة على هاتفكم الجوال. بعد ذلك سيقوم التطبيق بسؤالكم إن كنتم ترغبون بأن يقوم بأخذ نسخة عن الرسائل النصية المتواجدة على الجهاز. ينصح فريق «سايبر آرابز» باتباع هذه الخطوة لأنه من الجيد أن تكون كافة معلوماتكم مشفرة. بعد إتمام العملية، من الأفضل القيام بحذف الرسائل غير المشفرة من موقعها الأصلي.

في حال كنتم لا ترغبون بتشفير الرسائل الموجودة، إضغطوا على «Skip» أو «تخطي».

هنا، أصبحتم جاهزين لاستخدام تطبيق TextSecure كبرنامج للرسائل النصية، يرجى ملاحظة أنه في حال عدم رغبتكم بتبادل رسائل مشفرة، يبقى بإمكانكم أن تستعملوا TextSecure لتشفير الرسائل المرسلة والمتلقاة على جهازكم وتخزينها بشكل آمن، ويسمح ذلك ببقاء الرسائل غير مقروءة في حال وقع الهاتف بيد أي أحد.

من الضروري إجراء اتصال مؤمّن مع رقم الهاتف الذي ستتبادلون الرسائل المشفرة معه عبر TextSecure. تتم هذه العملية تلقائياً عبر أول رسالة نصية يتم إرسالها من خلال TextSecure، ولكن تأكدوا من أن هذه الرسالة لا تحتوي أية معلومات حسّاسة.



بعد ذلك، كل الرسائل ستكون مشفّرة عبر مجموعة من مفتاحين: مفتاح عام تعطونه للطرف الذي سيقوم بتوجيه الرسائل إليكم لتشفير الرسائل التي ستتلقونها، يكون مربوطاً بمفتاح خاص، تحتفظون به لفك تشفير الرسائل التي تتلقونها (من المهم أن تحافظوا على المفتاح الخاص ولا تسمحوا لأي أحد بالحصول عليه). إذا تمت عملية الاتصال المؤمّن بنجاح ستظهر على الشاشة لديكم الرسالتان التاليتان "Key exchange message" و"Received and processed key exchange message".

في قائمة الإعدادات (الأيقونة اليمنى > الإعدادات) بإمكانكم انتقاء عدة خيارات تتيح لكم استعمال TextSecure بالطريقة التي تختارونها. مثلاً، إن كنتم لا تريدون أن يقوم تطبيق TextSecure بتشفير كافة الرسائل، قوموا بإزالة التحديد عن "use for all SMS" و"use for all MMS". الإعدادات الأخرى التي تستطيع انتقائها تتضمن الحصول على «تقارير التوصيل»، وحذف الرسائل القديمة (غير المشفّرة)، وتغيير كلمة السر، بالإضافة إلى إعدادات أخرى تتعلق بالصوت والمظهر العام للتطبيق.

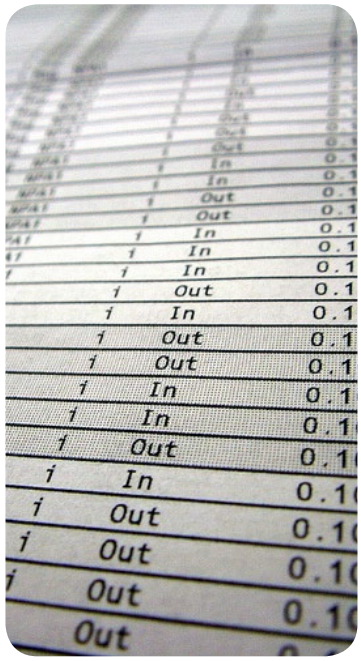
أمان برامج المراسلة النصية والصوتية

تعدّ برامج التواصل مثل واتساب وفايبر من أكثر البرامج انتشاراً لدى قراء «سايبر آرابز»، ولكن قليلون منهم يعلمون أن العديد من هذه البرامج غير آمنة ويجب تجنب استخدامها في تبادل المعلومات المهمة، لهذا السبب، قمنا بإعداد هذا الجدول الذي نستعرض فيه عدداً من هذه التطبيقات المتاحة ودرجة أمانها وآلية التشفير التي تستخدمها.

