مخاطر التكنولوجيا الرقمية وطرق الحماية منها

إعداد وكتابة: يوسف شعبان

مما لا شك فيه أن التكنولوجيا بصورها المختلفة أصبحت جزء لا يتجزأ من حياتنا اليومية، ولكن كما هي العادة فإن لكل شيء وجه إيجابي ووجه سلبي فإن التكنولوجيا لها العديد من المخاطر التي بدأت تتوغل في حياتنا، ستناول في هذا الموضوع ثلاثة نواحي من مخاطر التكنولوجيا وهي (الكمبيوتر – الإنترنت – هواتف الأندرويد).

أولا: المخاطر الرقمية التي تواجه مستخدم الكمبيوتر:

١- *البرمجيات الخبيثة:*

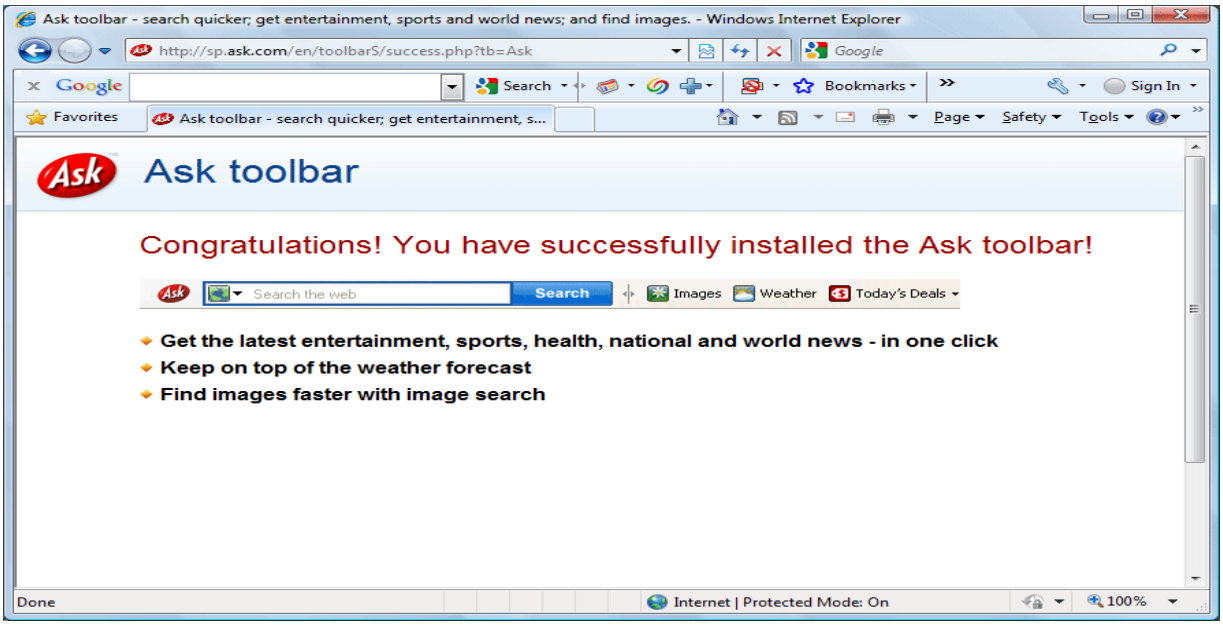
وتكون في العادة فيروسات متنكرة في شكل برامج التي تدعى أنها برامج (Software) مفيدة.

والأمثلة على ذلك كثيرة مثل برامج (Baidu Pc Faster-Baidu browser-Download.com Downloader-Free Antivirus-Ask Toolbar).

القاعدة في تجنب هذه البرامج: "أي برنامج يظهر في الإعلانات على الانترنت أو كبرنامج يثبت مع برنامج آخر فغالبا يكون ضار".

الحل: قم بإزالة كل هذه البرامج الضارة عن طريق Control panel أما إذا كانت هذه البرامج ترفض إلغاء التثبيت فيجب عليك الاستعانة بأحد البرامج المتخصصة مثل **Revo UnInstaller** ويفضل إعادة تثبيت نسخة الويندوز من جديد.

٢- *الأشرطة الدعائية:*



وأشهرها شريط ASK وغالبا ما تثبت على متصفح انترنت إكسبلورر أو تكون في شكل إضافات Extensions لمتصفحي جوجل كروم وموزيلا فاير فوكس.

الحل: تستطيع إزالة هذه الأشرطة بطريقة بسيطة وفعالة عن طريق برنامج **AdwCleaner** وهو برنامج صغير حجمه ١ ميجا تقريبا يعمل بدون تثبيت.

رابط تحميل البرنامج: https://toolslib.net/downloads/finish/1

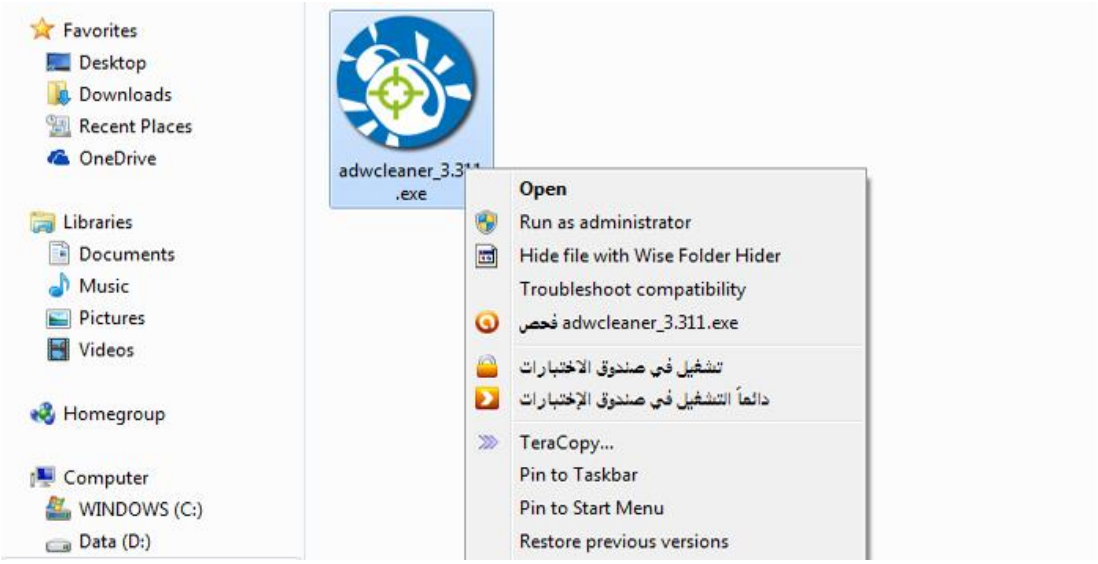
يقوم البرنامج بإزالة كلا من:

- البرامج الضارة (**Adware**).
- البرامج الدعائية (**Ads Softwares**).
- البرامج غير المرغوب فيها (**Potentially Undesirable Program**).
- الشرائط الدعائية الخاصة بالمتصفحات.
- برامج واضافات تغيير الصفحة الرئيسية للمتصفح.

