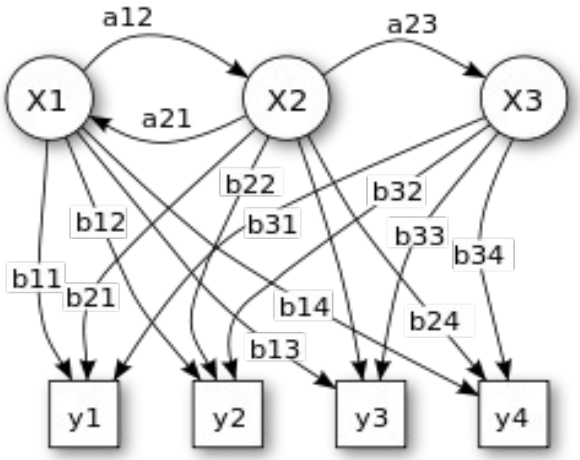
# الدليل السريع لإخفاء الهوية على الشبكة الإلكترونية

**كيف تبتعد عن المراقبة الإلكترونية و تخفي هويتك الرقمية على الإنترنت في دقائق معدودة**



# مقدمة

يعتبر هذا الكُتيب الصغير دليل سريع لأهم الوسائل المستخدمة في حماية و إخفاء الهوية الإلكترونية للأفراد ولن يأخذ من وقتك أكثر من 10 دقائق، ستتعرف خلال صفحاته على أهم البرامج لحمايتك من تعقب أثارك و ما تفعله على الأنترنت سواء على جهاز الحاسوب أو عبر هاتفك المحمول.

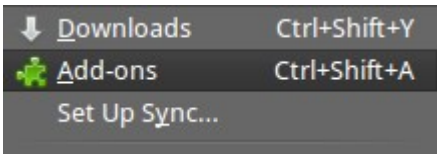
جميع الإجراءات و الأدوات الموجودة في الكتاب مجانية تماماً و مفتوحة المصدر و أغلب هذه البرامج تعتمد على التشفير و استخدام قنوات الاتصال الخفية و الآمنة عبر شبكة التشفير المشهور TOR



**عبدالله على عبدالله**

**سبتمبر عام 2013**

# الإجراء الأول: اضافات للمتصفح تمنع المواقع من تعقبك




الإضافات التالية Add-ons يمكنك تنصيبها بسهولة على متصفح الأنترنت Mozila Firefox و كذلك Google Chrome لجميع أنظمة التشغيل و تساهم في الحد من تعقب المواقع الإلكترونية لك و تتبع ما تقوم به على الانترنت، لتنصيب هذه الإضافات على الفايرفوكس توجهه إلى قائمة الأدوات Tools ثم اختار Add-ons و ابحث عن الأسماء التالية.

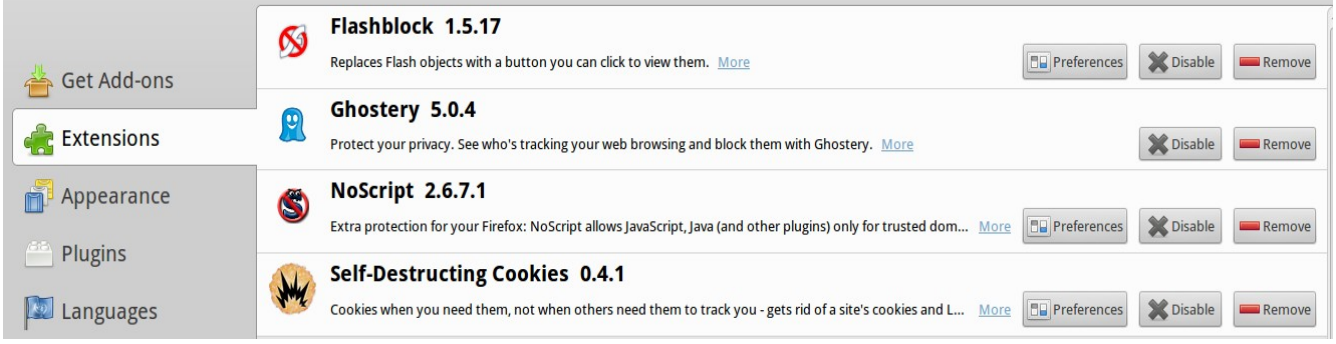
**Ghostery:** تقوم هذه الإضافة الرائعة بتعطيل أكواد التعقب الموجودة في صفحات المواقع كما تخبرك أي المواقع تحاول أن تتعقب تصرفاتك و يمكنك ضبطها لتعطيل جميع أكواد التعقب المدمجة بالصفحات أو استثناء صفحات معينة و السماح لها بتعقب تصرفاتك على الانترنت.