وكما ترون فإن تطبيقات مثل فايبر وواتساب غير آمنة، فيما ننصح مستخدمي هذه التطبيقات بالاستعاضة عنها بتطبيقي ريد فون وتكست سيكيور. يأتي بعدها في الدرجة الثانية كل من أوستيل و سايلنت سيركل، أما فيما يخص تطبيقي سكايب وفيس بوك فإنهما ليسا سيئين، خاصة إذا ما تم استخدام VPN أو SSH معهما، وطبعاً يجب على الطرف الآخر من الاتصال استخدامهما أيضاً لضمان أمان هذه التطبيقات.

التطبيق	الوظيفة	التشفير	ملاحظات	آمن؟
فايبر	مراسلة نصية وصوتية	غير مشفر، يقوم فقط بتمويه الصوت	شركة إسرائيلية المصدر والإدارة	لا
واتساب	مراسلة نصية	تطبيق سيئ لتشفير SSL	يستخدم رقم الهاتف للتفعيل	لا
سكايب	مراسلة نصية وصوتية	تشفير قوي لكن قد يوجد باب خلفي يمنح سكايب وجهات أخرى إمكانية النفاذ (AES 256 bit)	يستخدم جهات اتصال سكايب والاتصال بالهاتف العادي غير آمن	معقول
غوغل هانغ آوتس	مراسلة نصية وصوتية	تشفير SSL آمن، ولكن قد يتمكن غوغل من الإطلاع على بياناتكم	تستخدم جهات اتصال غوغل+	نعم
لاين	مراسلة نصية وصوتية	غير معروف. من الممكن ألا يكون مشفراً	يستخدم رقم الهاتف للتفعيل	لا
فيسبوك مسنجر	مراسلة نصية	يستخدم تشفير SSL ولكن قد يرى فيس بوك بياناتكم	تستخدم جهات اتصال فيس بوك	نعم
سايلنت سيركل	مراسلة نصية وصوتية وفيديو	نعم قوي جداً (ZRTP)	يستخدم رقم الهاتف للتفعيل	نعم
ريد فون	مراسلة نصية وصوتية	نعم قوي جداً (ZRTP)	يستخدم رقم الهاتف للتفعيل	نعم
تكست سيكيور	مراسلة نصية	نعم قوي جداً (OTR)	تعمل باستخدام رسائل نصية قصيرة SMS	نعم
أوستيل	مراسلة صوتية	نعم قوي جداً (ZRTP)	لا تعمل باستخدام رقم هاتف	نعم
تانغو	مراسلة نصية وصوتية وفيديو	التشفير غير معروف، من السهل اختراقه	يستخدم رقم الهاتف للتفعيل	لا

التجسس على رسائل الهواتف النقالة وخدمات الاتصال



تنتشر التطبيقات المجانية المستخدمة في المراسلة والاتصال مثل واتساب وسكايب وفايبر وتانغو بشكل واسع بين مستخدمي الهواتف الذكية، فهي تتيح للمستخدمين التواصل فيما بينهم صوتياً أو إرسال الرسائل عبر هذه التطبيقات دون الحاجة إلى الدفع لشركات الاتصال. أشرنا في مقالٍ سابق إلى أن هذه التطبيقات ليست دائماً آمنة. فتطبيق فايبر لا يقوم بتشفير بياناته، وسكايب ليس آمناً تماماً. الرسائل النصية القصيرة والاتصالات الهاتفية العادية هي أيضاً بالطبع غير آمنة.

تحاول العديد من الحكومات وشركات الاتصالات في كثير من الدول حول العالم حجب هذه الخدمات المجانية، وبحجج عديدة تخفي وراءها السبب الرئيسي، وهو أسباب ماديّة.

حين تقوم بالتواصل مع أصدقائك عبر السكايب مثلاً فإن شركات الإتصال تخسر فرصة لكسب النقود منك عبر اتصالك بأصدقائك عن طريق شبكتهم. وقد يكون هناك سبب آخر خلف هذا الحجب: المراقبة والتجسس.

على سبيل المثال، أمرت مؤخراً هيئة تقنية المعلومات والاتصالات السعودية (CITC) شركات الاتصالات بالقيام باتفاقية لمراقبة أو حظر الوصول إلى خدمتي سكايب وواتساب. وفي دول أخرى مثل سوريا وإيران، هذه الخدمات محجوبة بالأصل، على الرغم من أنه من غير المستحيل بالنسبة إلى الحكومات فك تشفير اتصالاتكم عبر هذه الخدمات المجانية، إلا أن وجود نوع من التشفير يصعّب المهمة.
لهذا السبب، غالباً ما تتعاون الحكومات بالعمل مع مطوري التطبيقات، في دول كالصين، وعلى سبيل المثال، تقوم سكايب بطرح نسخة بديلة من برنامجها تتيح للسلطات إمكانية الوصول إلى معلوماته، فيما قام عدد من الشركات الأخرى بإقامة صفقات شبيهة مع الحكومات في عدد من الدول.