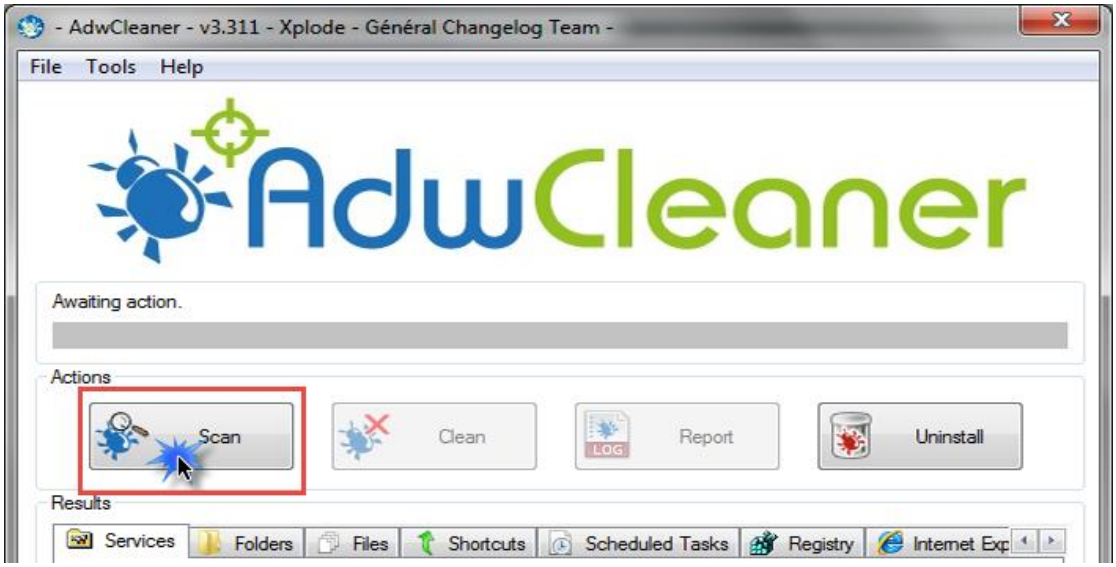
طريقة استخدام البرنامج:

١- قم بتحميل البرنامج من الرابط بالأعلى.

٢- قم بفتح البرنامج كمسئول (**Run As Administrator**).



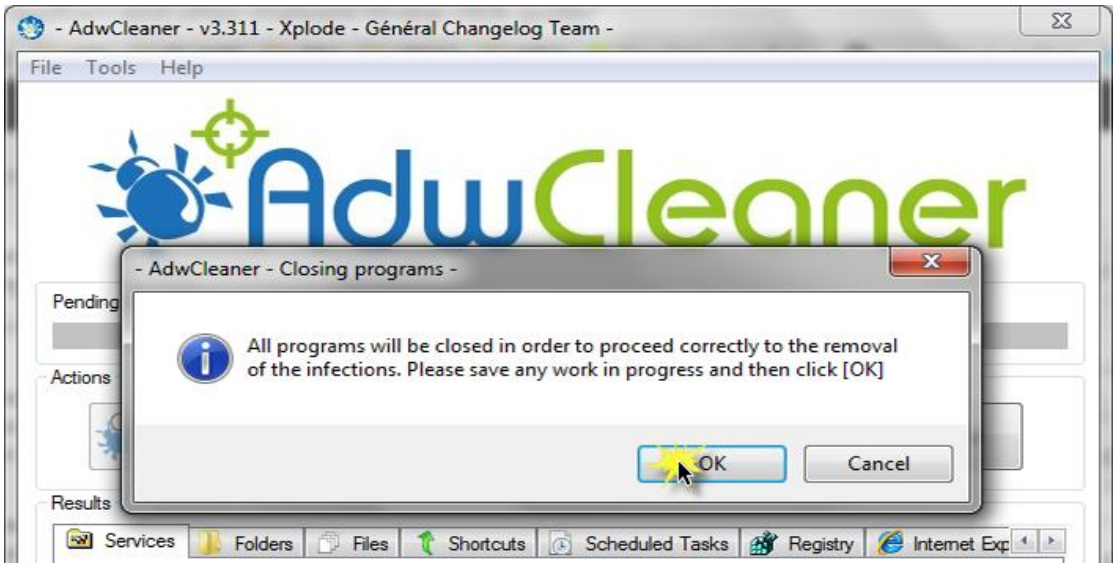
٣- اضغط على زر **Scan** ليبدأ البرنامج بفحص جهازك.



٤- ننتظر حتى البرنامج من الفحص.

٥- بعد انتهاء البرنامج من الفحص يظهر اختيار **Clean**.

٦- عند الضغط عليه يظهر البرنامج رسالة تحذيرية أنه سيتم اغلاق جميع البرامج ومتصفحات الانترنت والنوافذ المفتوحة حاليا اضغط **OK**.



٧- سيقوم البرنامج الآن بالتنظيف وبعدها ستظهر لك رسالة أخرى تخبرك بأنه سيتم إعادة تشغيل الجهاز لإتمام عملية التنظيف اضغط **OK**.

٨- بعد إعادة تشغيل الجهاز سيقوم البرنامج بعرض ملف **Log** به العمليات التي قام بها والملفات التي قام بحذفها.

```
# AdwCleaner v3.000 - Report created 20/08/2013 at 10:35:00
# Updated 20/08/2013 by Xplode
# Operating System : Microsoft Windows XP Service Pack 3 (32 bits)
# Username : User - TEST-CA133D
# Running from : C:\Documents and Settings\User\Desktop\AdwCleaner.exe
# Option : Clean

***** [ Services ] *****

[x] Not Deleted : 24x7HelpSvc
[#] Service Deleted : BackupStack
Service Deleted : CltMngSvc
[#] Service Deleted : WebCakeUpdater

***** [ Files / Folders ] *****

[x] Not Deleted : C:\Documents and Settings\All Users\Application Data\IBUpdaterServi
Folder Deleted : C:\Documents and Settings\All Users\Application Data\Tarma Installer
Folder Deleted : C:\Documents and Settings\All Users\Application Data\WeCareReminder
Folder Deleted : C:\Documents and Settings\All Users\Start Menu\Programs\24x7 Help
Folder Deleted : C:\Documents and Settings\All Users\Start Menu\Programs\PC Performer
Folder Deleted : C:\Program Files\Conduit
Folder Deleted : C:\Program Files\MyPC Backup
Folder Deleted : C:\Program Files\PC Performer
Folder Deleted : C:\Program Files\SearchProtect
Folder Deleted : C:\Program Files\Speed Analysis 2
Folder Deleted : C:\Program Files\appbario12
Folder Deleted : C:\Documents and Settings\User\Local Settings\Application Data\Condu
Folder Deleted : C:\Documents and Settings\User\Local Settings\Application Data\appba
Folder Deleted : C:\DOCUME~1\User\LOCALS~1\Temp\CT3279411
Folder Deleted : C:\Documents and Settings\User\Application Data\24x7 Help
Folder Deleted : C:\Documents and Settings\User\Application Data\file scout
Folder Deleted : C:\Documents and Settings\User\Application Data\PerformerSoft
Folder Deleted : C:\Documents and Settings\User\Application Data\SearchProtect
Folder Deleted : C:\Documents and Settings\User\Application Data\SpeedAnalysis2
Folder Deleted : C:\Documents and Settings\User\Start Menu\Programs\MyPC Backup
Folder Deleted : C:\Documents and Settings\User\Application Data\Mozilla\Firefox\Prof
```

وبهذا تكون قد اكتملت عملية التنظيف بنجاح.