**Self-Destructing Cookies:** عادة تقوم المواقع بحفظ ملفات الـ cookies للتعرف على المستخدمين و تسجيل نشاطهم على الموقع و كذلك حفظ بيانات الدخول و كلمات المرور، كما تستخدم كذلك في تعقب المستخدمين و معرفة سلوكهم على مواقع الانترنت المختلفة، تعمل هذه الاضافة على تدمير جيمع ملفات الكوكيز و كذلك تسمح لك باستثناء ما تشاء من هذه الملفات و مسح البقية.

**NoScript:** تعمل هذه الإضافة على تعطيل الـ Java scripts وكذلك منع ثغرات المتصفحات و التي يستخدمها الهاكرز و المواقع لإصابة الأجهزة ببرمجيات خبيثة مثل الفيروسات و أحصنة طروادة مع ملاحظة أن بعض المواقع تستخدم الجافا سكربت في تحسين أداء و تفاعل الموقع مع المستخدم، مثل الاضافات السابقة يمكنك ان تحدد بعض المواقع لتسمح لها بتشغيل الجافا سكربت بينما تقوم بالغاء المواقع الاخرى.

**Flash Block:** مثل الإضافة السابقة الا أنها تمنع تشغيل ملفات الفلاش

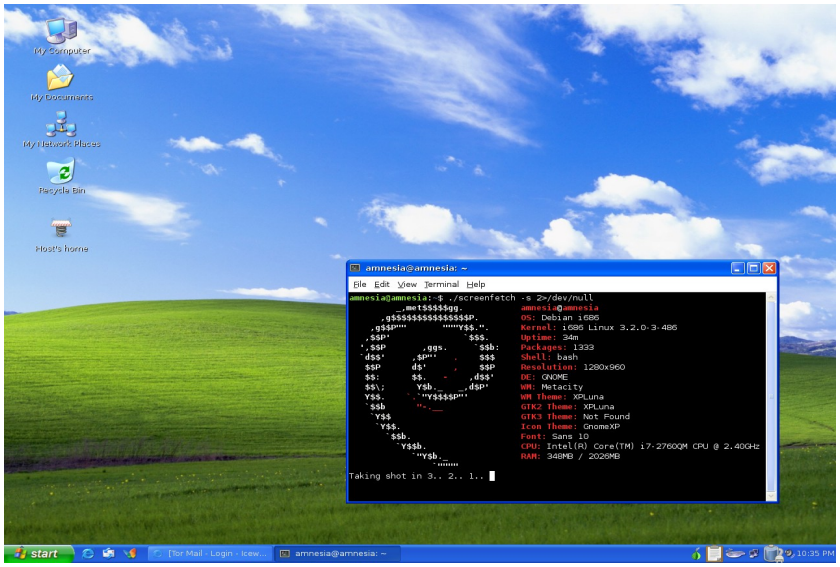
**الصورة التالية توضح جميع الإضافات بعد أن تم تنصيبها بنجاح**



# الإجراء الثاني: استخدام نظام التشغيل Tails

يضمن استخدام نظام تشغيل Tails توفير بيئة عالية الأمان و مزودة بطبقة تشفير على جميع الاتصالات الإلكترونية الخارجة و الواردة منها سواء كانت تصفح موقع Web browsing أو محادثة chat أو عملية تحميل للملفات من أي نوع حيث تمر جميع البيانات عبر سلسلة من المنافذ الخاصة من نوع socks proxy من عدة دول في شبكة التشفير TOR و عبر أنفاق خاصة encryption tunnels حتى تصل إلى الوجهة النهائية و بذلك يكاد يكون مستحيل تحديد الشخص المستقبل لهذه البيانات.