بالنسبة للمستخدمين، لا يوجد دائماً بديل جيد؛ بعض خدمات الاتصال والمراسلة النصية من الصعب جداً فك الحجب عنها على أجهزة الهواتف النقالة، وهذا يعود لكون معظم أنظمة تشغيل الهواتف النقالة تم إنشاؤها بحيث يكون من المستحيل تغيير إعداداتها، دون أن يتم تعطيل بعض الخصائص التي تتيح فتح ثغرات أمنية في نظام التشغيل، هذه العملية يطلق عليها عادةً «فك القفل». نحن في «سايبر آرابز» لا ننصح المستخدمين بفك قفل أجهزتهم لما له من مخاطر أمنية.

وتبقى أفضل طريقة للتحايل على الحجب هي باستخدام خدمة VPN، وأفضل طريقة لاستخدامها هي باستعمال حساب VPN خاص، إذا كنتم تملكون جهاز أندرويد واسم مستخدم وكلمة سر لحساب الVPN بامكانكم تفعيله عبر الذهاب إلى: إعدادات > الشبكة اللاسلكية > VPN
أو Settings > Wireless & Network > VPN

أما بالنسبة إلى الأشخاص الذين لا يملكون حسابات VPN خاصة بهم، بإمكانهم استعمال خدمات VPN مجانية مثل Hotspot Shield. توجد بدائل أخرى قد تعمل في دولتكم بإمكانكم القراءة عنها هنا.

من السهل تثبيت تطبيق Hotspot Shield، ما عليكم سوى تحميل التطبيق وتنصيبه عبر متجر غوغل للتطبيقات أو من هنا في حال كان المتجر محجوباً. بعد إتمام تنصيب التطبيق، قوموا والنقر على Start protection، ستلاحظون ظهور إشارة مفتاح في الزاوية اليسرى للشاشة، تخبركم بأنه تم الاتصال بالشبكة، بعد اتمام الاتصال يصبح بإمكانم استخدام خدمات المراسلة النصية والاتصال المجانية التي ترغبون بها.

يرجى ملاحظة أن التجسس على تطبيقات مثل سكايب وواتساب ليست مستحيلة حتى باستخدام VPN، وذلك يعتمد على الدولة التي تقومون بالاتصال منها وآليات المراقبة التي تستخدمها شركات الاتصالات في تلك الدول، خاصةً أن الدول التي قامت بحجب تطبيق مثل سكايب تجعل من الصعب فك الحظر عنه، كما تقوم أيضاً بحجب معظم خدمات VPN والطرق الأخرى للتحايل على الحجب.

الهواتف الفضائية

يصلنا إلى «سايبر آرابز» العديد من الطلبات لنشر معلومات عن وسائل الاتصال الفضائي، وبالتحديد الهواتف الفضائية. الهاتف الفضائي هو هاتف نقال يقوم بإنشاء قناة اتصال عبر أقمار صناعية ثابتة أو متحركة بالنسبة إلى الأرض عوضاً عن الشبكة العالمية للاتصالات GSM. وكون الهواتف الفضائية لا ترتبط بشبكات هاتف تخضع للدول، فهذا يسهل عمليات الاتصال في المناطق التي لا تتوفر فيها تغطية.

يتم استخدام هذا النوع من الهواتف في المناطق التي تقع تحت سيطرة المعارضة في سوريا إضافة إلى صحراء شمال أفريقيا والصومال.

وعلى الرغم من إيجابية كونها توفّر التغطية في كافة المناطق، إلا أن أحد مساوئها أنها ليست أكثر أمناً من الهواتف النقالة العادية (رابط).

في الواقع، من الناحية الأمنية، فإن الهواتف الفضائية تعتبر كابوساً، لهذا السبب ننصح باستخدام هذه الهواتف للضرورة القصوى فقط، حين لا يتوفر وسائل اتصال أكثر أماناً منها.