٣- الفيروسات:

هي من أكثر ما يكرهه جميع مستخدمين الكمبيوتر الفيروسات، تلك البرمجيات الخبيثة التي يسعى صانعوها الى افساد متعة حياتنا وإفساد ما يمكن افساده على أجهزتنا.

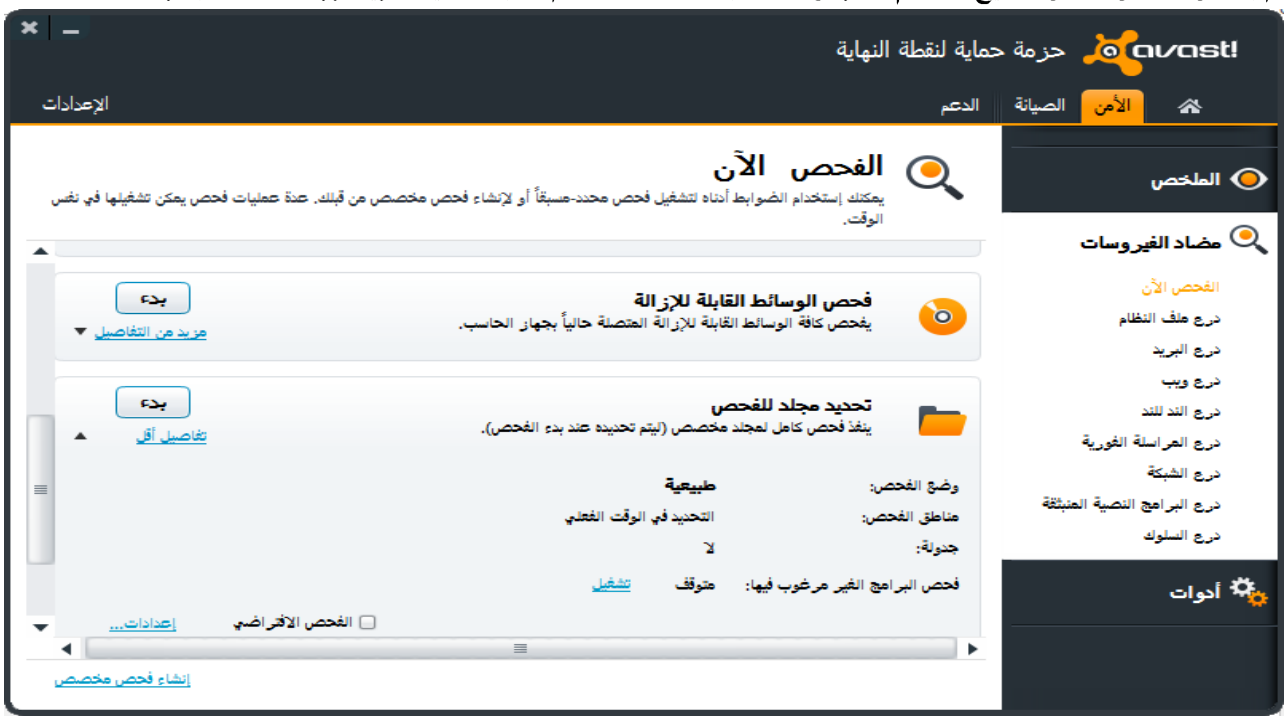
بكل حال من الأحوال إذا كان سبب الفيروس هو فلاشة أو برنامج خبيث أو تحميل من على الإنترنت فالطريقة لا تختلف كثيرا:

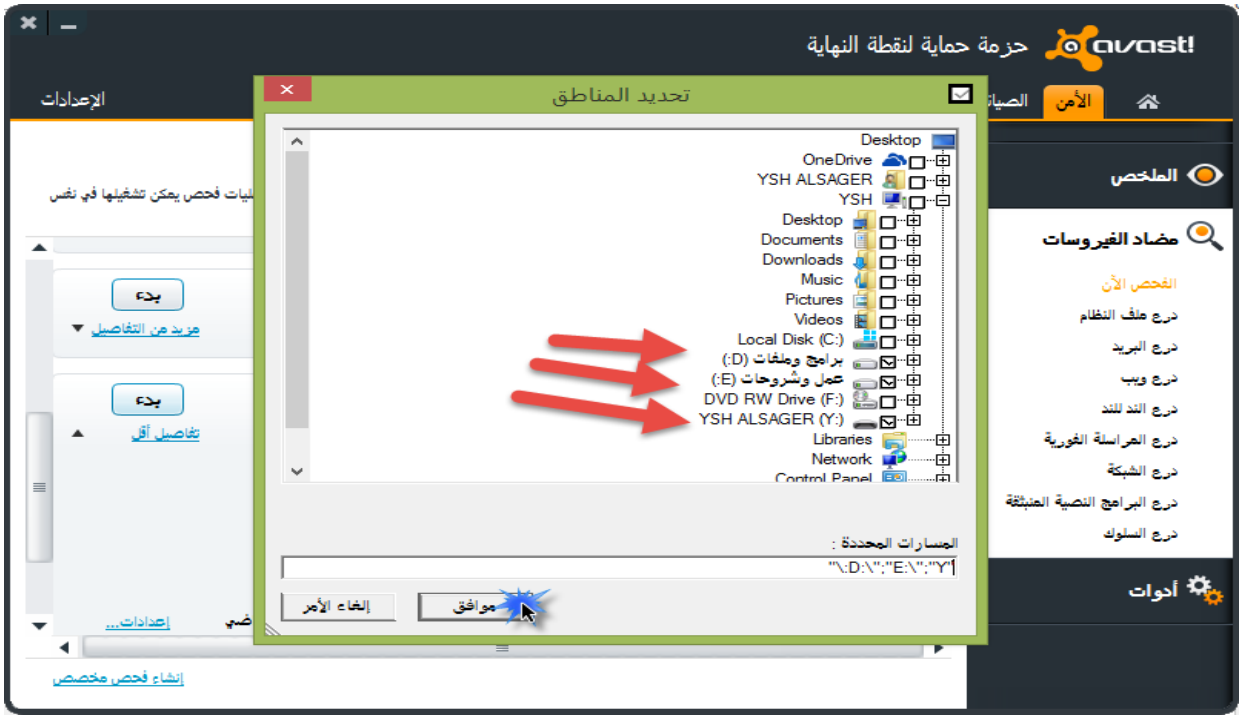
١- يفضل جدا إعادة تثبيت نسخة الويندوز من جديد (وعمل فورمات للقسم **C** أو القسم المثبت عليه الويندوز).