يمكن تنصيب وتشغيل هذا النظام جنباً إلى جنب مع نظام ميكروسوفت ويندوز بحيث تختار بينهما عند اقلاع الجهاز boot أو يمكن تنصيب النظام على فلاش ديسك Flash Disk أو أي هارد ديسك متنقل و بذلك يمكن تحويل أي جهاز الى منصة تواصل فائقة الأمان و عالية التشفير في خلال ثواني عن طرق الإقلاع من هذه الفلاش ديسك، يجب على جميع الأفراد الذين يودون التواصل بأمان أن يستخدموا جميعاً نظام التشغيل tails اما بتنصيبه مباشرة أو استعمال Flash Disk




**الأدوات المطلوبة (بعدد الأفراد):**

- جهاز الحاسب الآلي سواء مكتبي أو محمول
- فلاش ديسك بمساحة 4 جيجا على الأقل و يفضل مساحة 8 جيجا
- ملف الـIso لنظام Tails
- اسطوانة DVD فارغة

**المراجع:**

https://www.torproject.org

https://tails.boum.org/doc/first_steps/usb_installation/index.en.html

**من مميزات نظام tails انه يمتلك واجهه رسومية مطابقة لنظام Windows XP لذلك حتى و إن لم تكن لديك خبرة بنظام لينكس فستتمكن من التعامل بسهولة جدا مع نظام tails لما له من واجهه بسيطة مماثلة لويندوز**

# الإجراء الثالث:استخدام نظام CyanogenMOD للهواتف


هذا النظام هو نسخة صافية تماماً ومشتقة من اندرويد Android و متوفر بعدة اصدارات مناسبة لأغلب أجهزة المحمول الذكية المتوفرة بالأسواق، يمكن تنصيبه على أي جهاز محمول يعمل بأندرويد مسبقاً و تتمثل الفائدة الأساسية من استخدامة في ازالة معظم برامج التعقب التي تكون مدمجة بواسطة الجهات التالية:

- شركات المحمول Mobile Operator التي تبيع الهواتف مسبقة الأعداد للعمل على شبكة الشركة فقط
- شركات صناعة الهواتف نفسها مثل SAMSUNG و SONY
- البرامج الخبيثة التي يتم تنزيلها من الجهات الحكومية في الدولة بمساعدة مشغلي المحمول

**الأدوات المطلوبة:**

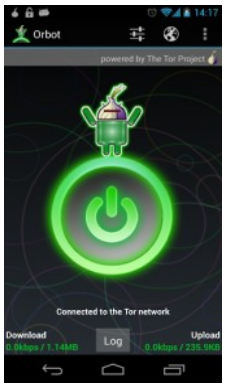
- هاتف محمول ذكي يعمل بنظام اندرويد و مدعوم من قبل cyanogenMod
- كابل USB الخاص بتوصيل الهاتف بالحاسب الآلي
- برنامج ODIN لتحميل نظام cynogenMod

**المراجع:**

www.cyanogenmod.org

*www.cyanogenmod.org/devices*

# الإجراء الرابع: تشفير بيانات الهواتف الذكية




**أولاً: برنامج Orbot للتصفح الخفي و المشفر للانترنت**

يعمل هذا البرنامج على توفير اتصال بشبكة التشفير TOR للهواتف المحمولة الذكية العاملة بنظام تشغيل أندرويد و بذلك يمكنك تشفير بيانات التصفح و التراسل الفوري chat الخارجة و الواردة إلى هاتفك المحمول عبر طبقة تشفير قوة جداً مع ملاحظة أنه يجب الاحتراس من البرامج التي يمكنها تجميع بيانات عن الجهاز و ارسالها إلى جهات مشبوهه مثل برنامج Viber الاسرائيلي فحتى و ان استخدمت شبكة TOR فسيظل البرنامج قادر على التجسس على ما تفعل في هاتفك و بالتفصيل سواء شفرت جميع بياناتك أو لم تشفرها.