كيف تعمل الهواتف الفضائية؟

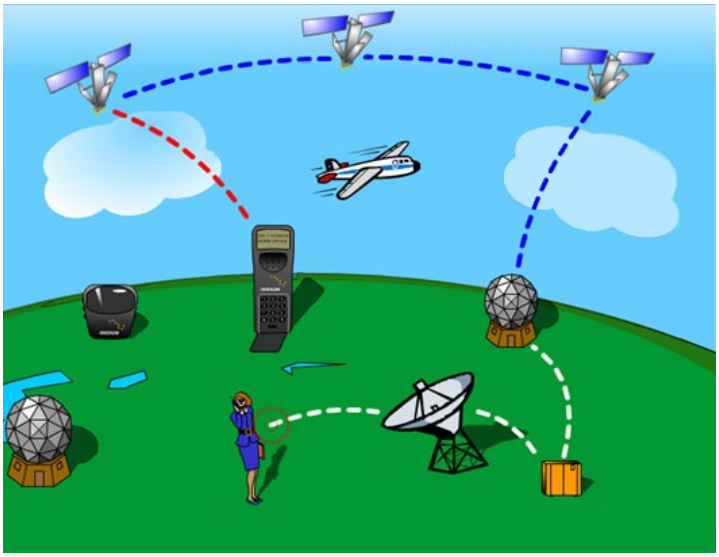
بشكلٍ عام، هناك نوعان من أنظمة الهواتف الفضائية، أحدهما يقوم بالاتصال بأقمار صناعية ثابتة (أي متمركزة في مكان معيّن في الفضاء) والآخر يقوم بالاتصال بمجموعة من الأقمار الصناعية

تقوم بالدوران المستمر في المدار الأرضي المنخفض. ويقوم الأخير فقط بتوفير التغطية التامة لشركة Iridium إحدى أكثر الشركات شهرة في هذا المجال، أما الشركات التي تقوم بالاعتماد على الأقمار الصناعية الثابتة – والتي تتوفر في الشرق الأوسط وشمال أفريقيا– تتضمن InmarSat و Thuraya.

تقوم الهواتف الفضائية عوضاً عن الاتصال بعمود إرسال GSM، بالاتصال بقمر صناعي يتواجد على علوّ يزيد عن ٧٠٠ كيلومتر فوق الأرض. لهذا السبب، تحتاج الهواتف الفضائية إلى أجهزة إرسال واستقبال أقوى من تلك المستخدمة في شبكة GSM، ما يجعل هذه الأجهزة أكبر حجماً من الهواتف النقالة المعتادة.

يجب أيضاً استخدام الهاتف الفضائي في الأمكنة غير المسقوفة، حتى ولو كانت بعض هذه الهواتف قد تعمل داخل المنازل إلا أنها تعمل بشكل ضعيف، ولن تعطي وضوحاً في الاتصال، كما أن للأحوال الجوية السيئة والغيوم والأشجار والمباني تأثيراً على إمكانية وجودة الاتصال عبر هذه الهواتف.

حالما يقوم الهاتف الفضائي بإجراء الاتصال مع القمر الصناعي، يقوم هذا القمر بتحويل طلب الاتصال إلى الأرض مجدداً عن



طريق ما يسمى بـ «محطة البوابة الأرضية» أو GES، التي تقوم بإنشاء الاتصال بين هاتفكم الفضائي وبين الهاتف الذي تحاولون الاتصال به.

يذكر أن معظم الهواتف الفضائية توفر إمكانية إرسال واستقبال المكالمات والرسائل النصية القصيرة كما توفّر اتصالاً بسيطاً بالإنترنت (غالباً يكون بطيئاً جداً).

للحصول على خدمة الهاتف الفضائي، تحتاجون إلى الاشتراك مع إحدى الشركات المزودة للخدمة وذلك بالحصول على بطاقة SIM وجهاز هاتف خاصين بالشركة المزودة للخدمة، حيث – وعلى عكس الهواتف النقالة المعتادة– يعمل الهاتف الفضائي فقط على الشبكة التي قمتم بالاشتراك فيها.

تتراوح أسعار الهواتف الفضائية بين ٥٠٠ و١٠٠٠ دولارٍ، وتختلف تكلفة الاتصال باختلاف مكان الاتصال ولكن بشكل عام، تتراوح التسعيرة بين دولار واحد ودولارين لكل دقيقة أو رسالة نصية.

طريقة الاستخدام

عند الاشتراك والحصول على جهاز الهاتف الفضائي وبطاقة الـ SIM، لن يكون صعباً المباشرة باستخدام الخدمة، ولكن يرجى الانتباه إلى أن استخدام الهواتف الفضائية محظور في العديد من الدول ما لم تحصلوا على رخصة لحيازته، ولأنه من السهل جداً على السلطات معرفة أماكن وجود أجهزة الهواتف الفضائية، فإننا ننصح بعدم استخدامها في الدول التي تحظرها. يجب أخذ الحذر حين استخدام أي هاتف فضائي غير مرخّص في لبنان وسوريا والسعودية والبحرين وإيران والسودان. تأكدوا من الحصول على آخر المعلومات الضرورية قبل استخدام الهاتف الفضائي.