٢- بعد انتهاء تثبيت الويندوز إياك وأن تقوم بفتح أي من أقسام القرص الصلب.

٣- قم بثبيت مضاد فيروسات قوى مثل **Avast-Bitdefenter-Kasper** (يفضل أن يكون غير مجاني لضمان كفاءته)

٤- قم بعمل فحص كامل لجميع أقسام القرص الصلب (ماعدا القسم المثبت عليه الويندوز لأننا قمنا بفرمتته).





٥- بعد اكتمال الفحص قم بحذف جميع الملفات المصابة. (نصيحة: لا تقم بعمل اصلاح للملفات)

٦- قم بتثبيت برنامج **USB disk security** لمنع أي فيروسات موجودة على الوسائط القابلة للإزالة (الفلاشات).

الموقع الرسمي:http://www.zbshareware.com

نصائح لتجنب حدوث هذه المشاكل:

١- لا تقم بنقل ملفات من الفلاشات إلا إذا كنت تثق أنها نظيفة.

٢- لا تقم بالاستغناء عن برنامج مضاد الفيروسات لأي سبب.

٣- قم بتحديث مضاد الفيروسات أولا بأول.

٤- تجنب التحميل من المواقع غير المعروفة والمواقع المشبوهة.

٥- قم بتحميل البرامج من مواقعها الرسمية.

ثانيا: المخاطر الرقمية التي تواجه مستخدم الإنترنت:

١- الروابط الخبيثة:

وهي الروابط التي تؤدى الى الفيروسات أو البرمجيات الخبيثة أو الى مواقع احتيالية.

الحل ا: موقع **scamadviser**

الموقع يتيح للمستخدمين التأكد من هذه المواقع بسرعة ويحدد نسبة الثقة فيها ويقدم معلومات ضرورية للمتسوق عبر الانترنت للحفاظ على امنه. كل ما على المستخدم بعد فتح صفحة الموقع الرسمية وضع اسم الموقع المراد الكشف عنه في المستطيل الخاص بذلك ثم الضغط على **check it now**. ستظهر نتيجة الفحص في شكل نسبة مئوية داخل درع للحماية اصفر اللون لو ان النسبة أكثر من ٥٦ في المئة فالموقع صادق ويمكنك التعامل معه. وإذا كانت أقل من ذلك فابتعد عن الموقع لأنه نصاب أو يمارس الاحتيال مع اعضائه. ويحصل الموقع الجدير بالثقة ١٠٠٪ على درع حماية اخضر اللون .

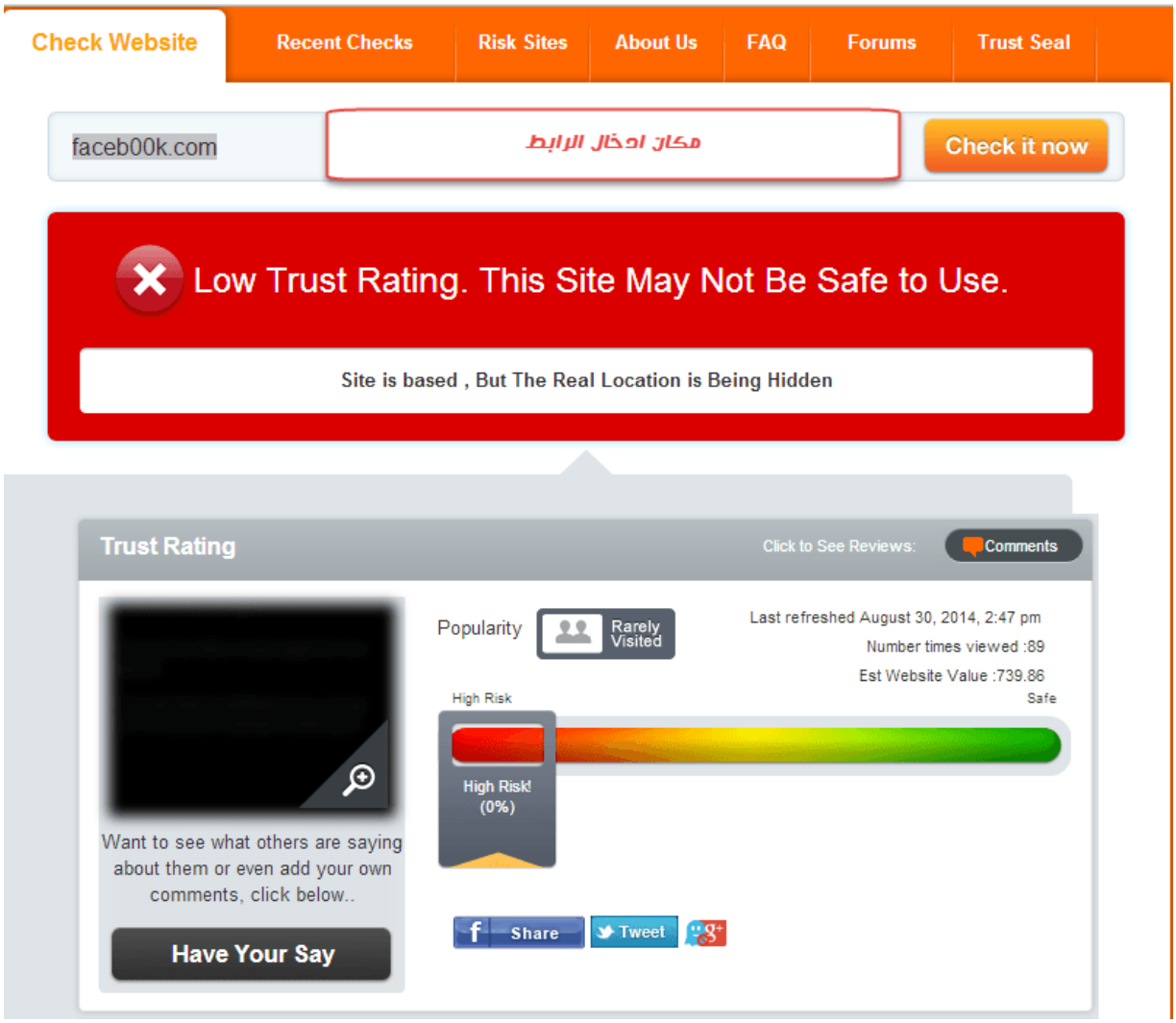
يتيح الموقع بيانات عن المواقع المراد الكشف عنها مثل سرعة الموقع وبلد المنشأ ويوضح إذا كان يستخدم برنامج اخفاء للهوية او برامج عدم التتبع وكذلك ترتيبه على موقع اليسكا وتحليل بسيط عنه. ويسمح الموقع للمستخدمين بالتعليق على النتائج مع امكانية رفضها من خلال الضغط على **report a false positive**

لإرسال رسالة الى الموقع وشرح اسباب رفض التقييم وسيقوم الموقع بعد ذلك بفحصة واعادة تقيمه .