باستخدامك لهذا البرنامج ستتمكن من نقل البيانات عبر الأنترنت دون أن تتمكن شركات المحمول المزود لخدمة الانترنت من التجسس عليك مع العلم أن برنامج Orbot لا يقوم بتشفير المكالمات الواردة و الصادرة على خطوط المحمول و تظل هذه الشركات قادر على التجسس على محتوى المكالمات الصوتية المارة عبرها.

**ثانياً: برنامج Ostel للمكالمات الصوتية المشفرة**

اذا احببت أن تجري مكالمة صوتية مشفرة و آمنة عليك أن تستخدم أحد برامج التواصل الصوتي عبر الانترنت المشفرة و منها برنامج Ostel و الذي يعتمد على تشفير المكالمات عبر شبكة TOR مثل باقي البرامج المذكورة سابقاً و تتوفر نسخة من البرنامج تعمل على هواتف الأيفون من شركة أبل https://ostel.co

**ثالثا: برنامج Gibberbot للتواصل الفوري المشفر Instant Messaging**

يعمل هذا البرنامج على اضافة طبقة حماية أخرى حيث يوفر خدمة التواصل الفوري باستخدام الرسائل المشفرة، حيث تم تشفير الرسالة عند كتابتها و كذلك ارسالها عبر قنوات شبكة TOR لاضافة المزيد من الحماية على الرسائل و يعتبر من أفضل البدائل للبريد الإلكتروني و برامج الـ chat

**المراجع:**

https://guardianproject.info/apps

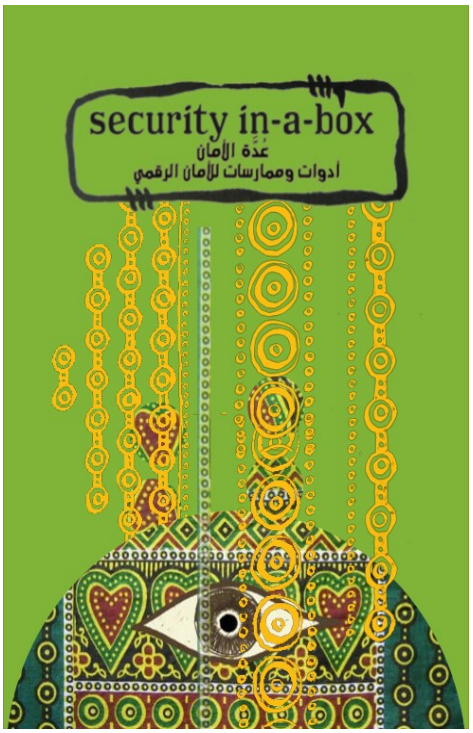
https://market.android.com/details?id=org.torproject.android

https://market.android.com/details?id=info.guardianproject.otr.app.im

# الخاتمة

جميع الإجراءات و الأدوات السابقة يجب أن تستخدم بحكمة و لتعلم أنه دائما هناك فرصة و لو ضئيلة بإمكانية تعقب أفعالك على الأنترنت حتى و ان طبقت كل الاجرائات السابقة لذلك احترس من زيارة المواقع المشبوهة ولا تكتب بياناتك الحقيقة إلا في المواقع الموثوقة فقط.

يمكنك تعلم المزيد حول أساليب الحماية و الاختفاء الرقمي عن طريق الكتب التالية (كلها كتب مجانية و مفتوحة المصدر):

| | |
|---|---|
| عُدَّة الأمان الرقمي<br>http://librebooks.org/security-in-a-box | The CryptoParty Handbook<br>https://www.cryptoparty.in/documentation/handbook |
|  |  |

أحترس مما تقول و تكتب  فالكلمات
تعيش عمراً أطول منك ..!!