لا يعمل الهاتف الفضائي بشكل دائم، كالهواتف النقالة، فمثلاً إن كنتم تضعونه في حقيبة، لن يكون متاحاً لأنه لا يستطيع الاتصال بالقمر الصناعي. عند تشغيل الهاتف يجب أن تتواجدوا في مكان يمكنكم أن تروا السماء منه بشكل واضح، ويتمكن خلاله القمر الصناعي من «رؤية» الهاتف، ويكون كلاهما قادر على الاتصال ببعضهما البعض، ومعظم أجهزة الهواتف الفضائية مجهزة بهوائي كبير علينا سحبه حتى يستطيع الاتصال مع القمر الصناعي.

حين يستطيع الهاتف والقمر الصناعي إيجاد بعضهما البعض تلقائياً، يقومان بتبادل معلومات المكان، غالباً عن طريق إحداثيات نظام التموضع العالمي GPS، وبناءً على ذلك، يقوم القمر الصناعي بتحديد موقعكم على الخريطة وتتبعكم بإشارته وإنشاء الاتصال مع الشبكة. تستطيعون الآن إجراء المكالمات وإرسال الرسائل النصية والوصول إلى شبكة الإنترنت (في حال توفرها). ولكن إذا فقد الهاتف الاتصال مع القمر الصناعي لسبب ما مثل الدخول إلى منزل أو إغلاق الهوائي أو وضع الهاتف في حقيبة، عليكم أن تقوموا بإعادة عملية الاتصال مجدداً.

عندما يتم تشغيل الهاتف، يبدأ تلقائياً بمحاولة العثور على إشارة الشبكة، هذه العملية تسمى «Location fix» وتستغرق فترة زمنية تتراوح من بضع ثوانٍ إلى عشرة دقائق، وقد

تستغرق هذه العملية وقتاً طويلاً خاصة في المرة الأولى التي يتم فيها استعمال الهاتف في مكان جديد لذا تحلوا بالصبر، لأن الهواتف الفضائية ليست دائماً بوضعية الاستعداد، وهي ليست بأدوات مثالية للاتصالات الطارئة، مثلاً إذا كنتم داخل مكان ما وتحتاجون لأن تكونوا على اتصال مباشر، أو لا تملكون وقتاً للانتظار كي تقوموا بإجراء الاتصال.

المخاطر

كما ذكرنا سابقاً، يجب ألا يتم اعتبار الهواتف الفضائية كأدوات اتصال آمنة، ولاسيما في البيئات التي تخضع للمراقبة. إن كنتم لا تودون أن يتم رصد مكانكم أو اتصالاتكم من قبل السلطات، فالهواتف الفضائية تعتبر خياراً سيئاً، ويجب استخدامها فقط في حال لم تتوفر أية وسيلة اتصال أخرى.

أحد الأسباب وراء ذلك هو أنه من السهل نسبياً كشف موقعكم، فخلال فترة القيام بعملية location fix، يقوم الهاتف الفضائي بإرسال إحداثيات موقعكم، والتي يمكن كشفها من على بعد مئات الكيلومترات. فقد مرّت علينا حالات حيث قام الأشخاص بتشغيل هواتفهم الفضائية غير المرخصة، ثم تم كشفهم من قبل الأمن بوقت قصير، ولأن الهاتف الفضائي يقوم بالتواصل عبر موجات الراديو، فإنه من الممكن تحديد مكانكم عبر آلية التثليث، وهي عملية هندسية تستخدم لتحديد المواقع ويتم اعتمادها عادة لضبط المحطات غير القانونية في منطقة ما.

وعلى الرغم من أن جميع الهواتف الفضائية تستخدم التشفير، إلا أنه يجب ألا يراها البعض بمثابة حماية كافية ضد التنصت. في سوريا على سبيل المثال، من المعروف أن رموز فك التشفير لهواتف الثريا هي في متناول يد النظام، وحدث هذا لأن الموزع الرئيسي لخدمة الثريا في سوريا تملكه الحكومة السورية. وهذا ما تسبب وقوع الناس في مشاكل خطيرة أثناء استخدامهم هواتف الثريا في سوريا، لهذا السبب ننصح بعدم استخدام هذه النوعية من الهواتف في سوريا.