ويشير الموقع الى انه مجرد دليل مساعد للمستخدم لتقيم المواقع ويجب عدم اغفال حس المستخدم (نحن نبذل قصارى جهدنا لتوفير تصنيف دقيق ومدروس ولكن من الضروري معرفة أن الشركات يمكنها أن تتلاعب باستخدام تقنيات خفية للتظاهر أو اخفاء هويتهم الحقيقية تحت عباءة. لا يمكننا ضبط وتقديم تقرير عن كل موقع واحد في كل مرة حتى الان على الاقل) .

ويختلف هذا الموقع عن نظائره امثال جوجل. نورتون. مكافى وغيرها التي تقدم تقرير عن تلك المواقع معتمدين على معايير فيروسات او معايير اجتماعية معينه. اما موقع سكام ادفيزر يحاول دمج عدة مصادر مختلفة للمعلومات وتقديم تقرير معلومات أكثر تفصيلا مثل مكان نشأة الموقع حقا. ويقوموا بتغير أنظمة البحث والاستنباط باستمرار حتى يتمكنوا من التقاط تلك المواقع الخبيثة. فهناك الكثير من المواقع الوهمية الخادعة التي تظهر والموقع يساعد على توفير البيانات للمساعدة في تحديدها .

ويمكن من خلال الموقع الكشف عن اخر ٢٠ موقع تم فحصهم وكذلك اخر ٢٠ موقع غير آمن تم الكشف عنهم. قدم الموقع ما يقرب من ٥,٥ مليون كشف بمعدل ٤٨ كشف في اليوم الواحد ووجد منهم ٤٩٠ ألف موقع خطر.



الحل ٢ (الأفضل): أن تستعمل مضاد فيروسات يقوم بحماية الانترنت أيضا (Internet Security /Total Security).

الحل ٣ (بالنسبة لحسابات الفيس بوك):

توجد العديد من الروابط التي تظهر في حسابنا على الفيس بوك، فإما هي لصفحات معجبين بها او اصدقاء يشاركونها، هكذا فإن امر تحديد سلامة الروابط مهم بنسبة كبيرة لتفادي الاختراق او التحايل، لهذا فإن تطبيق كـ **Norton Safe Web** للفيس بوك سيمكنك من تحديد سلامة تلك الروابط عبر فحصها كليا قبل النقر عليها، حيث يمكن الرجوع إلى التطبيق في كل مرة شككت في رابط معين او في مجموعة من الروابط الصادرة عن صفحات او اصدقاء خلال اخر ٢٤ ساعة.

كل ما عليك هو تثبيت التطبيق **Norton Safe Web** على حسابك في الفيس بوك حيث سيفتح اوتوماتيكيا لعمل مسح للروابط المتواجدة في حسابك، كما انه سيعمل على ترتيبها في تصنيفات حسب درجة خطورتها. (**norton secured safe caution warning**) كل ما عليك هو النقر على التصنيفات من اجل تحديد الروابط الخطيرة او السليمة على حسابك كما هو مبين في الصورة اسفله.

٢- *البرامج المزيفة:*

سبق التحدث عنها بالتفصيل بالصفحة رقم ١.

أيضا عند تصفح المواقع الإلكترونية لا تقوم بتنزيل برامج الحاسب الغير معروفة.

٣- *الإعلانات المزعجة:*

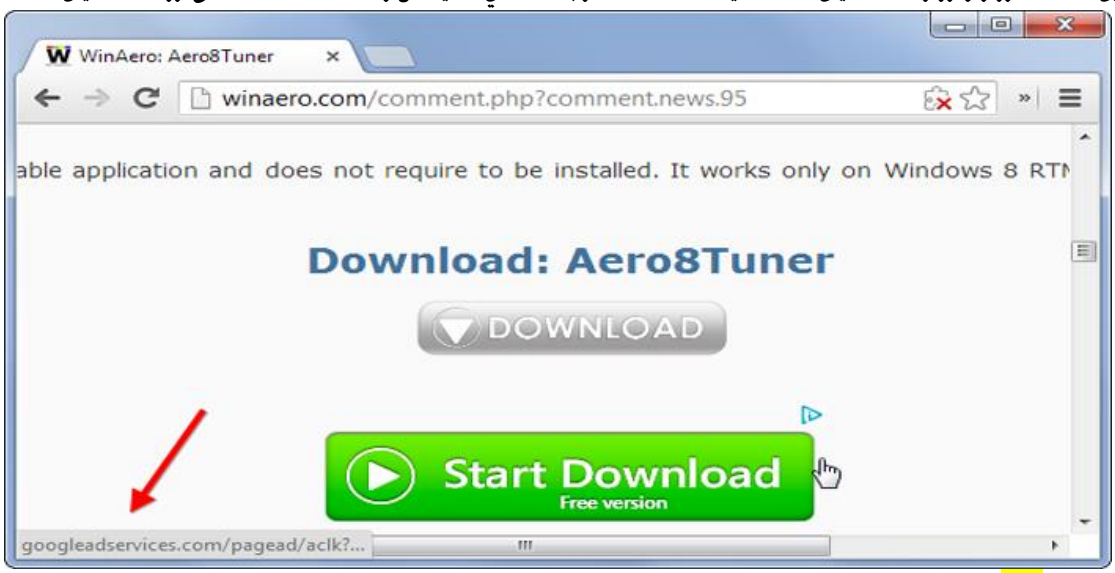
تمتلئ شبكة الإنترنت بالبرامج الدعائية والإعلانات المزعجة وروابط التحميل المزيفة والتحذيرات الكاذبة والنوافذ المنبثقة والعديد من هذه الأشياء التي يكرها جميع مستخدمي الإنترنت.

أولا: كيفية التعرف على روابط التحميل المزيفة:

١- عندما نقوم بالدخول على معظم مواقع التحميل أو عندما نبحث عن البرامج المجانية نجد العديد من أزرار التحميل كما بالصورة. هذه الأزرار تكون ملونة وكبيرة ولامعة حتى تخدع المستخدم. وليس هذا فقط بل وتجد مكتوب عليها **Start Download/Free Download/Download Now** عند الضغط على أحد هذه الأزرار يقوم الموقع بتحميل ملف غير الملف المطلوب وغالبا ما يكون ملف ملغم ذو امتدادين (**.rar.exe**) مثلا.

هذه الأزرار المزيفة ما هي إلا عبارة عن إعلانات لربح المال عن طريق الضغط عليها (تخيل معى كم عدد الأشخاص الذين يضغطون على مثل هذه الأزرار كل يوم مما يدر أموال طائلة على الأشخاص الذين يضعون هذه الإعلانات).

للتمييز بين هذه الأزرار وأزرار التحميل الصحيحة لاحظ الرابط الذي سيظهر عندما تقف على زر التحميل:



إذا وجدت كلمة AD في الرابط فأعلم أنه اعلان على الفور.

غالبا يجب أن يقودك الرابط الأصلي الى الملف المرفوع على نفس الموقع.

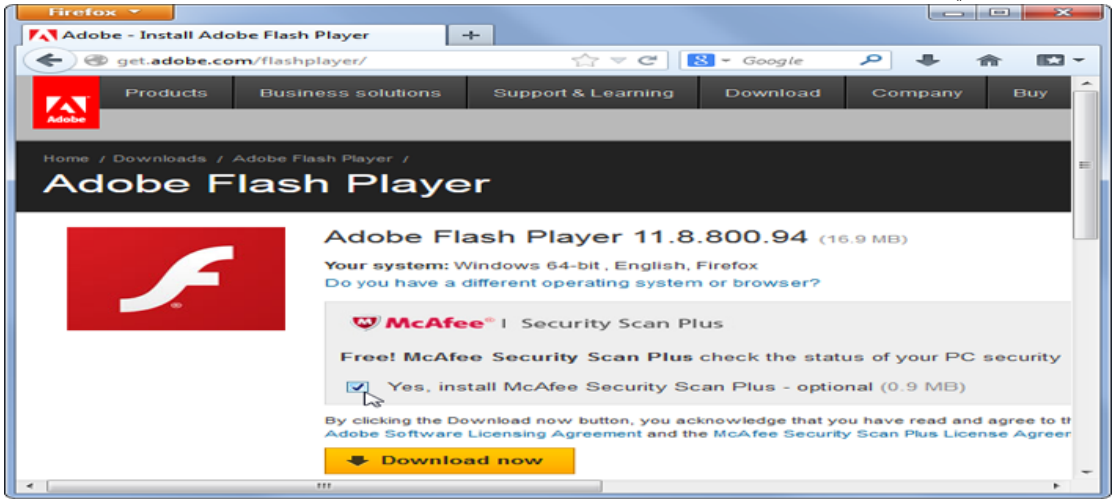
٢- البرامج الدعائية المدمجة مع البرامج المحملة من الانترنت:

تقوم معظم البرامج المحملة من الانترنت بوضع اختيار افتراضي لتحميل برامج مساندة أخرى أو برامج موصى بها من قِبل الشركة (وهذه البرامج ما هي إلا برامج دعائية مزعجة ليس لها أي استخدام مفيد).

على سبيل المثال برنامج أدوبى فلاش:

فعندما تقوم بتحميل البرنامج من الموقع الرسمي تجد انه بشكل افتراضي سيتم تحميل برنامج **McAfee Security Scan Plus** إذا لم تقم بإزالة هذا الاختيار سيتم تثبيت برنامجين على جهازك.

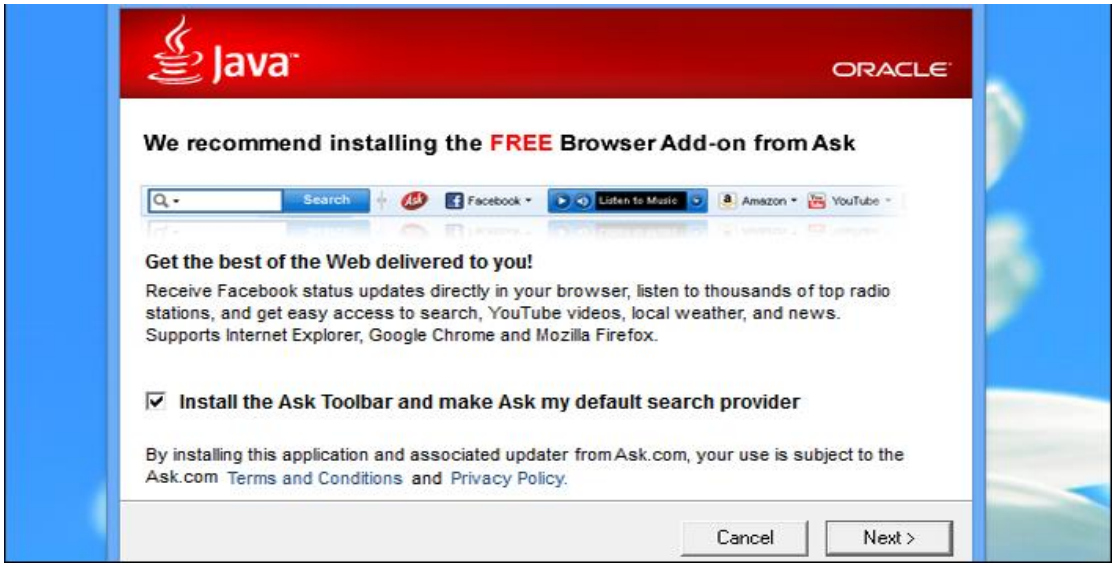
لذلك يجب عليك إزالة أي علامات قبل التحميل لتجنب تحميل هذا النوع من البرامج.



٣- البرامج المزعجة المدمجة مع ملفات البرامج:

هذا النوع من البرامج المزعجة يقوم بتحميل شرائط واضافات للمتصفحات والتي تقوم بدورها بعرض الإعلانات المزعجة داخل المتصفح ولعل أشهر هذه الأشرطة هو شريط **ASK** المزعج الذي يوجد في معظم البرامج.