على الرغم من صعوبة فك تشفير الهواتف الأخرى، إلا أنها يجب ألا تصنّف على أنها آمنة. فقد تم تطبيق الهندسة العكسية (آلية تتيح معرفة طريقة عمل جهاز معين من خلال تحليل بنيته) على معياري التشفير القياسي المستخدمين في الهواتف الفضائية المعروفين بـGMR-1 وGMR-2، من قبل فريق أمني ألماني، كما من المعروف أن العديد من الحكومات تمتلك رموز فك تشفير هذه الهواتف، لذا عليكم تفادي التواصل ومشاركة المعلومات الحساسة عن طريق الهاتف الفضائي.

أحد المخاطر الأخرى للهواتف الفضائية، هي في حال سرقتها أو مصادرتها من قبل السلطات، فمعظم هذه الهواتف تحتفظ بنسخة موسّعة من سجلّات البيانات كأماكن التواجد السابقة، والاتصالات التي قمتم بإرسالها وتلقيها، وعدا عن ذلك، يقوم العديد من الأشخاص بالاحتفاظ بمعلومات حساسة – كأرقام وعناوين البريد الإلكتروني لجهات الاتصال – على هواتفهم. وفي حال تمت مصادرة أو سرقة الهاتف، فإن كل هذه المعلومات ستتوفر بيد الشخص الذي يمتلك الهاتف وسيكون لديه القدرة بالتحكم بهذه المعلومات والإطلاع على شبكة معارفكم، لهذا السبب، تجنّبوا تخزين الأرقام وعناوين جهات الاتصال على هواتفكم الفضائية إن لم يكن ذلك ضرورياً، لأن وحده تحطيم جهاز الهاتف يستطيع ضمان مسح هذه المعلومات المخزّنة.

الاستخدام الآمن

أفضل ما يمكن تذكره هو معرفة أن استخدام الهاتف الفضائي غير آمن تماماً. لذلك استخدموه فقط عند الضرورة، وفي حال كنتم تتواصلون عبر الهاتف الفضائي مع أشخاص بشكل متواصل، قوموا بالاتفاق على لغة مرمّزة، على سبيل المثال، كأن تتفقوا على الإشارة إلى المظاهرات بـ«تجمّع عائلي» وتفادوا استخدام أسمائكم الحقيقية.

ولأن الهواتف الفضائية يبدو شكلها مختلفاً، ولهذا السبب قد تلفت انتباه الأشخاص المحيطين بكم، حاولوا ألا تستخدموها في حال وجود أشخاص لا تعرفونهم أو لا تثقون بهم. أيضاً قوموا بإخفاء هاتفكم حين تقومون بالتنقل، أو ضعوه في مكان لا يستطيع عناصر الأمن العثور عليه.

لمزيد من المعلومات، راجعوا هذا الكتيب.

تشفير الملفات باستخدام AES CRYPT

يمتلك الجميع ملفات يفضلون عدم مشاركتها مع الآخرين ويفضلون حمايتها بطريقة آمنة، وقد يتضمن ذلك صور ومقاطع فيديو، أونصوص أو أنواع أخرى من الملفات. للحرص على عدم وقوع هذه الملفات في الأيدي الخطأ، يمكنكم أن تشفّروا هذه الملفات، ويعني ذلك أن محتواها يصبح غير مقروء لأي شخص لا يملك كلمة السر لفتح الملف. شرحنا في مقالات سابقة كيفية تشفير الملفات باستخدام برنامج TrueCrypt (الرابط). يعتبر TrueCrypt مفيداً بشكل خاص في حال أردتم أن تنشئوا سواقة افتراضية تحفظ كل ملفاتكم السرية. إلا أن في بعض الأحيان قد تريدون أن تشفروا ملفاً واحداً فقط، على سبيل المثال إذا أردتم أن ترسلوا ملفاً عبر البريد الإلكتروني بشكل آمن. لبلوغ هذه الغاية يمكنكم أن تستخدموا تطبيقاً اسمه AES Crypt، ويعني الاسم "معيار التشفير المتقدم". هذا التطبيق سهل الاستخدام ويمكن تشغيله من سطح المكتب في الحاسوب لأنه يصبح جزءاً من القائمة التي تظهر عند النقر على الملف بالزر الأيمن من الفأرة، من دون الحاجة إلى إطلاقه كبقية التطبيقات التقليدية.

لتحميل AES Crypt:
http://www.aescrypt.com/download

لمشاهدة فيديو الشرح:
http://www.youtube.com