على سبيل المثال برنامج الجافا:

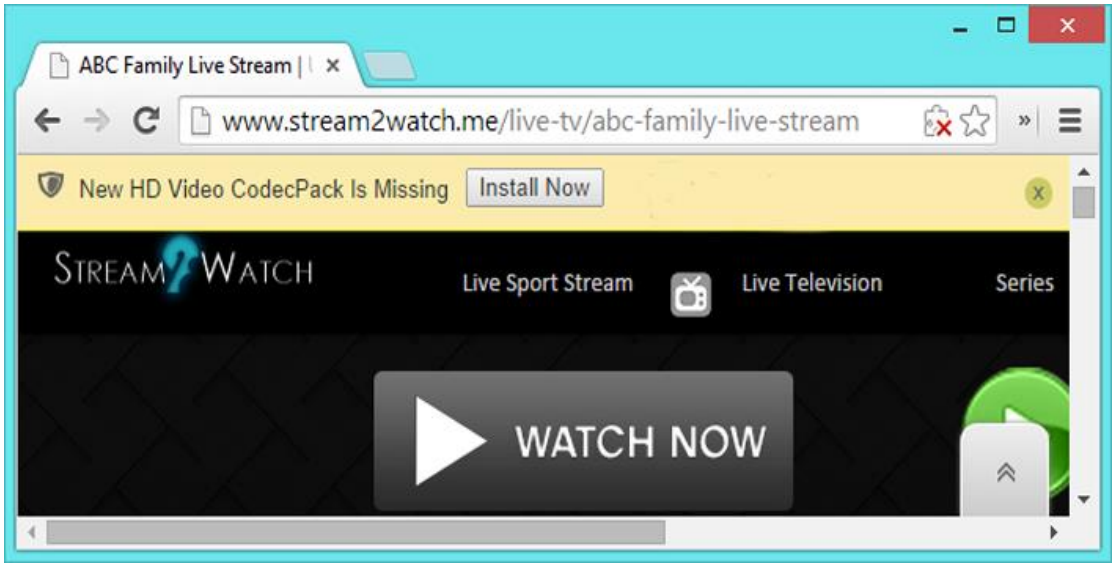


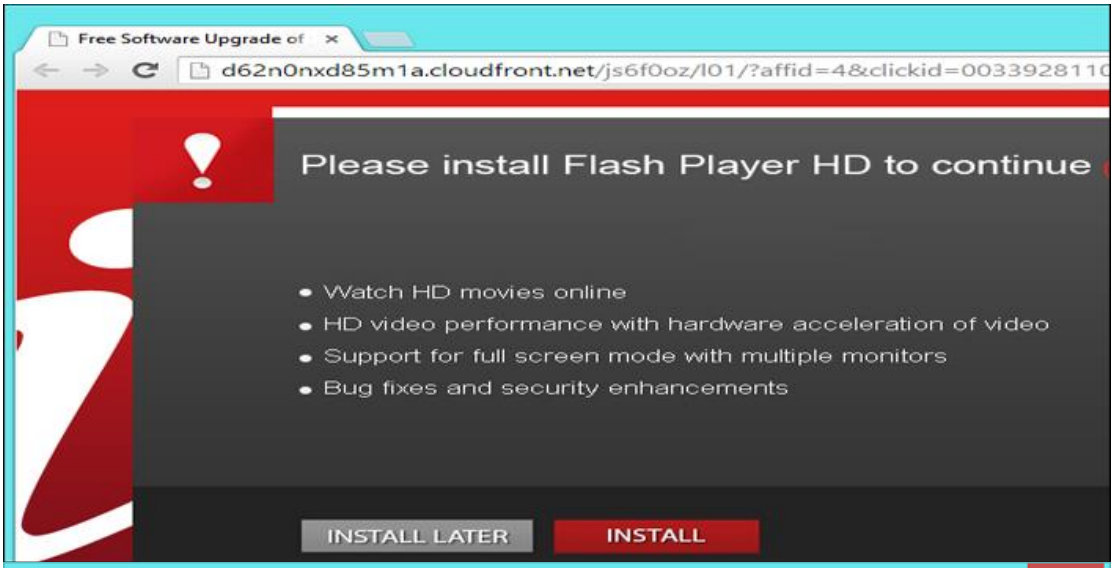
كما ذكرت من قبل تأكد من العلامات الموضوعة ولا تقم بضغط **Next** دون أن تقرأ المعلومات.

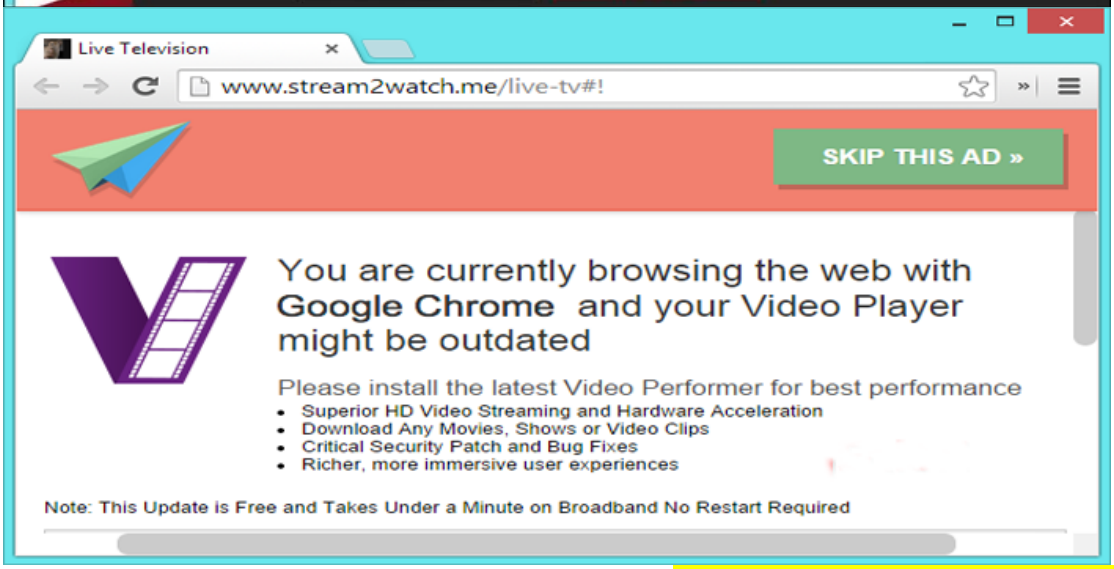
٤- برامج الكوديك والوسائط:

يجب عليك الحذر كل الحذر من تحميل هذه البرامج بالكامل فهذا النوع بالتحديد هو فيروسات وتروجان.

صور لهذا النوع:







الحل النهائي لتجنب كل هذه المشكلات:

قم بتحميل إضافة **Adblock Plus** لمنع ظهور الإعلانات نهائيا:

١- قم بالدخول الى موقع الإضافة من هنا.

٢- قم باختيار المتصفح الذي تستعمله ومن ثم ثبت الإضافة.

٣- بعد انتهاء تثبيت الإضافة لن تجد أي إعلانات أو ازرار تحميل مزعجة نهائيا.

هذا هو زر التحميل الحقيقي الوحيد الموجود بالموقع وباقي الأزرار قد اختفت لأنها مجرد اعلانات.

٤- *التصيد (وخصوصا على موقع الفيس بوك)*:

هي طريقة للحصول على كلمة سر مستخدم لخدمة ما أو موقع ما على الإنترنت. تعتمد الطريقة على إيهام الشخص المستهدف بأنه على الموقع الصحيح المعتاد حيث يدخل كلمة سره عادة للدخول إلى حسابه على الموقع (كموقع البريد الالكتروني) لكن في الحقيقة يكون الموقع موقعا "فاسدا ومزيفا" يديره أحد لصوص كلمات السر. بالتالي إذا خدع المستخدم وأدخل كلمة سره في ذلك الموقع تصل كلمة السر بكل بساطة إلى الهاكر.

الحل: قبل إدخال أي كلمة في صفحة ما على الإنترنت تأكد من النقاط التالية:

١- أنّ العنوان صحيح.

٢- أنّ البروتوكول المستخدم هو بروتوكول **Https**.

٣- وجود رمز القفل بجوار العنوان.

ثالثا: المخاطر الرقمية التي تواجه مستخدم هواتف الأندرويد:

١- *الإعلانات المزعجة (مرة أخرى)*:

هل لديك هاتف أندرويد؟ اذن تعاني من الإعلانات المزعجة التي تملأ غالبية التطبيقات المجانية. بالطبع يمكنك تحمل الإعلانات السفلية. أما الإعلانات التي تملأ الشاشة فأنا عن نفسي لا أطيقها وقد يصل الحد الى أن أقوم بإلغاء تثبيت هذا التطبيق الذي يفرض الإعلانات على المستخدم.

بعد بحث طويل عن الحل وجدت تطبيقين رائعين لمنع جميع الإعلانات التي تكون على اتصال الواى فاى ولكن للأسف التطبيقان غير موجودين على جوجل بلاي. اليكم التطبيقان:

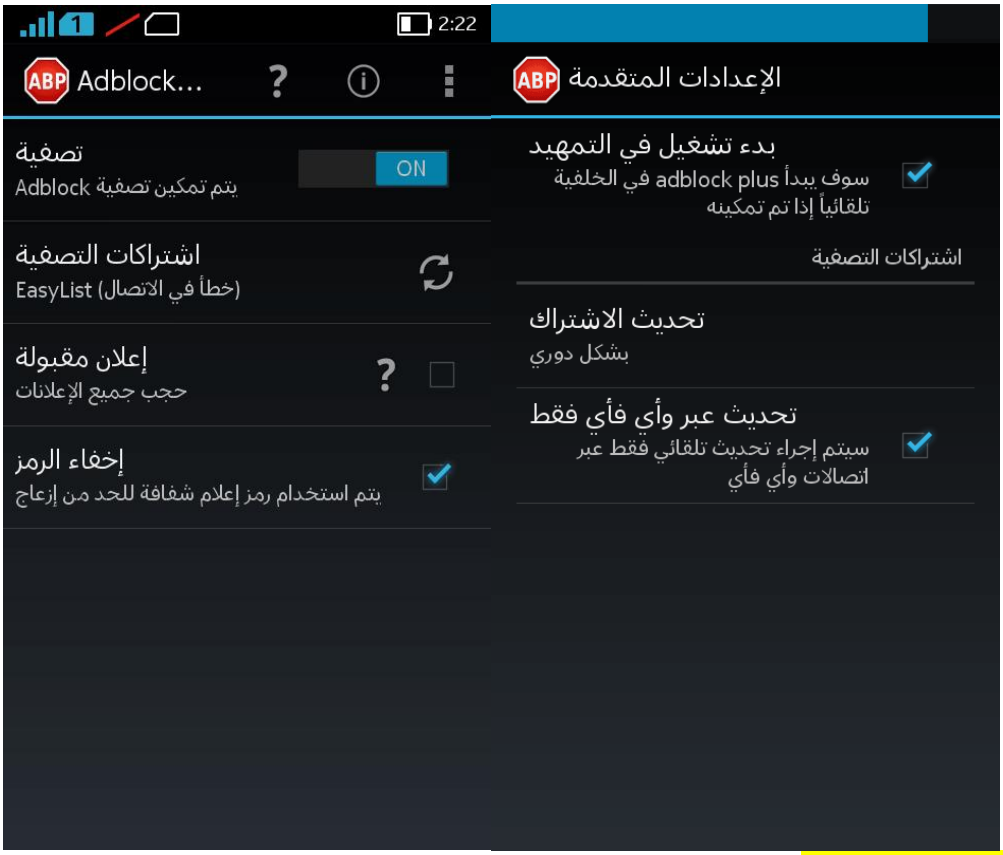
التطبيق الأول هو: Adblock Plus

ميزات هذا التطبيق: يقوم بمنع جميع الإعلانات دون الحاجة لوجود صلاحيات الرووت (لا تعلم ما معنى رووت اقرأ الموضوع من هنا).

تحميل **Adblock Plus** (الحجم ٣,٢٢ **Mb**).

حمل من هنا

صور من التطبيق:



التطبيق الثاني هو: Adaway

يعمل هذا البرنامج على أندرويد ٢,١ أو أحدث، ولكن عيبه الوحيد أنه يحتاج لصلاحيات الروووت من أجل منع الإعلانات.

وهو التطبيق المفضل لدى والذي أنصحكم بتثبيته.

حمل تطبيق **Adaway** (الحجم ٢,٩ **Mb**).

حمل من هنا

كيفية تثبيت التطبيقين:

حمل أحد التطبيقين من الروابط الموجودة بالأعلى (لا أنصح بتثبيتهما معا).

قم بفتح التثبيت من مصادر غير معروفة.

قم بثبيت التطبيق واستمتع بتطبيقات خالية من الإعلانات.

٢- *التطبيقات الدعائية والفيروسات:*

هما عنصران مرتبطان ببعض بصلة وثيقة ويرتبطان أكثر بالإعلانات فإذا منعت الإعلانات من الوصول لهاتفك فأنت في أمان.

بعض النصائح لتجنب التطبيقات المزيفة والخبيثة على متجر جوجل بلاي:

١- عند الرغبة في تثبيت أي تطبيق يجب التأكد من الصلاحيات التي يطلبها، فمن غير المعقول أن يكون تطبيق المُنبه يطلب صلاحيات للوصول إلى الصور أو الأسماء أو الرسائل، لذا يجب تجنب هذا النوع من التطبيقات من خلال قراءة الصلاحيات.

٢- بعض التطبيقات تنتشر على أنها تطبيقات لإطالة عمر البطارية أو توفير مساحة تخزين إضافية لكن في الحقيقة تقوم فقط بعرض الإعلانات أو سرقة بيانات المستخدم. لذا ومع هذا النوع من التطبيقات يجب التأكد من موقع مطوّر التطبيق ومحاولة الحصول على رابط التحميل من الموقع الرسمي للشركة.

٣- بعض التطبيقات تتوفر للتصوير بأشعة x التي تُعرف بـ **X-Ray**. كشف الكذب. إعادة شحن البطارية أو الربح مادياً. هذا النوع من التطبيقات ٩٩٪ خبيث ويجب تجنبه تماماً.

رابط المدونة: www.efhamtechnology.blogspot.com

المدونة على مواقع التواصل الاجتماعي: