## إشارات تدل على وجود برامج تجسس:

# هل أنت مُراقب؟

نظرة شاملة للحماية

من الأختراقات وملفات التجسس Windows

إعداد وتقديم \\: عزالدين إبراهيم

# مقدمة

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

إن الحمد لله، نحمده ونستعينه ونستغفره ونستهديه، ونعوذ بالله من شرور أنفسنا وسيئات أعمالنا من يهده الله فلا مضل له، ومن يضلل فلا هادي له وأشهد أن لا إله إلا الله وحده لا شريك له، وأشهد أن محمداً عبده ورسوله من يطع الله ورسوله فقد رشد، ومن يعصهما فإنه لا يضر إلا نفسه ولا يضر الله شيئا.

**بداية يا أخواني الأعزاء اود ان الفت انتباهكم إلى ان هذا الكتاب مُرخص تحت رُخصة CC على النحو التالي:**

**النِسبة : يَجب عَليك ان تُنسبَ الكتاب بصفتهُ الخَاصة إلى المُؤلف أو المُرخص.**

**غَير تُجاري : لا يُمكن أستخدام هذا الكِتاب لأغراض تُجارية بتاتاً.**

**انشُر بالمَثل : إذا غيرت في الكِتاب أو حَولته أو أضِفت له , يَجب عَليكَ نَشر العَمل النِهائي بنفس الرُخصة التي حَصلت عَليها بهذا الكِتاب.**

**لإعادة أستخدام او التوزيع يجب عليك التأكد من توضيح شروط رُخصة الأستخدام للأخرين , اي أن هذه الشروط يمكن أن لا يُعمل بها إذا حصلت على تَرخيص من صاحب الملكية فقط.**

**إذا رغبت في أستغلال هذا العمل لغرض تجاري أو نشر في مجلة أو في وسائل نشر تجارية فيرجى الأتصال بنا على البريد الألكتروني التالي:**

Ezz313@gmail.com

## أهدي هذا العمل

**الي**

والدي العزيزين رمزي للعطاء والحب وكل شيء في حياتي بعد الله سبحانه وتعالى.

الي كل المنتديات العربية التي تدعم تطوير الأمن والحماية وتبادل الخبرات.

الي كل طالب عِلم يرغب في التَعلم.

الي منتديات مكتوب , الحاسب في حياتنا , العاصفة , المشاغب , المعرفة , سيكيورتي كودرز , و ترانيدنت.

أشكركم جميعاً

# حول الكتاب

- نشر الوعي الألكتروني حول كثير من المغالطات في عالم مصطلحات الأمن والحماية الأمنية.

- هذا الكتاب ليس به أي شروحات لطرق أختراق الأجهزة أو البريد الألكتروني , فهو كتاب للحماية من هذه الهجمات فقط لا أكثر ولا أقل.

- هذا الكتاب لإغراض تربوية تعليمية فقط والمؤلف غير مسئول عن الأضرار أو سوء الأستخدام.

- هذا الكتاب يتحدث عن الحماية من الأختراقات وملفات التجسس وسرقة البريد الألكتروني في أنظمة التشغيل ويندوز.

- أرجو المعذرة والتنبيه عن أي غلطات إملائية او تقنية في الكتاب الألكتروني إن وجد ونرحب بأي مقترحات أضافية حول الكتاب على البريد الألكتروني التالي:

**Ezz313[at]gmail[dot]com**

# الفهرس

الدرس الأول

# 1 – أسباب الأختراق والضعف الأمني


## أولاً : أسباب الأختراق

لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها إلى عالم الوجود. وقد أجمل المؤلفون الثلاثة للمراجع التي استعنت بها في هذه الدورة الدوافع الرئيسية للاختراق في ثلاث نقاط أوجزها هنا على النحو التالي :

1- الدافع السياسي والعسكري: مما لا شك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي والتجسسي بين الدولتين العظميين على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغيير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاعتماد كلياً على الحاسب الآلي وعن طريقه أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.

2- الدافع التجاري: من المعروف أن الشركات التجارية الكبرى تعيش هي أيضاً فيما بينها حرب مستعرة (الكوكا كولا والبيبسي كولا على سبيل المثال) وقد بينت الدراسات الحديثة أن عدداً من أكبر الشركات التجارية يجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم.

3- الدافع الفردي : بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة إلى تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الإنترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية. بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على انظمة شركاتهم السابقة مقتحمينها ومخربين لكل ما تقع أيديهم عليه من معلومات حساسة بقصد الانتقام. وفي المقابل هناك هاكرز محترفين تم القبض عليهم بالولايات المتحدة الأمريكية وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية السي آي أيه وبمكتب التحقيقات الفيدرالي الأف بي أي وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة إليهم.

نأتي الأن للشباب العربي وسبب معظم الشباب العربي أو ما أسميهم أنا أطفال الأسكربت Script Kids , هم مجرد أطفال في الحقيقة , قد لا يتعدى عمرهم الواحد منهم 12 عاماً , يبحثون عن سكربت في أحد مواقع السيكيورتي وكل ما عليه أن يقوم بنقل هذا الأسكربت Copy ثم Past ليقوم بأختراق الموقع هذا سواء موقع أو جهاز وبعد ما يخترقه يقول انا الهاكر الأوقى بالعالم من يتحدى؟؟ أنا السفير انا قاهر القلوب و و و و وهو في الحقيقة , لا يعلم اي شيء بأي شيء , واذا سألته عن هذا السكربت الذي استخدمه في الأختراق وما وظيفته؟ او ماذا يعمل؟ ولماذا؟ لا يعرف شيئاً سوا انه اخترق الجهاز فقط , وهذا هو ما كان يرغب فيه , المشكلة بهذه الأمورالكثيرة المعقدة بالنسبة لهذا الشخص وكل ما يدور برأسه فقط هو ان يخترق هذا الجهاز او الموقع ولا يهمه كيف؟ او لماذا؟

في الأيام الأخيرة تتكررت بأستمرار عمليات الأختراقات لأن برامج الأختراق المشفرة أنتشرت كثيراً بين الأطفال , وهم في الحقيقة ليسوا بمخترقين او هاكرز محترفين , أغلبيتهم أطفال لا يتعدوا عمرهم ال 12 عاماً فقط , وهم يأملون ان يكونوا مخترقين في يوم من الأيام , ولكن كل همه هو مجرد اثبات وجود , او قلة عقل , او فرد عضلات , لا أكثر ولا أقل.

يخترقك ويقول لك مزاجي او كل يوم بخترقكم , وكثير بنشاهدها من العرب ولا أعلم لماذا لا يذهب هؤلاء الأشخاص بدلاً اختراق مواقع عربية وأجهزة عربية الي اختراق الاجهزة اليهودية او موقع يهودي مثلاً او موقع جنسي يجعله الله بشرة خير له يوم القيامة على عمل الخير , وغيره من أمور قد يكسب من وارئها خبرة كبيرة في أمن وحماية مواقعه العربية ولكن طبعاً لا يستطيع لأن حمايتهم تفوق قدارته وهو لا يرغب في التعلم هو يرغب في فرد عضلاته فقط و بدون اي معرفة في كيف تعمل كل هذه الأمور هو فقط مطبق للأوامر.

" ملحوظة مهمة للجميع : الشخص الذي يعلم كيف يتم الأختراق فهو ايضاً يعلم كيف يتم الحماية سواء كان جهاز او سيرفر لأن عقله الأن اصبح يفكر كما يفكر المخترق , ولذلك فأن متعلم الأختراق يستطيع حماية نفسه من الأختراق هو نفسه متعلم الحماية الأثنين سواء في مجال واحد هدفهم شيء واحد وهي "الأمن والحماية" سَواء كَسر شفرتها وأختراقها أو حمايتها.

## ثانياً : الضعف الأمني

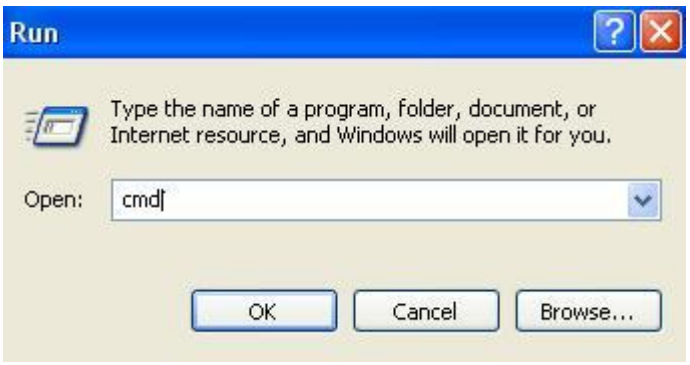
معظم الأجهزة او الأشخاص الذين يستخدمون Windows XP وبالرغم من تثبيت برامج الحماية مثل Norton أو NOD32 أو Kaspersky وتفعيل الجدار الناري Firewall للويندوز ولكن للأسف بعد كل هذا الأمن والحماية الموجود يتم اختراقهم ولا يعلم كيف تم ذلك. المشكلة هو في الوعي الفردي في الأمن , لأن معظم هؤلاء الأشخاص يعتقدون أن برامج الحماية فقط هي كل شيء.

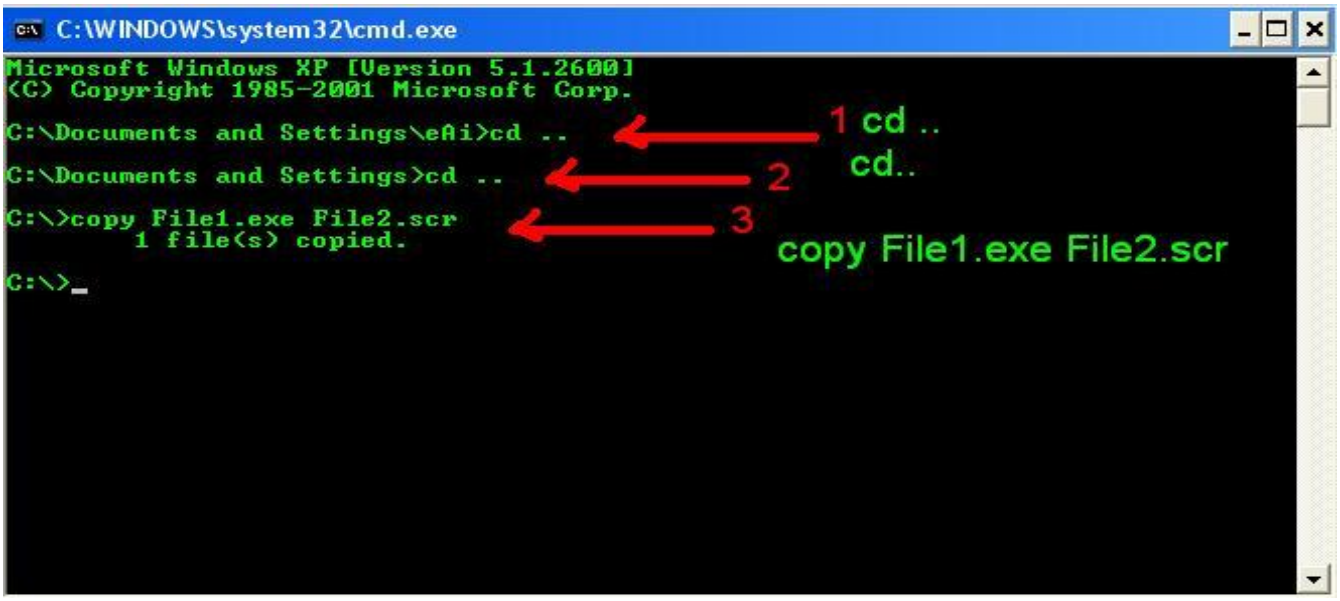
سوف أخبرك كيف يتم اختراقك وما هو الضعف الأمني الموجود لكي يتم المخترق اللوج بجهازك , المشكلة ليست بالنظام فقط بالتحديد ولكن من برامج الحماية ايضاً هذه وقل كفائة الجدار الناري و قلة الوعي الفردي في الأمن والحماية كل هذه الامور و أن في بعض الأحيان هناك فيروسات وتروجانات قد لا يكتشفها هذه البرامج اذا لم يتم تحديثها وفي بعض الأحيان لا يكتشفها بعد التحديث او ان هذه الفيروسات او التروجانات قام الشخص الذي ابتكرها بتشفيرها من برامج الحماية هذه حتى لا يتم أكتشافها. ولذلك توخ الحذر جداً من هذه النقطة السابقة.

الضعف الأمني موجود بالملفات التفيذية بالتحديد exe. او bin. , يتم بواسطة هذه الملفات التنفيذيه بأعطاء أوامر للنظام بفتح منفذ أو بورت PORT خاص للنظام , واذا كانت هذه الملفات مدموجة بفيروس او تروجان قد تؤدي لوقف برامج الحماية في جهازك وتخريبه قبل اكتشافها , مما قد لا يكتشفها برامج الحماية قبل الكشف عنها على ان هذا الملف التنفيذي فايروس , واذا كان تروجان لهاكرز فعند تفعيل فتح المنفذ او البورت بالنظام يستطيع المخترق من خلال هذا المنفذ او البورت PORT بالتحكم الكامل بجهازك وملفاتك. عن طريق برامج الأختراق او ما يطلق عليها Remote Desktop وهو برامج يتم بواسطتها التحكم بالجهاز عن بُعد الفكرة مقتبسة عن مقاهي الأنترنت تماماً عندما تكون في مقهى أنترنت مثلاً , فصاحب المقهى يملك الصلاحيات لكي يغلق جهازك ويقوم بفتحه من جهازه , وايضاً يستطيع مراقبة جهازك وهو على مكتبه ولكن في هذه الحالة لا نعتبر هذا أختراق بالمعنى الصحيح ولكنه تحكم عن بُعد , مثله مثل برامج الأختراق , فهي تعتبر برامج التحكم في الأجهزة عن بُعد , ولكي تستطيع التحكم بالجهاز عن بعد يجب على الجهاز المستهدق قبول هذا الأمر او الطلب الذي يطلبه المخترق او السيرفر وهو السيطرة والتحكم الكامل بالجهاز عن بُعد , ويتم ذلك عن طريق السيرفر او بمعنى أخر التروجان او ملف التجسس هذا , ويتم بواسطة هذا الملف التنفيذي بتخريب ووقف برامج الحماية في جهازك عن العمل , "حتى واذا قمت بتثبيت برنامج حماية وتحديثه" , لذلك يجب أن تعلم ان برامج الحماية التي في جهازك ليست هي كل شيء في الحماية الأن يستطيع المخترق تشفير الفايروس حتى لا يتم أكتشافه من قبل برامج الحماية.

هناك حيل كثيرة يتعبها المخترقون يجب ان تتوخ الحذر منها مستقبلاً وهو ليس كل ملف .exe او .bin هو ملف تجسسي او تروجان لأن بأستطاعة المخترق ان يدمج اي ملف تنفيذي exe او .bin بصورة او ببرنامج معروف عالمياً مثل الياهو او الأم اس ان وغير ذلك من أمور كثيرة , فمثلاً يستطيع اي مخترق ان يحول ا ي ملف تفيذي .exe الي ملف .JPG صورة بواسطة الدوس DOS فقط حتى لا يشك بالملف الضحية او المستهدف تابع معي الطريقة. كيف يتم ذلك؟

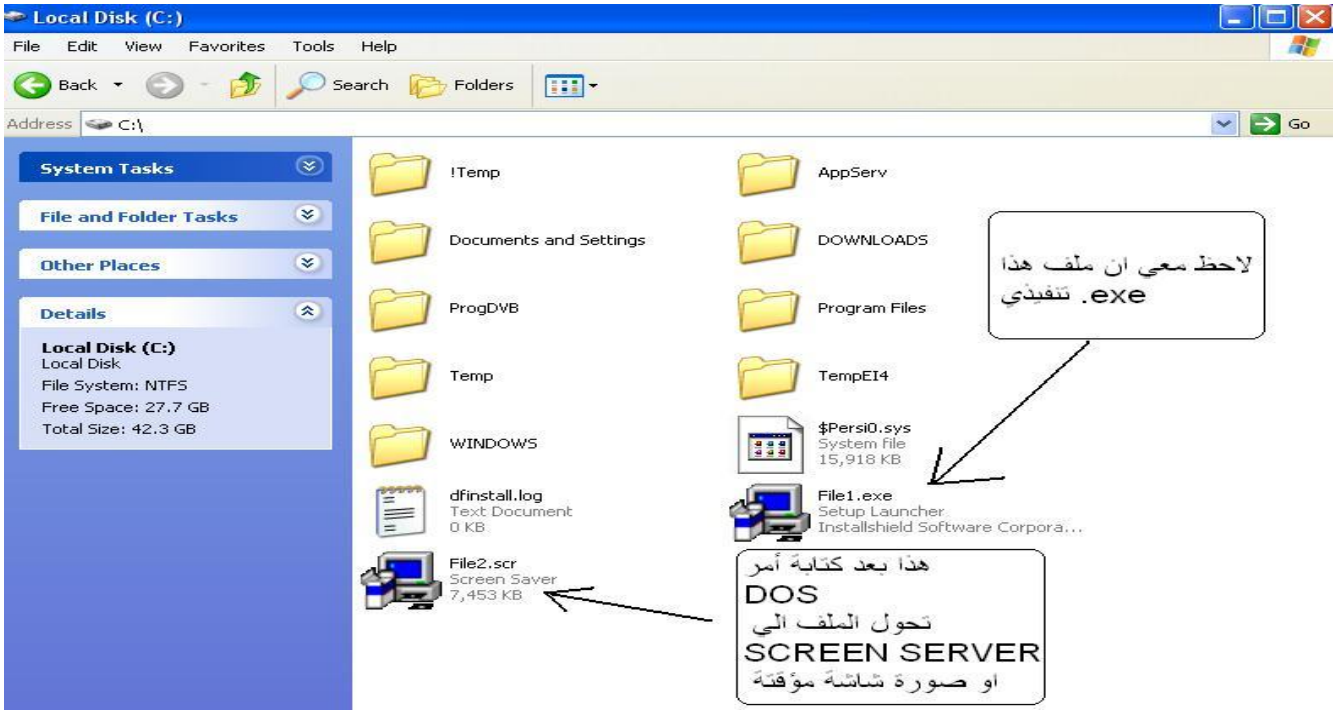
من Command او الشيل
Start >>> Run >>> cmd




هذه الأوامر هي لتحويل ملف تنفيذي .exe على القرص C:/> الي صورة شاشة مؤقتة .scr صورة متحركة ومن الدوس بدون أستخدام اي برامج.

لاحظوا ماذا حدث بعد الأمر السابق في COMMAND , قمنا بتحويل الملف التنفيذي File1.exe الي ملف شاشة مؤقتة File2.scr.




هذا كان مجرد مثال لتوصيل فكرة معينة , وهو أمكانيه المخترق بتحويل صيغ أمتداد الملفات التنفيذية الي ملف صورة لينخدع فيه الضحية لا أكثر ولا أقل.


يتبع هذه العملية تحويل ايقونة الملف الي ملف صورة لكي يكون الملف التجسسي او التنفيذي للمستخدم المستهدف كصورة وبأمتداد scr او jpg بواسطة برامج تغيير الأيقونات , وللأسف ينخدع المستخدم المستهدف من قبل المخترق بكل سهولة , لأن المخترق قام بخداع المستخدم او المستهدف ببعض الأمور السهلة بالنسبة له والبسيطة وبالصعبة والتي يغفل عنها الكثيرين من المستخدمين , وهي تغيير شكل السيرفر او ملف التجسس بحيث لا يشك به الضحية او المستخدم وتشفيره من برامج الحماية بواسطة برامج التشفير الموجودة بالمنتديات العربية , ثم تحويل الملف التجسسي الي صورة حتى لا يشك به الضحية , وتغيير شكل أيقونة الملف التجسسي الي شكل صورة , مما قد لا يشك بالملف التجسسي الضحية او المستخدم ابداً , ان هذا الملف التجسسي او بمعنى أخر فايروس منتشرة بكثرة في المواقع المشبوهه , او موقع معين قمت بتحميل ملف من خلاله سواء كان صورة او ملف تنفيذي او اي كان يكون غالباً ملف "داونلودر" وهذا معناه ان المخترق تم رفع ملف تجسسي صغير الحجم حتى لا يشك الضحية ببطء في التصفح اثناء تحميل الملف في الجهاز , ويتم من خلال هذا الملف الصغير الحجم تثبيت نفسه بالجهاز ثم يقوم هذا الملف الصغير الحجم بأستدعاء الملف الكبير الحجم وكل هذا تم من صفحة انترنت , ومن ملف بمساحته صغيرة حتى لا يشعر الضحية ببطء في التصفح , فهو بمثابة ربط ملفين تجسس ببعض , وعن طريقه يتم زرع ملف التجسس الأصلي بملف system32 في القرص C وهو أهم قرص بالجهاز , فهو مدير النظام ككل ويتم من خلاله تشغيل اي برنامج تنفيذي في كل بدأ تشغيل للنظام , ومن خلاله يتم انتشار الفايروسات وملفات التجسس للأجهزة وعبر الرسائل الفورية والبريد الألكتروني لأنه ينتشر في جميع البرامج المثبته على الجهاز , ان شاء الله في الدروس المقبلة سوف اشرح لكم كيف تحمي نفسك من هذه الفيروسات والأختراقات وملفات التجسس بأذن الله.

الدرس الثاني

# 2- مقدمة في البرامج التجسسية Spyware وماذا يمكن ان تعمل وكيفيه عملها؟

دائما يخلط البعض في المصطلحات فيسمي التروجان والدودة فيروس وهذا غير صحيح فالكلمات تروجان وفيروس ودودة هي مصطلحات تطلق على أنواع مختلفة من البرمجيات المؤذية للحاسب,, وسوف أقوم بإيضاح الفروقات بين هذه المسميات .فكل نوع له طريقة عمل خاصة به ولذالك أطلقت التسميات المختلفة.

## ما هو الفيروس؟

الفيروس هو مجموعة من التعليمات البرمجية التي ترفق نفسها ببرنامج أو ملف لتتمكن من الانتشار من كمبيوتر إلى آخر. وتؤدي إلى الإصابة أثناء تنقلها. بإمكان الفيروسات إعطاب البرامج، والأجهزة، والملفات الخاصة بك. فيروس (اسم) تعليمات برمجية تمت كتابتها بهدف واضح وهو نسخ نفسها. يرفق الفيروس نفسه ببرنامج مضيف ثم يحاول الانتشار من كمبيوتر إلى آخر. وقد يؤدي إلى إعطاب الأجهزة، أو البرامج، أو المعلومات. كما تتفاوت الفيروسات التي تصيب البشر في خطورتها من مرض الإيبولا إلى الإنفلونزا البسيطة التي تستمر لمدة 24 ساعة فقط، فإن فيروسات الكمبيوتر تتفاوت من تلك التي تسبب إزعاجاً بسيطاً إلى تلك التي تسبب خراباً شاملاً. الأمر الجيد هو أن الفيروس الحقيقي لا ينتشر بدون تدخل بشري. يجب على أحد أن يتشارك في ملف أو يقوم بإرسال بريد إلكتروني كي يتحرك الفيروس.

## الدودة:

الدودة قريبة من الفيروس في التصميم ولكن تعتبر جزءاً فرعياً من الفيروس. الإختلاف الذي يفرق الفيروس عن الدودة بأن الدودة تنتشر بدون التدخل البشري حيث تنتقل من جهاز إلى آخر بدون عمل أي إجراء.
الجزء الخبيث في الدودة هو قدرتها على نسخ نفسها في جهازك بعدة أشكال وبذلك يتم إرسالها بدلا من مرة واحدة سترسل آلافاً من النسخ للأجهزة الأخرى. مما يحدث مشاكل كبيرة. وتستغل الدودة طرق الأتصال التي تقوم بها لإتمام هذه العملية لذلك قد ترى في بعض الأحيان ظهور نافذة طلب الأتصال اتوماتيكياً بدون طلبك أنت فانتبه فقد يكون لديك دودة.
وآثار الدودة عادة هي زيادة في استخدام مصادر الجهاز فيحصل في الجهاز تعليق بسبب قلة الرام المتوفر وأيضا تسبب الدودة في توقف عمل الخوادم فعلى سبيل المثال يمكنك تخيل التالي. لو كان عندك دودة فستقوم الدودة بنسخ نفسها ثم إرسال لكل شخص من هم لديك في القائمة البريدية نسخة وإذا فتح أحدهم هذه الرسالة ستنتقل إلى كل من لديه هو في قائمته البريدية وهذا يولد انتشاراً واسعاً جداً.
وأفضل مثال على الدودة هي ما حصل العام الماضي دودة البلاستر التي كانت تدخل لجهازك لتسمح ببعض الأشخاص بالتحكم بجهازك عن بُعد .

## التروجان:

التروجان يختلف كلياً عن الفيروس والدودة . التروجان صمم لكي يكون مزعجاً أكثر من كونه مؤذياً مثل الفيروسات.
عندما تقوم بزيارة أحد المواقع المشبوهة أحيانا يطلب منك تحميل برنامج معين. الزائر قد ينخدع في ذلك فيعتقد انه برنامج وهو في الحقيقة تروجان .
يقوم التروجان في بعض الأحيان بمسح بعض الأيقونات على سطح المكتب. مسح بعض ملفات النظام. مسح بعض بياناتك المهمة. تغير الصفحة الرئيسية للإنترنت إكسبلورر. عدم قدرتك على تصفح الانترنت. وأيضا عرف عن التروجانات أنها تقوم بوضع باكدور في جهازك من ما يسمح بنقل بياناتك الخاصة إلى الطرف الآخر بدون علمك.
وهذا هو الخطير في الأمر.

علما بأن التروجان لا يتكاثر مثل الدودة ولا يلحق نفسه ببرنامج مثل الفيروس ولا ينتشر أيضا سواء عن تدخل بشري أو لا.

الفيروسات المنتشرة عبر الأنترنت , لكن أغلبها ما يقع تحت هذه النقاط الستة:

1- فيروسات بدء التشغيل اوBoot Sector Virus
هذا النوع من الفيروسات يصيب قطاع الأقلاع في الجهاز , و هو المكان المخصص الذي يتجه إليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول الى النظام ويمنعه من إقلاع الجهاز.

2- فيروس الملفات اوFile Virus
يصيب البرامج عادة , و ينتشر بين الملفات الأخرى و البرامج الأخرى عند تشغيله.

3- فيروس الماكرو اوMacro Virus
هذه الفيروسات تصيب برامج الميكروسوفت أوفيس مثل الوورد و الأكسل, و تعتبر ذات إنتشار واسع جداً تقدر ب75% من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصاً الوورد , قد تجد بعض التصرفات الغير منطقية في بعض الأحيان مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد , و ايضاً تجد بعض الكلمات قد تغير مكانها و اضيفت كلمات جديدة لا علاقة لها بالموضوع .

هي اساساً ليست ضارة, لكنها مزعجة نوعاً ما و قد تكون مدمرة احياناً!

4- الفيروس المتعدد الأجزاء اوMultipartite Virus
و هو الذي يقوم بإصابة الملفات مع قطاع الأقلاع في نفس الوقت و يكون مدمراً في كثير من الأحيان اذا لم تتم الوقاية منه.

5- الفيروس المتطور اوPolymorphic Virus
هي فيروسات متطورة نوعاً ما حيث انها تغير الشفرة كلما انتقلت من جهاز الى آخر. نظرياً, يصعب على مضادات الفيروسات التخلص منها لكن عملياً و مع تطور المضادات فالخطر أصبح غير مخيف.

6- الفيروس المختفي اوStealth Virus
تخفي نفسها بأن تجعل الملف المصاب سليماً و تخدع مضادات الفيروسات بأن الملف سليم و ليس مصاباً بفيروس. مع تطورمضادات الفيروسات أصبح من السهل كشف هذا النوع.

**هناك ايضاً مصطلح يطلق على ملفات التجسس Trojan هو ملف تنفيذي تجسسي من الدرجة الأولى حيث يقوم بالسيطرة الكاملة على الجهاز المستهدف مثل الفيروسات التي تقوم بتخريب الأجهزة والأنتشار على حسب نوعية الفايروس ولكن التروجان هو ملف تنفيذي تجسسي غير قابل للأنتشار بين الأجهزة عكس الفيروسات ولكن يقوم بواسطته فتح منفذ بالجهاز PORT يستطيع من خلاله المخترق الدخول على الجهاز المستهدف والسيطرة الكاملة عليه والتحكم في كل شيء فيه من ملفات وكلمات سرية خاصة , هذه الملفات التجسسية قد تكون بشكل صورة JPG. او ملف تنفيذي exe. او دانلودر downloader من صفحة انترنت في موقع مشبوه مثلاً , الداونلودر هو ملف تنفيذي صغير الحجم يتم رفعه على احدى صفحات الويب الأنترنت يتم من خلاله تحميل الملف التجسسي الدونلودر لجهازك ويقوم هذا الملف الصغير الحجم غالباً بزرع نفسه في جهازك ثم يقوم بتحميل الملف التنفيذي الأصلي كبير الحجم.**
**وحتى لا يشعر المستهدف بوجود شيء غير طبيعي اثناء التصفح.**

# أولاً : مقدمة عن البرامج التجسسية Spyware

يعتبر التجسس نوع من أنواع برامج أجهزة الحاسوب التي تربطهم بواسطة طرق معينة بنظامك التشغيل. تستطيع برامج أجهزة الحاسوب امتصاص المعلومات من قوة معالجة جهازك الحاسوب وقد صمموا لتتبع خطواتك على الانترنت.

بالنسبة للتقييمات الحديثة بينت أن أكثر من ثلثي أجهزة الحاسوب الشخصية تتأثر ببعض أنواع برامج التجسس ولكن قبل ابعاد جهازك الحاسوب عن الشاشة الرئيسية والقائها إلى جزيرة صحراوية عليك ان تقرئها.

في هذه المقالة سوف نوضح كيف أن التجسس يظهر في جهازك الحاسوب وما هي الطريقة للتخص منه.

بعض الناس يخلط بين برامج التجسس وفايروسات أجهزة الحاسوب. فايروسات أجهزة الحاسوب هي عبارة عن جزء من شيفرة أو هي رموز صممت لتكرار نفسها بأكبر عدد ممكن، وهي تنتشر من جهاز حاسوب مرتبط مع جهاز اخر وعادة ما يتم التحميل بينهم والذي من الممكن أن يدمر ملفاتك الشخصية أو حتى نظامك التشغيل.

برامج التجسس من جهة أخرى وبشكل عام غير مصممة لتدمير جهازك الحاسوب فهي تعرف بشكل أشمل كأي برنامج يدخل على جهازك بدون اذن ويختفي في الخلفية بينما يحدث تغييرات غير مرغوب بها للمستخدم. وتسبب برامج التجسس تدمير الملفات أكثر من انتاجها والتي تحقق هدفك الدعائي أو عمل محركات البحث مواقع رئيسية أو نتائج البحث .

في الوقت الحاضر من أكثر غايات التجسس فقط نظام تشغيل النوافذ، ومعظم شركات التجسس المشهورة تحتوي على: ( Bonzi Buddy, 180 Solutions, ،Gator DirectRevenue, Cydoor, CoolWebSearch, Xupiter, XXXDial and (Euniverse

إن "برنامج التجسس" هو مصطلح عام يستخدم لوصف البرامج التي تقوم بسلوكيات معينة، كعرض الإعلانات، أو جمع المعلومات الشخصية، أو تغيير تكوين الكمبيوتر، ويحصل ذلك عادةً من دون الحصول على موافقتك أولاً بالصورة الملائمة.

غالباً ما يتم إقران برامج التجسس بالبرامج التي تعرض الإعلانات (وتحمل اسم برامج الإعلانات المتسللة)، أو بالبرامج التي تتعقب المعلومات الشخصية أو الحساسة.

ولكن، لا يعني ذلك أن كافة البرامج التي توفر الإعلانات أو تتعقب نشاطاتك عبر إنترنت هي سيئة. فمثلاً، قد تقوم بالتسجيل للاشتراك بخدمة موسيقى مجانية، ولكن تقوم بـ "دفع" ثمن الخدمة عبر الموافقة على تلقي إعلانات هادفة. إذا فهمت الشروط ووافقت عليها، تكون قد قررت أن تلك هي عملية تبادل عادلة. قد توافق أيضاً على أن تتعقب الشركة نشاطاتك عبر إنترنت لتحديد الإعلانات التي ستعرضها عليك.

أما الأنواع الأخرى من برامج التجسس، فتُجري تغييرات مزعجة في الكمبيوتر قد تتسبب بإبطاء الجهاز أو بتعطيله.

فتستطيع هذه البرامج تغيير الصفحة الرئيسية أو صفحة البحث لمستعرض ويب، أو إضافة مكونات إضافية إلى المستعرض لا تحتاج إليها أو لا ترغب فيها. كذلك، تصعّب هذه البرامج عليك تغيير الإعدادات وإعادتها إلى ما كانت عليه في الأصل.

وفي كافة الحالات، الأهم هو ما إذا كنت قد فهمت (أنت أو مستخدم الكمبيوتر) أو لم تفهم ما سيقوم به البرنامج، ووافقت على تثبيته على الجهاز.

ثمة طرق عديدة تستطيع من خلالها برامج التجسس أو البرامج الأخرى غير المرغوب فيها الوصول إلى الكمبيوتر. وتكمن إحدى الحيل الشائعة في تثبيت البرنامج بشكل سري، خلال تثبيت برنامج آخر ترغب فيه، مثل برنامج مشاركة ملفات الموسيقى أو الفيديو.

كلما تقوم بعملية تثبيت على الكمبيوتر، احرص على قراءة كافة المعلومات التي تم الإفصاح عنها بعناية، بما في ذلك اتفاقية الترخيص وبيان الخصوصية. وأحياناً، يتم توثيق تضمين برنامج غير مرغوب فيه في تثبيت برنامج معين، ولكن قد يظهر في نهاية اتفاقية الترخيص أو بيان الخصوصية.

# ماذا يمكن أن تفعل برامج التجسس(Spyware) وكيفية عملها؟

بامكان برامج التجسس القيام بأمور عديدة عندما تدخل إلى جهازك أو أدق أن تتسلل إلى جهازك الخاص. فبرنامج التجسس يعمل على انه برنامج مخفي يتم تشغيله عند تشغيل الجهاز يجعل الجهاز بطيء نوعا ما ويتحكم في محرك شبكة الانترنت بحيث يجعل تحميل الصفحات بطيء ويتحكم في إطفاء وتشغيل الصفحات أو في عملية البحث على شبكة الانترنت ونتيجة البحث.

التسلل والسرقة

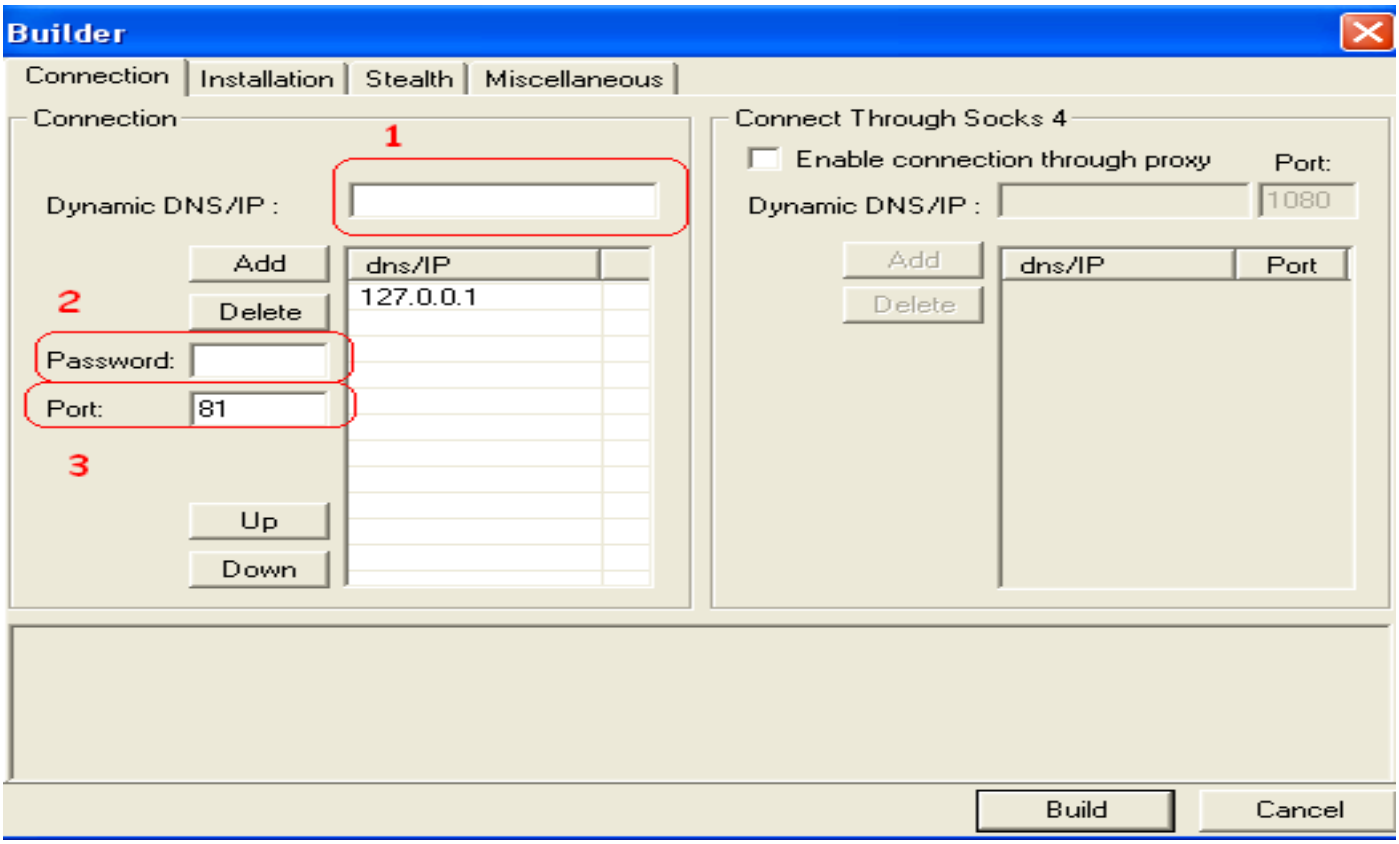
تتسلل البرامج التجسسية إلى جهاز الحاسوب وتعمل مثل الجاسوس الحقيقي بحيث تتجسس على المستخدم وتعرف أاسم المستخدم والرقم السري الخاص به وهي لها أدوات وطرق شبيهه في الفيروس أو لصوص الحاسوب.

وهي تظهر للمستخدم لكي تخدعه إما على شكل إعلان ما في طريقه فضولية أو مفاجئته حيث تجعل المستخدم متحمس للاشتراك دون التفكير أو أاخذ الحيطة أو عند تحميل صفحة ما أو فتح بريده الخاص تظهر على انها الصفحة المطلوبة وتتجسس عليه وتسرق عنوانه وتتحكم في عمله ومن هنا تتمكن من انتحال شخصيته وتعلم خصوصياته.

وان كان المستخدم من محبي التسوق وأاشتراك في مواقع البيع والشراء مثل
امازون( Amazon)و اي باي( eBay) تسرق رقم بطاقة الإتمان الخاصة به أي انها تسلب المستخدم كامل حقوقه وخصوصياته، وتتحكم في الجهاز من حيث السرعة والدقة والسعة والملفات.

## كيـــف تـعـــمـــل؟

البرامج التجسسية كثيرة ومتعددة يوجد منها المشفر ضد برامج الحماية والأخر غير مشفر يحتاج الي تشفيره لينتج سيرفر او تروجان مشفر ضد برامج الحماية , وهناك برامج تشفير مخصصة لتشفير السيرفرات او الملفات التجسسية , يتم انشاء الملف التجسسي بواسطة برامج التجسس يكون مساحته في الغالب لا تتعدى 70KB يتم ظبط اعدادته بواسطة برنامج التجسس من خلال ظبط IP و PORT وأسم الملف التجسسي بعد تشغيله وتفعيل الكي لوجر "قاريء الكيبورد" حتى يتمكن البرنامج من قراءة اي زر تضغط به على لوحة المفاتيح , تتعدد البرامج وتعدد المميزات في هذه البرامج التجسسية , هذا مثال على برنامج تجسسي وواجهته وإعدادته:

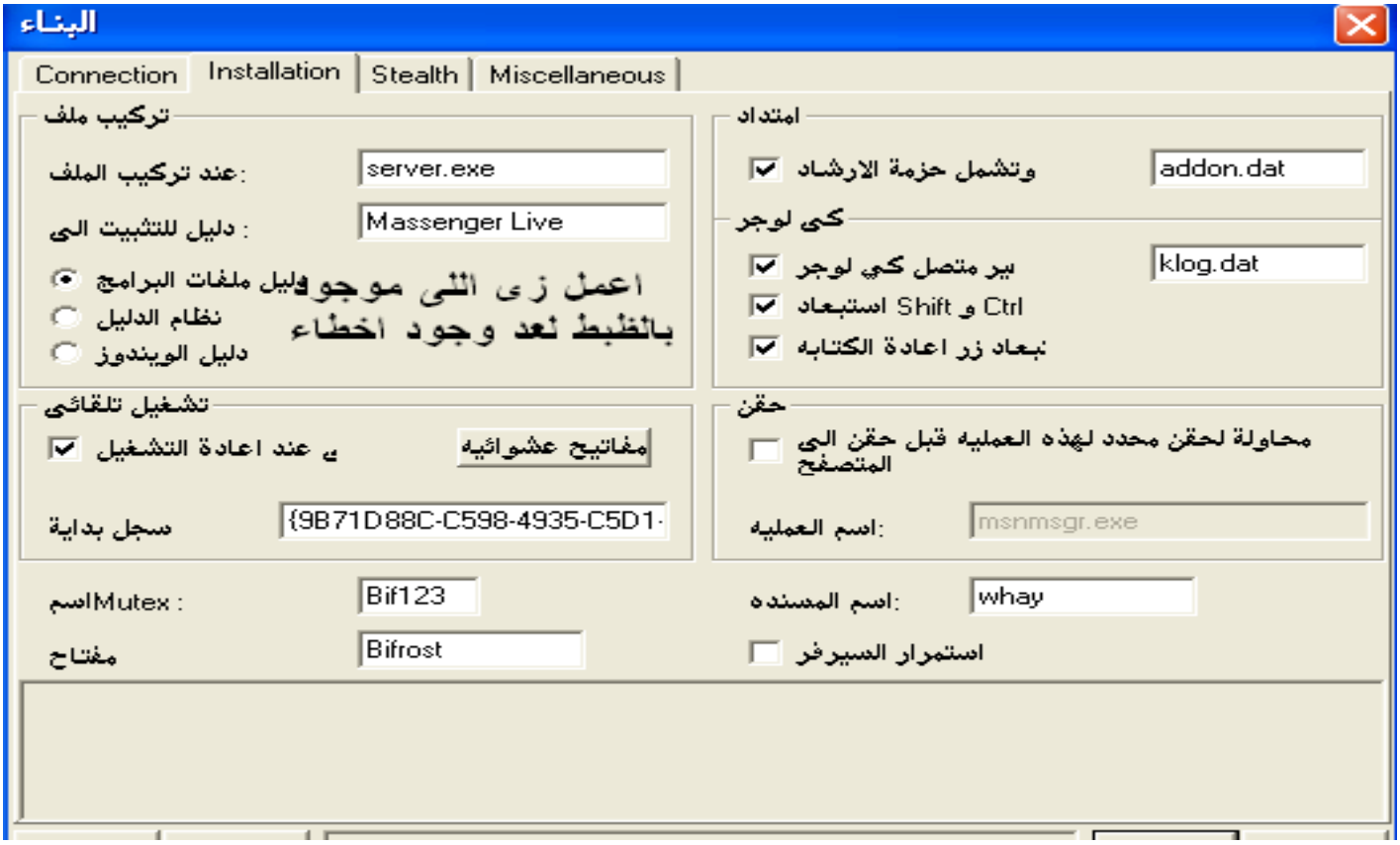



1 -هذه الخانة يتم وضع IP الخاص بالمخترق حتة يتم من خلاله فتح PORT قام المخترق بفتحه في جهازه وجهاز المستهدف ليتم الأتصال بهذا PORT من خلال هذا IP .

2 - وضع رقم سري خاص للمخترق للأتصال بالضحية او الهدف وحتى لا يستطيع اي أخر سواه بالدخول على الضحية الا من خلال وضع الرقم السري.

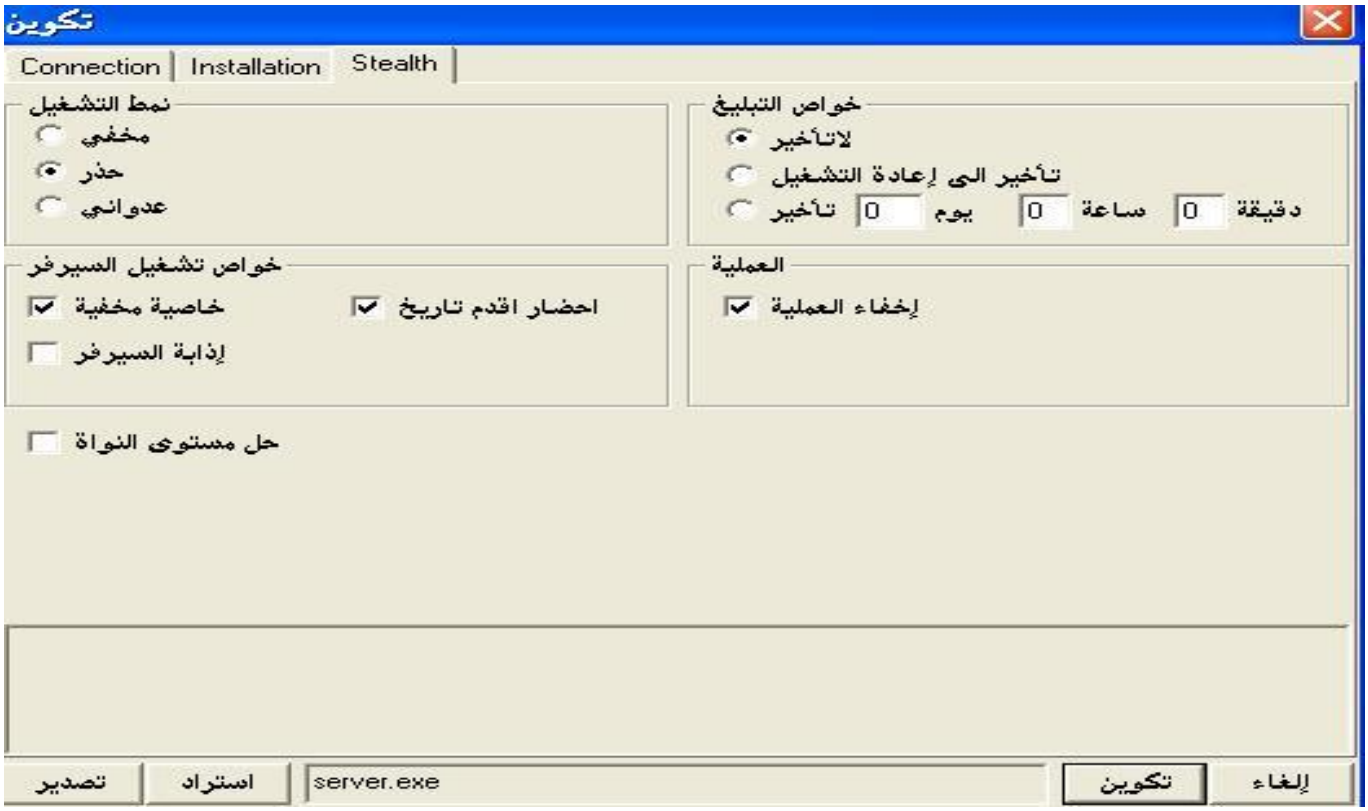
3 - البورت PORT الذي سوف يتم فتحه بين المخترق والضحية , ويجب ان يكون هذا الرقم مفتوح مبدئياً عند المخترق قبل الضحية ليتم أتصال المخترق بالضحية حيث يتم تشغيل السيرفر المنتج من برنامج التجسس.

وهذه قائمة Installation




يتم من خلالها ظبط أعدادت السيرفر المنتج من قبل البرنامج من حيث الأسم وتفعيل الكي لوجر وتشغيل السيرفر او الفايروس عند كل بدأ تشغيل للجهاز.

وهذه قائمة أخرى



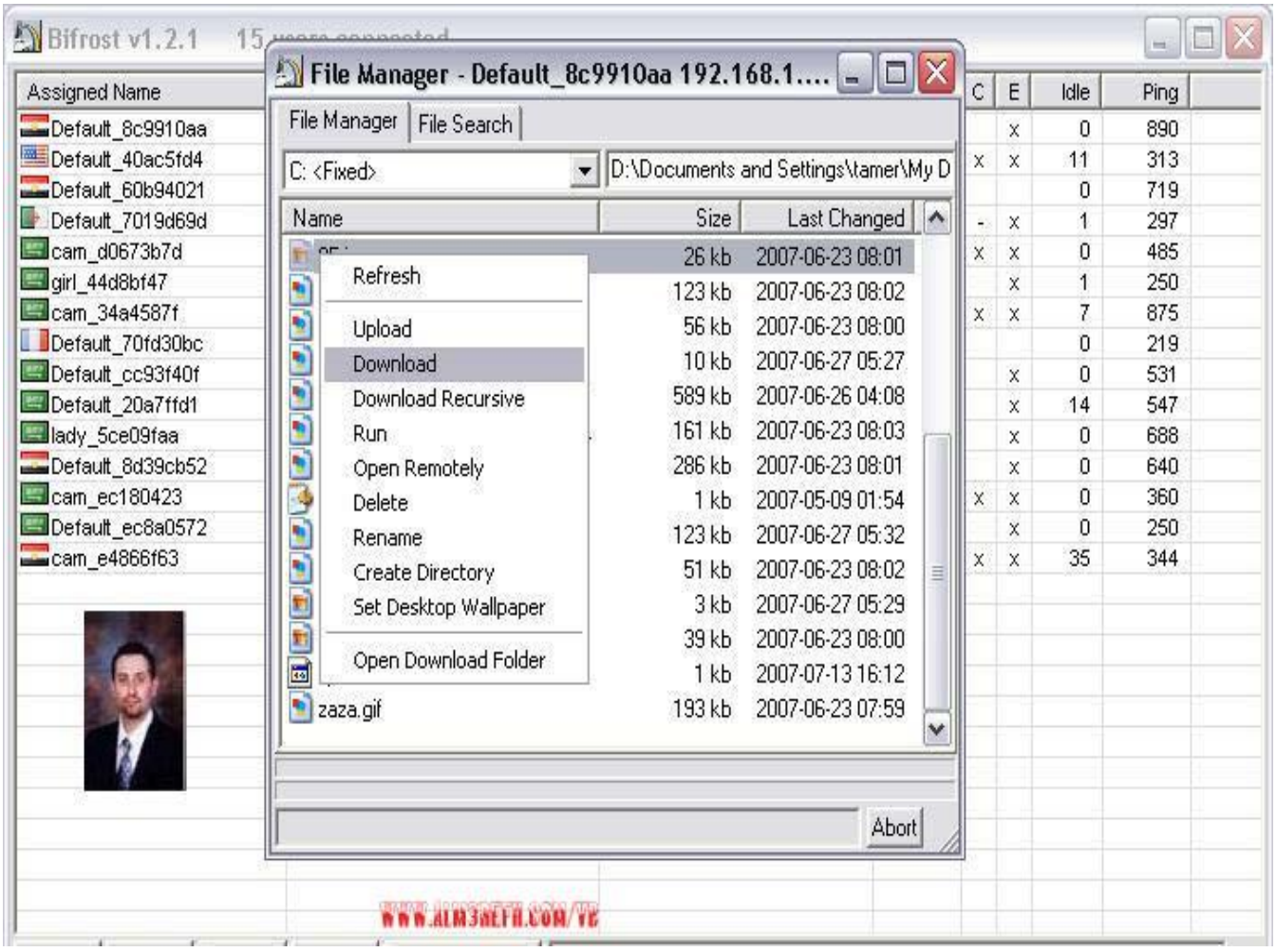
برامج التجسس خطيرة وسهلة للمبتدئين من حيث إنشاء الملف التنفيذي التجسسي.


بعد تنفيذ هذه الأوامر يتم انشاء الملف التنفيذي بهذا الشكل ليتم ارساله بعد ذلك للضحية بعد تشفيره وتغيير ايقونته عن طريق التبليغ بواسطة رقم IP.

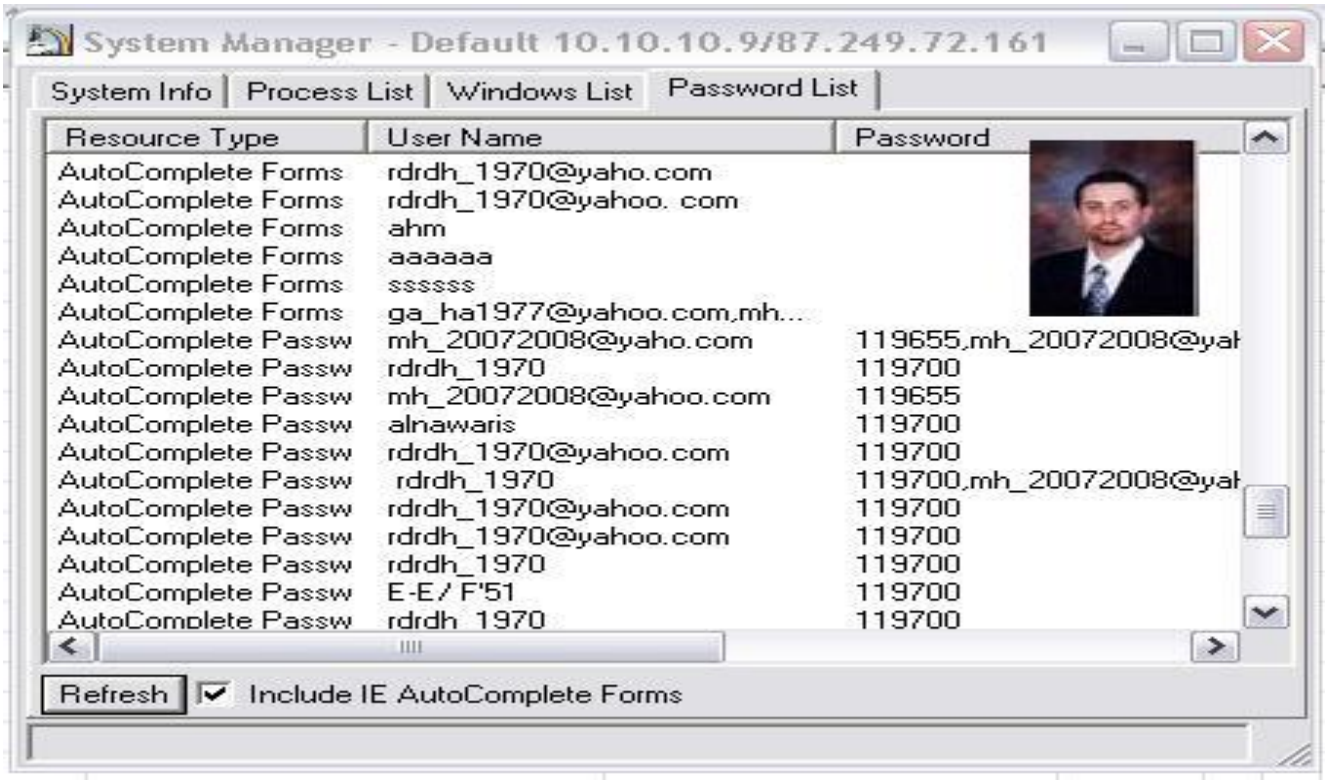
لاحظ إمتداد الملف exe. لهذا ركبه دائماً ان هذه الملفات خطيرة جداً جداً , يجب أن تكون حذر مع التعامل مع مثل هذه الملفات التفيذية وسأشرح لكم لاحقاً الأمور التي تدور في رأس المخترق لكي يتم اختراقك.

## من خلال هذا الملف التنفيذي البسيط يستطيع المخترق ان يقوم:

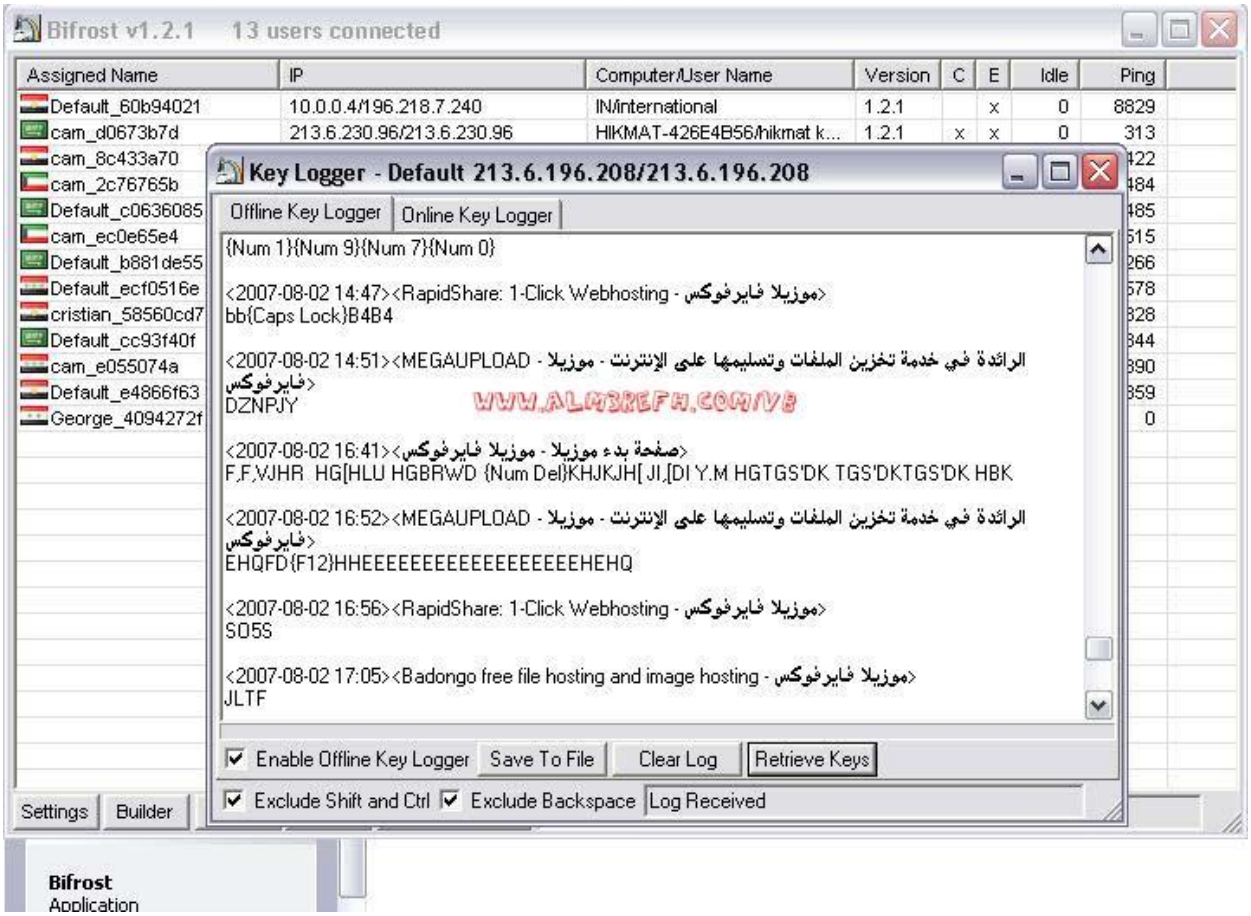
بتحميل صورك وملفاتك الخاصة من داخل جهازك الخاص:



كشف جميع الباسوردات وكلمات السر الخاصة بك في الجهاز:




قراءة لوحة المفاتيح "الكيبورد" الخاصة بك وبكل حرف تقوم بكتابته:

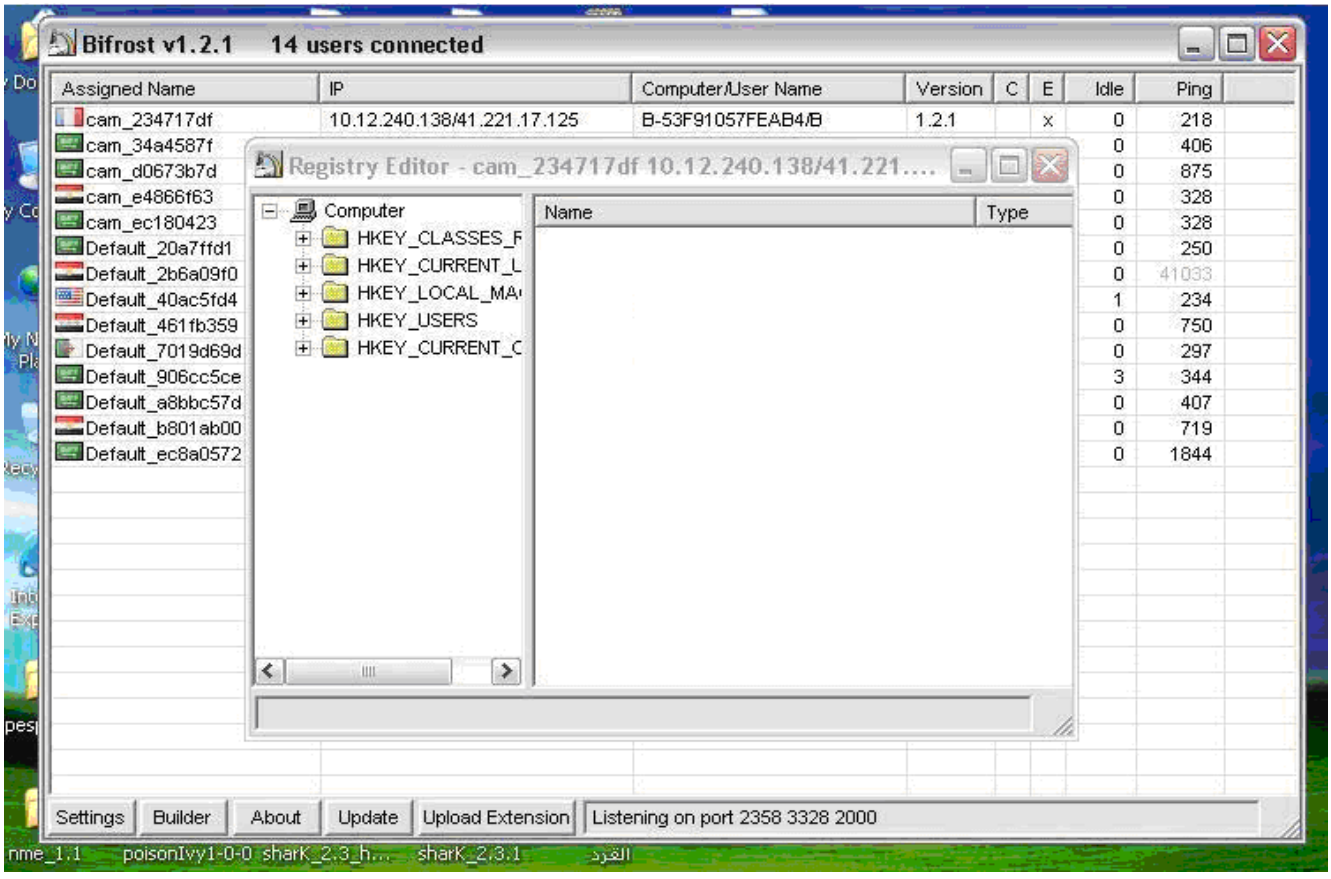


يستطيع كشف سطح المكتب الخاص بك ويرى كل ما تفعل من خطوات:


يستطيع ان يراك في الكاميرا الخاصة بك:

يستطيع تنفيذ أوامر Dos


يستطيع دخول ملفات الريجيستري Registry Editor




وهناك برامج تجسسية كثيرة ولكل برنامج إعدادته الخاصة وطريقة عمله المختلفة عن الأخر , ولكن كلها تعتمد على خاصية واحدة وهي التجسس او عملية Remote Computer التحكم بالأجهزة عن بُعد.

الدرس الثالث

# 3- إشارات تدل على وجود برامج تجسس: هل أنت مُراقب؟

في حال بدأ جهاز الكمبيوتر بالتصرف بغرابة أو أظهر أياً من الإشارات المذكورة أدناه، فمن المحتمل وجود برنامج تجسس أو برنامج آخر غير مرغوب فيه مثبت على الكمبيوتر.

**مهم جدا جدا جدا**

أرى إعلانات منبثقة باستمرار. تمطرك بعض البرامج غير المرغوب فيها بإعلانات منبثقة لا تتعلق بموقع ويب الذي تزوره. غالباً ما تكون هذه الإعلانات موجهة للراشدين أو مواقع ويب أخرى محل للإعتراض. إذا رأيت إعلانات منبثقة في إطارات حالما تشغل جهاز الكمبيوتر أو تستعرض ويب، فمن المحتمل وجود برنامج آخر غير مرغوب فيه مثبت على الكمبيوتر.

**مهم جدا جدا جدا**

تغيرت إعداداتي ويتعذر علي إرجاعها إلى حالتها السابقة. بإمكان بعض البرامج غير المرغوب فيها تغيير الصفحة الرئيسية وإعدادات صفحة البحث. من الممكن ألا تتعرّف على الصفحة الأولى التي تفتح عند تشغيل مستعرض إنترنت أو الصفحة التي تظهر لدى تحديد "بحث". حتى لو كنت تعرف كيفية ضبط هذه الإعدادات فهي تعود إلى الإعدادات السابقة في كل مرة تقوم فيها بإعادة تشغيل الكمبيوتر.

يحتوي مستعرض ويب على مكونات إضافية لا أتذكر أنني قمت بتنزيلها. أحياناً تقوم برامج التجسس والبرامج الأخرى غير المرغوب فيها بإضافة أشرطة أدوات لا تريدها أو لا تحتاج إليها إلى مستعرض ويب. حتى لو كنت تعرف كيفية إزالة أشرطة الأدوات هذه، فقد تعود لتظهر كلما أعدت تشغيل جهاز الكمبيوتر.

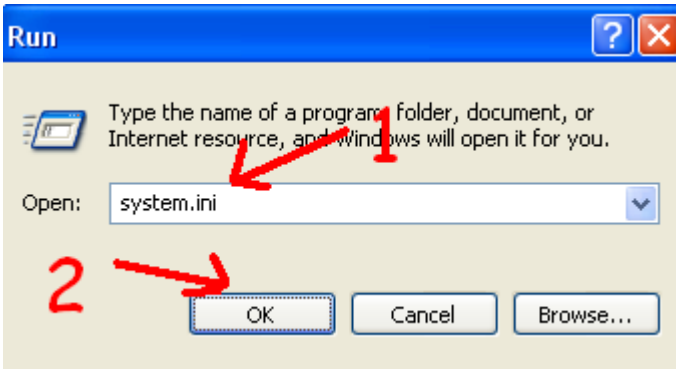
يعمل الكمبيوتر ببطء. ليست برامج التجسس والبرامج الأخرى غير المرغوب فيها مصممة بالضرورة بحيث تكون سريعة وفعّالة. فالموارد التي تستخدمها هذه البرامج لتعقب نشاطاتك ولإرسال الإعلانات تبطئ عمل الكمبيوتر والأخطاء في البرامج تتسبب في تعطله.

إذا لاحظت ارتفاعاً ملحوظاً في عدد مرات تعطل برنامج معين أو أنّ أداء الكمبيوتر في المهام الروتينية أبطأ من العادة، فمن المحتمل وجود برنامج تجسس أو برنامج آخر غير مرغوب فيه مثبت على جهازك.

# كيف تعرف أن جهـــــازك مراقب ؟

افتح قائمة (Start) ومنها اختر أمر (Run)،

أكتب التالي:
system.ini




ثم اضغط enter

سوف تظهر لك صفحة مفكرة وبها اسطر مثل التالية :

اذا ظهر رقم 850

EGA80WOA.FON= EGA80850.FON
EGA40WOA.FON= EGA40850.FON
CGA80WOA.FON= CGA80850.FON
CGA40WOA.FON= CGA40850.FON

فهذا يعني بان جهازك سليم 100/100 ولم يتم اختراقه ابدآ.

أما أذا ظهر لك WOA :

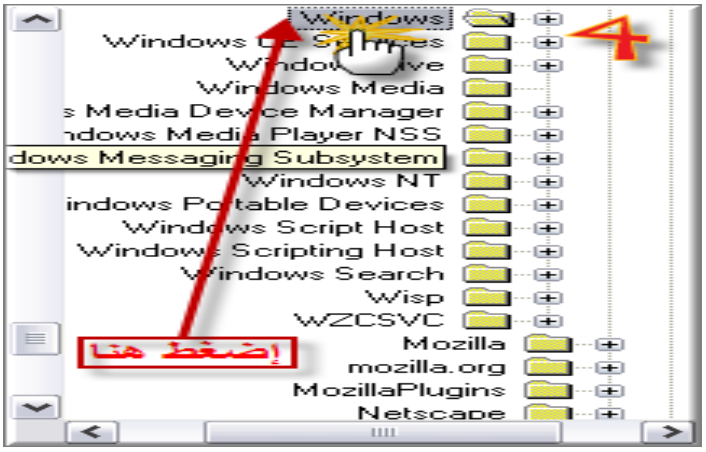
EGA80WOA.FON= EGA80WOA.FON
EGA40WOA.FON= EGA40WOA.FON
CGA80WOA.FON= CGA80WOA.FON
CGA40WOA.FON= CGA40WOA.FON

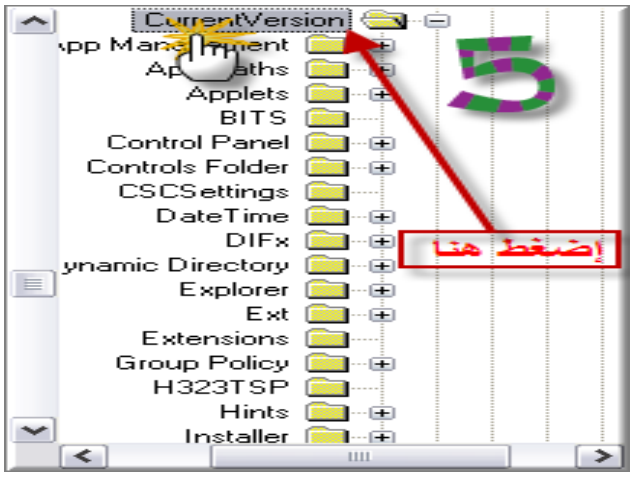
يعني جهازك فيه ملفات تجسس ويتم اختراقه بسهولة

# ملفات تسجيل النظام
# Registry








| الاسم | النوع | البيانات |
|---|---|---|
| (افتراضي) | REG_SZ | (لم يتم تعيين القيمة) |
| {C950420B-4182-... | REG_SZ | oem0.inf |
| CommonFilesDir | REG_SZ | C:\Program Files\Common Files |
| DevicePath | REG_EXPAND_SZ | %SystemRoot%\NLDRV\011;%SystemRoot%\NLDRV\0... |
| MediaPath | REG_SZ | C:\WINDOWS\Media |
| MediaPathUnexp... | REG_EXPAND_SZ | %SystemRoot%\Media |
| OEM_Reboot | REG_DWORD | 0x00000000 (0) |
| PF_AccessoriesN... | REG_SZ | البرامج الملحقة |
| ProductId | REG_SZ | 55435-640-8365391-23228 |
| ProgramFilesDir | REG_SZ | C:\Program Files |
| ProgramFilesPath | REG_EXPAND_SZ | %ProgramFiles% |
| SM_AccessoriesN... | REG_SZ | البرامج الملحقة |
| SM_ConfigurePro... | REG_SZ | تعيين افتراضيات البرامج والوصول إليها |
| SM_GamesName | REG_SZ | تسالي |
| WallPaperDir | REG_EXPAND_SZ | %SystemRoot%\Web\Wallpaper |

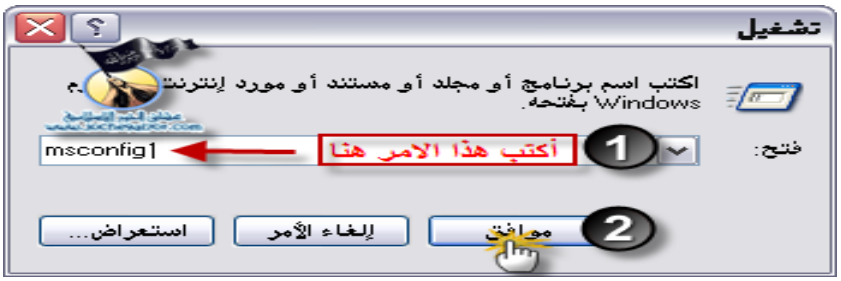
والآن من نافذة تسجيل -

انظر الي يمين النافذة بالشاشة المقسومة ستشاهد تحت Registry Editor أسماء Names عناوين الملفات Data قائمة النظام الملفات التي تعمل مع قائمة بدء التشغيل ويقابلها في قائمة.

لاحظ الملفات جيدا فإن وجدت ملف لا يقابلة Data -,او قد ظهر أمامة سهم صغير فهو ملف تجسس إذ ليس له عنوان معين بالويندوز عنوان بال.
تخلص منه بالضغط على الزر الأيمن للفارة ثم Delete -

# الأمر
# msconfig





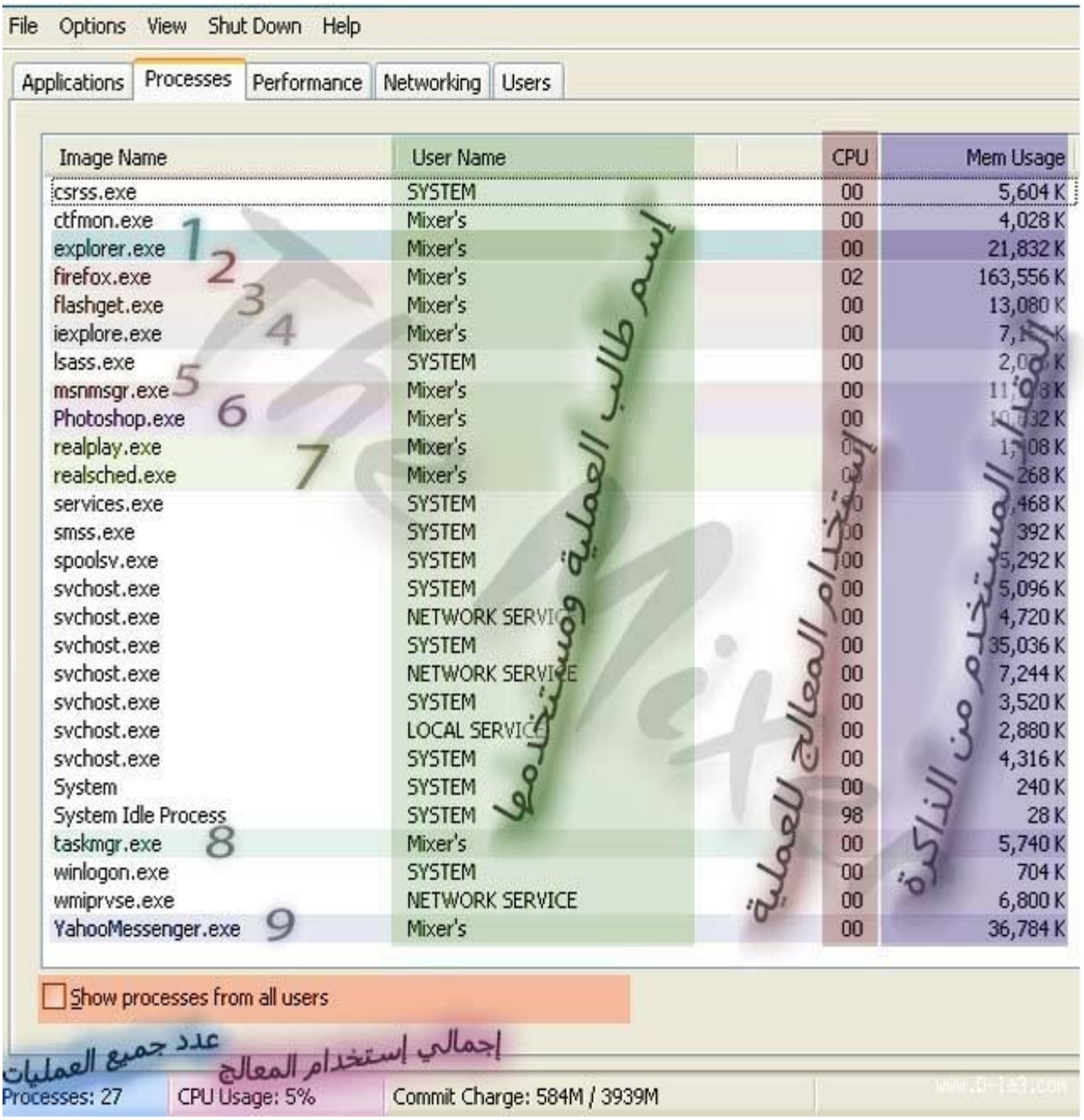


## ادارة المهام تحت المهجر Windows Task Manager

هي عملية مثلــها مثل أي عملية أخرى ولكن مهمتهــا الرئيسية إدارة عمليــات النظــام وغالبــاً ما تكون المرجع في إزاله الفيروسـات أو عمليــات التجسس أو في حالة توقف بعض البرامج عن العمــل وغير ذلــك.

ولكن جاءت الفيروسـات تعطلها لأهميـتها ووسائل الدخول إليها متعدده اولها نضغط Ctrl+Alt+Del ثم نذهب إلى إدارة العمليــات أو بضغــط الزر الأيمن على الشريط السريـع وأختيار ادارة المهام او العمليـات أو بالذهاب إلى أمر تشغيــل Start ثم Run وكتابة taskmgr

في حال تشغيــلهــا ستظهــر كالتــالي:



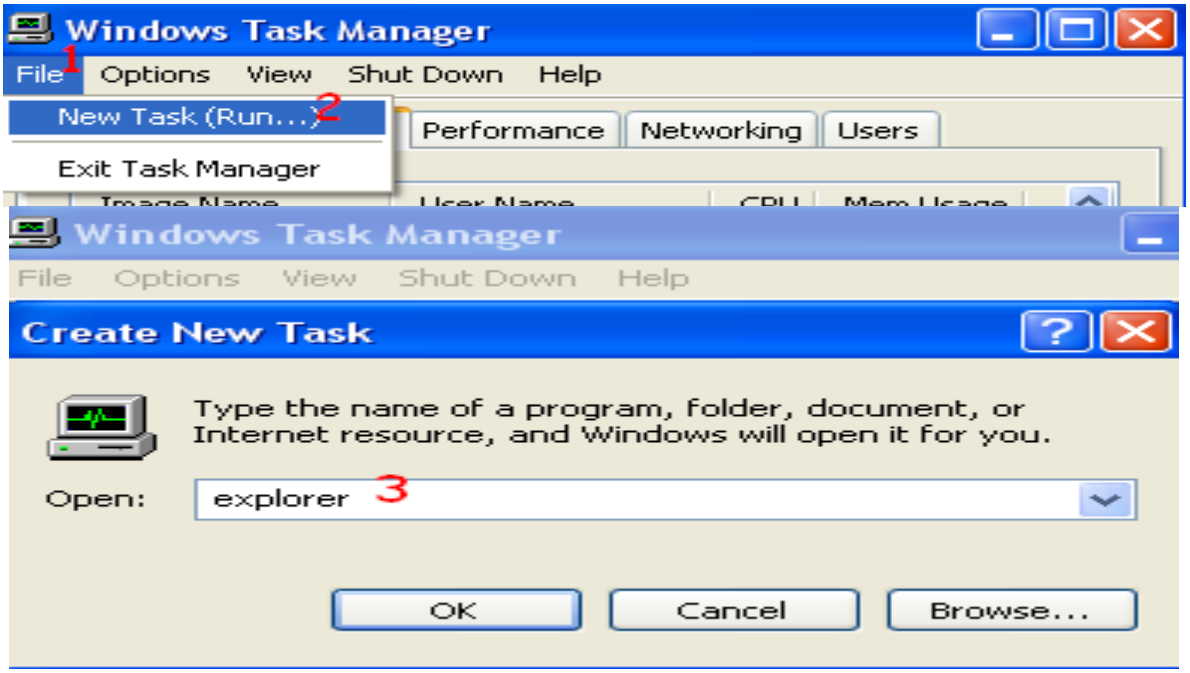
العمليــات الغير ملوونه هي تقريبــا من العمليــات الويندوز الأساسية والغالب لايمكن إنهائهــا...

امــا إذا إنهيــت واحدة منهـا بالغلط لا سمح الله إحتمـال يعرض لك رسالة مضمونهــا إن الجهاز سوف يغلق بعد دقيقه.

إحفظ كل أعمالك وسوف يظهر لك العداد قبل عملية الأغلاق , وحتى نوقف هذه العملية:

أذهب الي Start ثم Run وأكتب shutdown –a

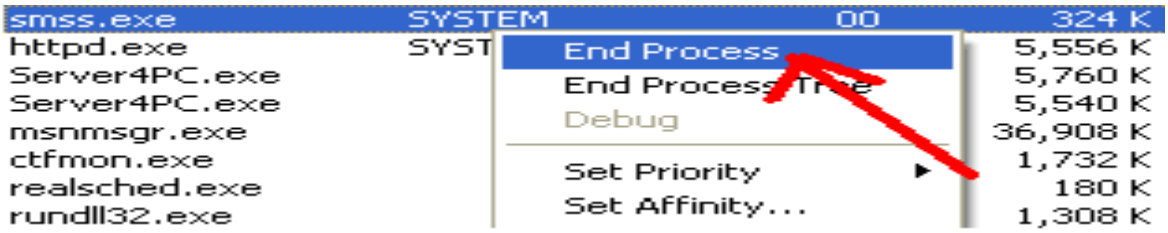
1 - متصفــح الوندوز الأساســي وهو العارض الافتراضي للنظام إذا أنهيــت هذي المهمــة .. سوف يختفي كل شيء في الجهاز امامك بما فيه الشريط السريع وسطح المكتب , ما عدا اداره العمليــات
في حال إنهائهــا إذهــب إلى ملــف File ومنه إلى مهــمة جديــدة وأكتب explorer .



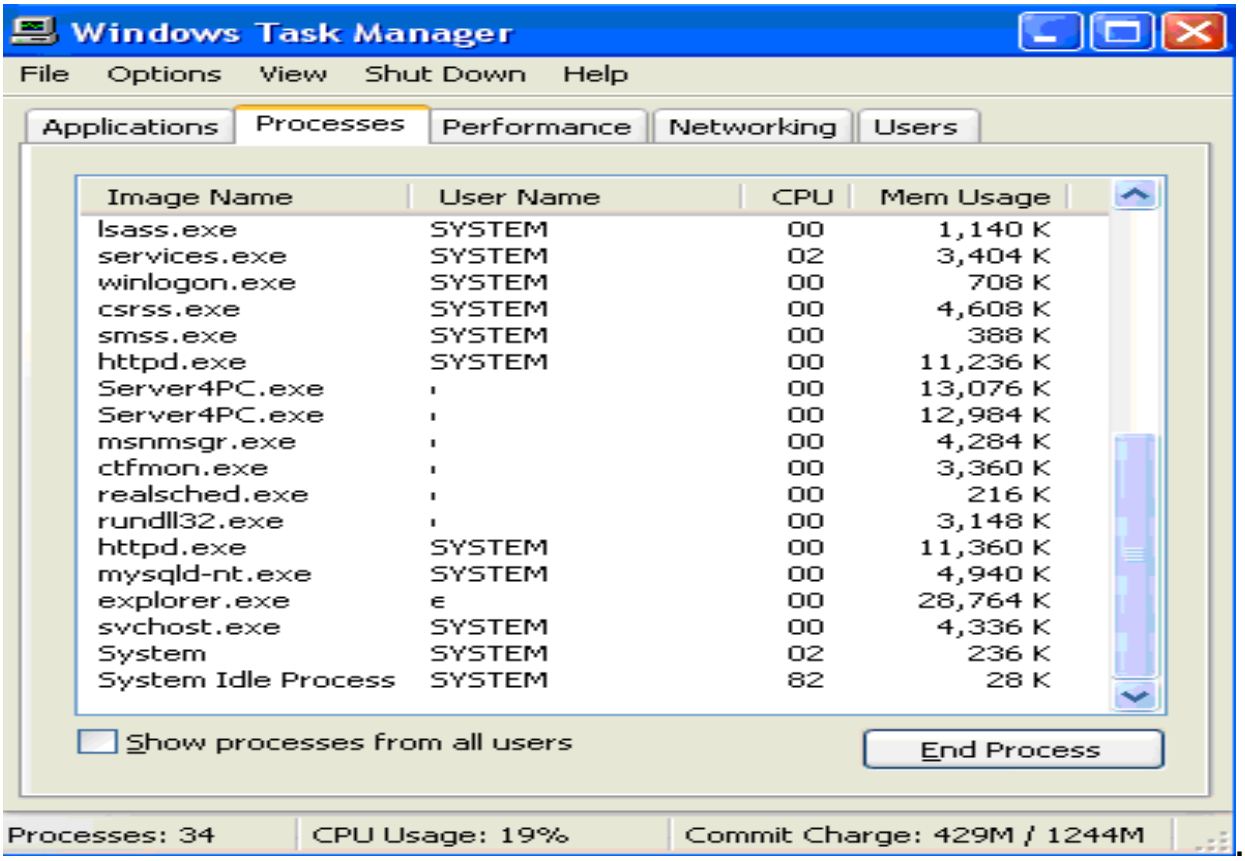

2 - العملية التابعه للمتصفح الشهيــر Mozilla Firefox ..
3 - العمليــة التابعــة لبرنامج التحميــل Flash Get ..
4 - وهي عملية مستعرض الأنترنت Internet Explorer في حال تشغيل أكثر من صفحه يكون تكرار نفس الاسم في نفس القائمة ..
5 - العملية التابعة للماســنجر الهوت ميل ..
6 - العملية التابعة لبرنامج الفوتوشوب ..
7 - RealPlayer هي لبرنامج الريال وكذلك realsched تابعه للبرنامج ولكن لخدمات البرنامج في الإنترنــت ..
8 - هي عملية إدارة العمليات لو إنهيتها راح تقفل إدارة العمليــات ..

ويوجد عمليـات تكون أسمائـها مبهمه شوي مثـل rundll32.exe فهذي إذا كانـت تعمل, معنى ذلك ان هناك عنصر من عناصر لوحه التحكـم يعمل أو عناصر الإداره ..

في حال تريد إنهاء برنامج لسبب ما , إضغط الزر الايمن على العملية التابعه له وإختر إنهاء العملية ..




ادارة المهام

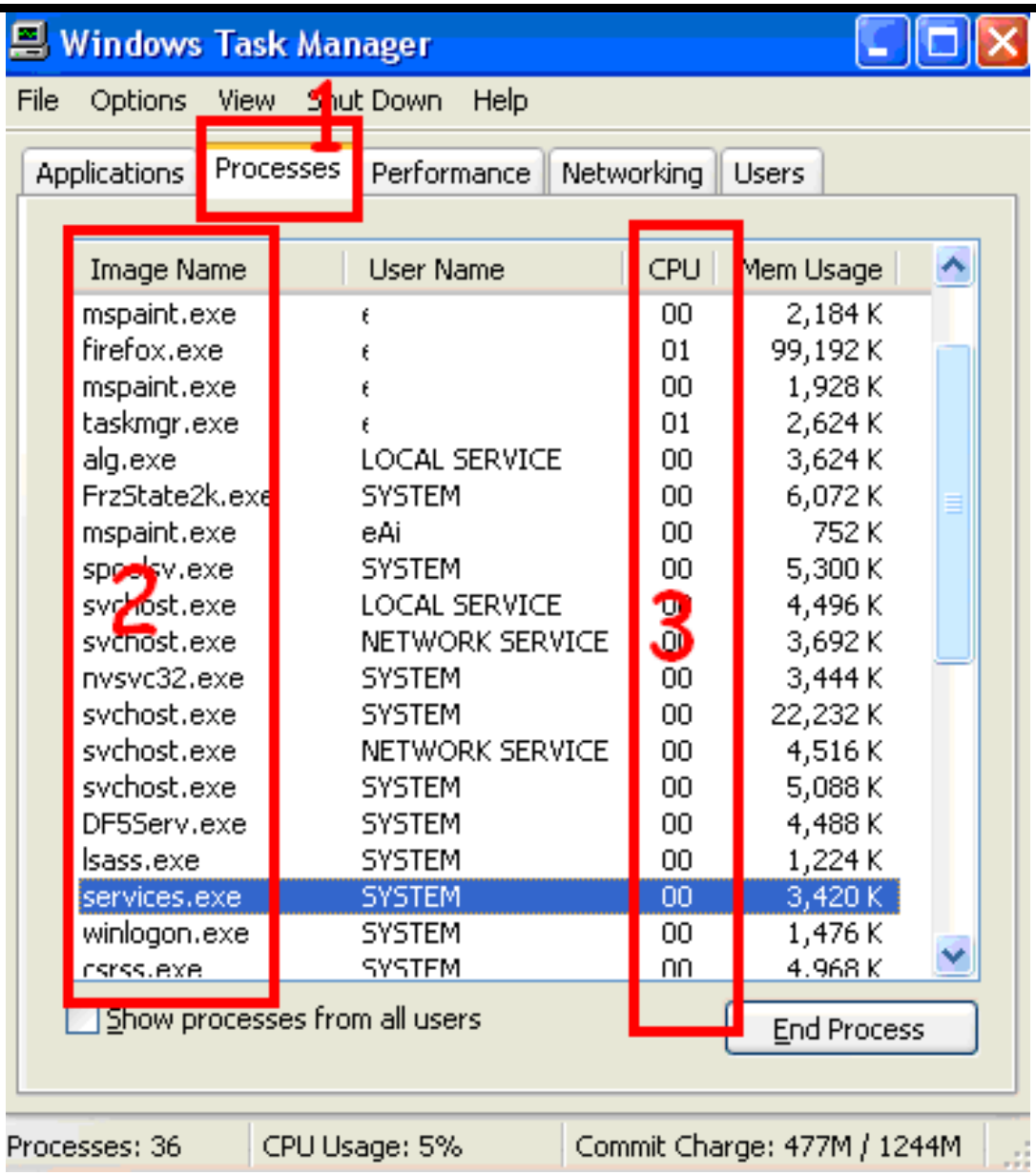



..

من لوحة المفاتيح أضغط Ctrl+Alt+Delete بيظهر لك Windows Task Manager

أختر منها Processes

كما بالصورة التالية:

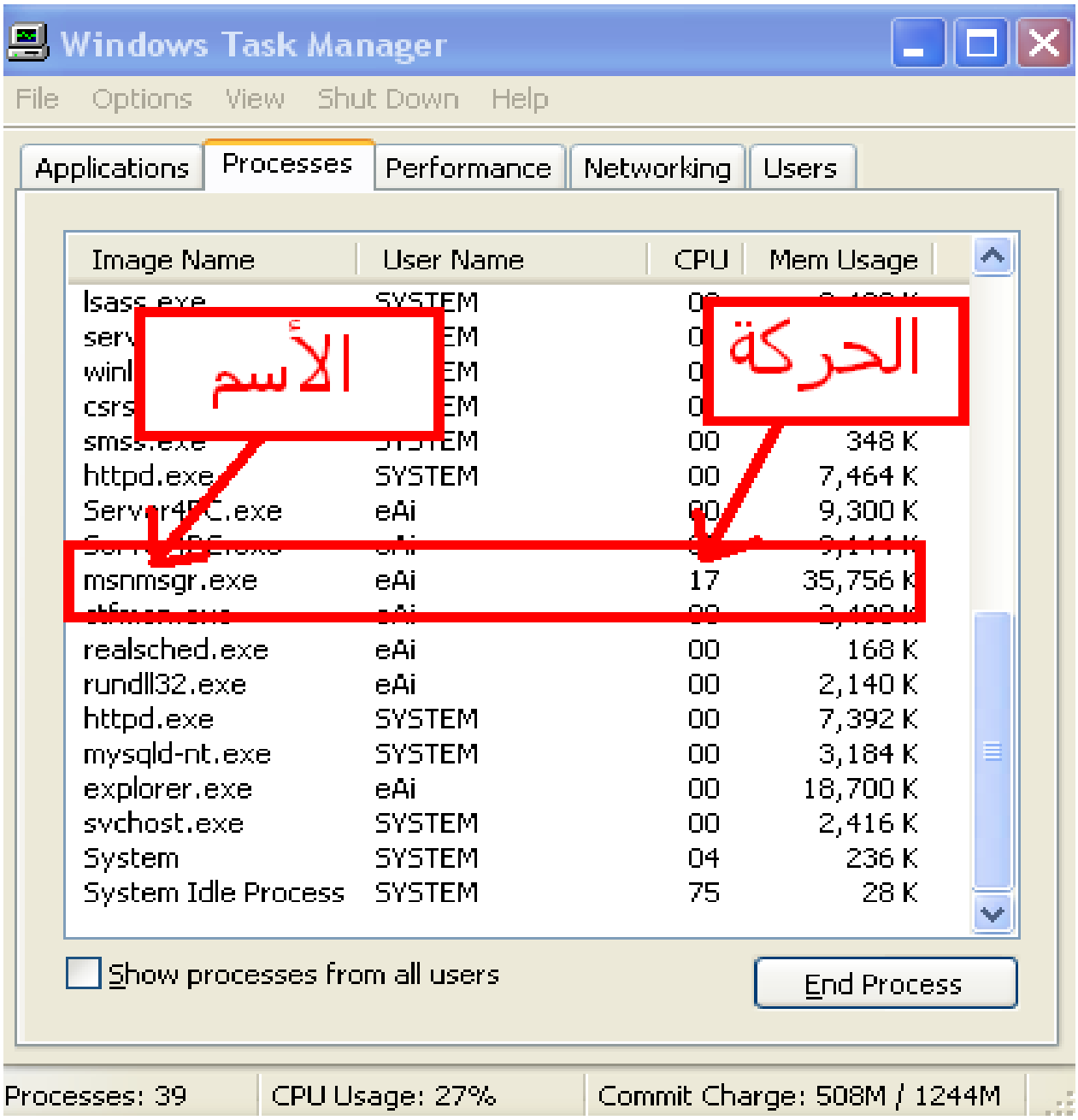



أهم شيء في هذه القائمة هي Image Name و CPU

لاحظ أن في قائمة Image Name كلها ملفات تنفيذية exe. وهي أما أن تكون برامج Programs مثبتة في جهاز او ملفات النظام System Files أو ملفات تجسسية Spyware بأي أسم وهمي , فأذا تم أغلاق ملف للنظام من هذه القائمة عن طريق الخطأ قد يتوقف النظام أو برنامج عن العمل وقد تضطر لأعادة تشغيل الجهاز اذا لم توقفها كما ذكرت سابقاً.

معنى هذا الكلام ان هذه الملفات مهمة جداً , ولكن يوجد بعضها غير مهمة وتكون ملفات تجسس يجب عليك حذفها في الوقت المناسب, لأن اي ملف تجسس في جهازك يكون موجود في هذه القائمة وغالباً ما يأخذ أسماء البرامج الأخرى ولكن زيادة حرف او اثنين مث ال alg.exe هذا الملف الأصلي للنظام يكون الملف التجسسي algg.exe وحتى لا يشك به المستخدم , اذا كيف نتعرف على هذه الملفات؟ لكي تتعرف على هذه الملفات التنفيذية هناك مواقع على الأنترنت من شركة ميكروسوفت تقوم بأعطائك بيانات اي ملف تنفيذي يعمل في هذه القائمة.

أولاً يجب عليك ان تتأكد من أن هذه الملفات تعمل من قائمة CPU كيف يتم ذلك ؟
في قائمة CPU هناك أرقام كثيرة وهي أستخدام المعالج للملف التنفيذي الذي يكون فعال ويعمل
تكون هذه الأرقام تعمل بجوار أسم الملف التنفيذي في قائمة CPU أنظر الصورة التالية:




في قائمة Image Name أسم ملف تنفيذي msnmsgr.exe يعمل بجواره قائمة CPU
مثلا وصل أستخدام المعالج 17 درجة هو ملف تنفيذي خاص بالMSN ولكن في بعض الأحيان
يكون المستخدم لا يعمل على برنامج MSN Messenger ويكون هناك ملف تنفيذي بنفس
هذ الأسم ولكي نتأكد من هذا الملف التنفيذي انه أمن , هناك مواقع كثيرة يمكنك من خلالها
البحث عن الملفات التنفيذية التي تشك بها و تعمل في قائمة المهام Windows Task
Manager

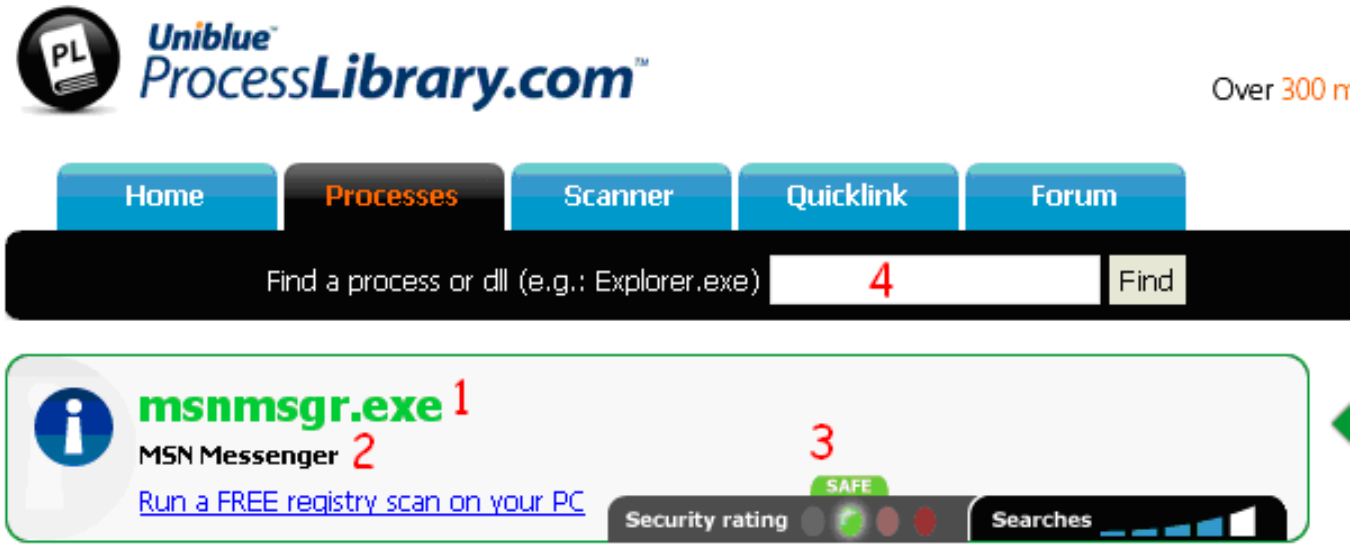
من هذه المواقع:
http://www.processlibrary.com/directory/files

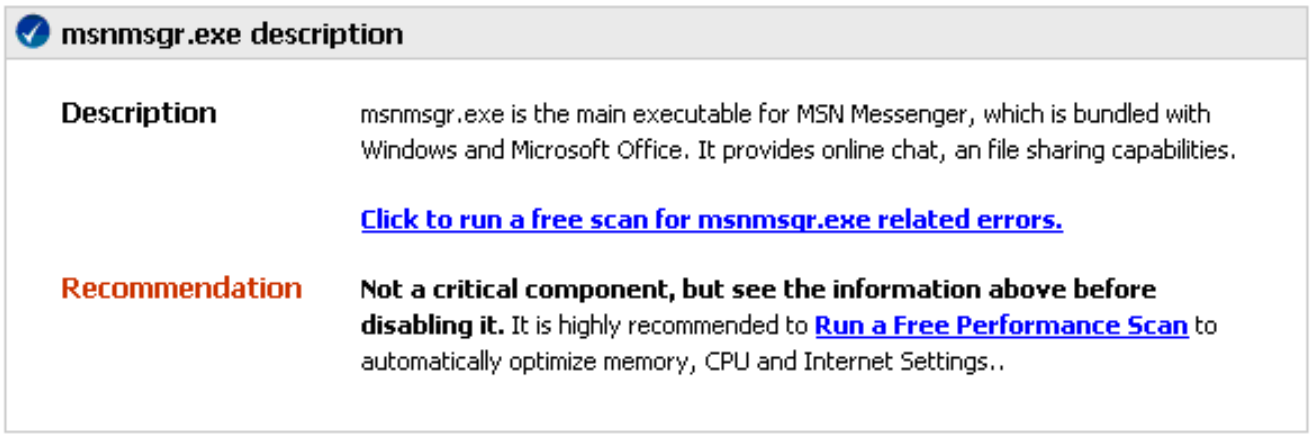
ثم اكتب اسم الملف بدون الأمتداد exe. بعد كلمة files
ليكون بهذا الشكل مثلاً:

http://www.processlibrary.com/directory/files/msnmsgr

ثم أبحث عنه

سوف يظهر لك الصفحة التالية




1 - أسم الملف msnmsgr.exe
2 - وصف الملف MSN Messenger
3 - مقياس خطر الملف SAFE يعني أمن
4 - خانة البحث عن الملفات exe. او dll.

الدرس الرابع

# 4- كيف تحمي نفسك من الأختراقات وملفات التجسس؟

- للحيطة و الحذر من الأختراقات أو الملفات التجسسية عبر الأنترنت ولكي لا يتم انتهاك خصوصيتك أتبع الخطوات التالية:

1- لابد من وجود برنامج حماية من الفيروسات وجدار ناري Zone Alarm في جهازك وأن تقوم بتحديثه بشكل دوري، **وإلا فلا فائدة من وجوده**.

2- لا تقم بفتح المرفقات في أي إيميل لا تعرف مرسله أو غير موثوق به.

3- لا تقم بفتح المرفقات في إيميلات أصدقائك إلا بعد فحصه في برامج الحماية لأن بعض التروجان والفيروسات يكون مدمج في ملف صورة ولا تقبل ملف من شخص لا تعرفه أبداً

4- لا تقوم بتحميل البرامج من مواقع غير موثوق بها أبداً وحاول بتحميل البرامج من المواقع المعروفة والموثوق فيها فقط وينصح بأستخدام نسخ قانونية و مسجّلة من البرامج.

5- لا تحاول أن تضغط على أي رابط موقع غير موثوق فيه من صفحة بريدك الألكتروني.

6- إذا قبلت ملفاً من شخص تعرفه، إفحصه أيضاً ببرنامج الحماية وتأكد أن برنامج الحماية محدث بأستمرار ، فقد يكون صديقك نفسه ضحية هذا الفايروس او ملف التجسس.

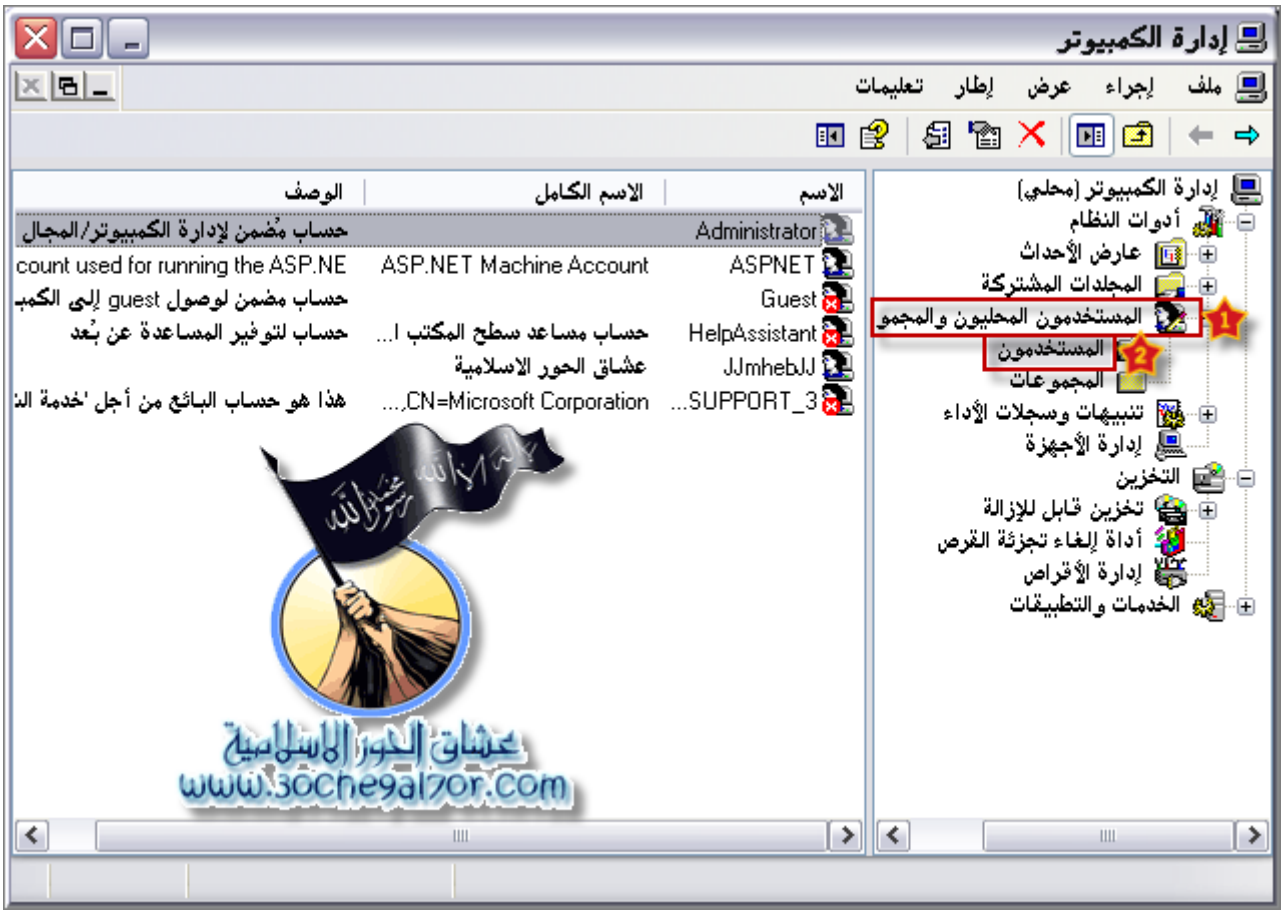
7- إحرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من قرص مرن أو سي دي. قبل أن تشغّلها.

8- أن تقوم بعمل باك أب Backup او حفظ لملفاتك المهمة بشكل دوري خارج القرص الصلب و ذلك لاسترجاعها في حالة فقدانها لأي سبب تقني أو تعرّضك لفيروس خطير قد يؤدي لتلف البيانات وتثبيت برنامج تجميد الأقراص Deepfreeze سأقوم بشرح هذه الخطوة المهمة في الدروس المقبلة لنصل سوياً للحماية القصوى إن شاء الله.

# انشاء كلمة مرور لـ حساب الـAdministrator

1


2



3


إدارة الكمبيوتر
بالموس كلك يمين
ملف إجراء عرض إطار تعليمات
الاسم
الاسم الكامل
الوصف
تعيين كلمة مرور...
كافة المهام
حذف
إعادة تسمية
خصائص
تعليمات
إدارة الكمبيوتر (محلي)
أدوات النظام
عارض الأحداث
المجلدات المشتركة
المستخدمون المحليون والمجمو
المستخدمون
المجموعات
تنبيهات وسجلات الأداء
إدارة الأجهزة
التخزين
تخزين قابل للإزالة
أداة إلغاء تجزئة القرص
إدارة الأقراص
الخدمات والتطبيقات
تعيين كلمة مرور المستخدم.
عشاق الحور الاسلامية
www.3oche9alzor.com

4


تعيين كلمة مرور إلى Administrator
إضغط هنا
متابعة
إلغاء الأمر
تعليمات
عشاق الحور الاسلامية
www.3oche9alzor.com

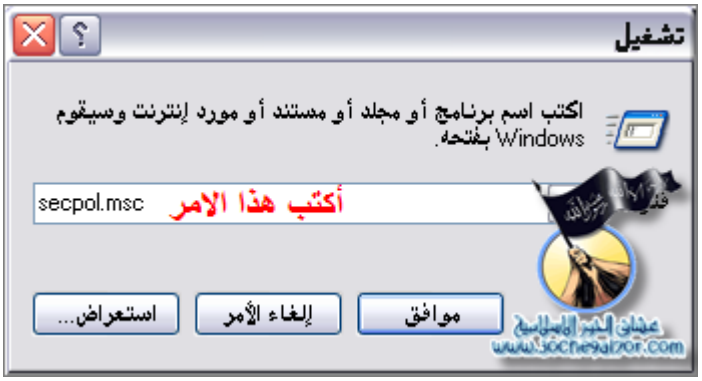
5


6


ملاحظة :تستطيع تطبيق هذه الطريقه على اي حساب موجود

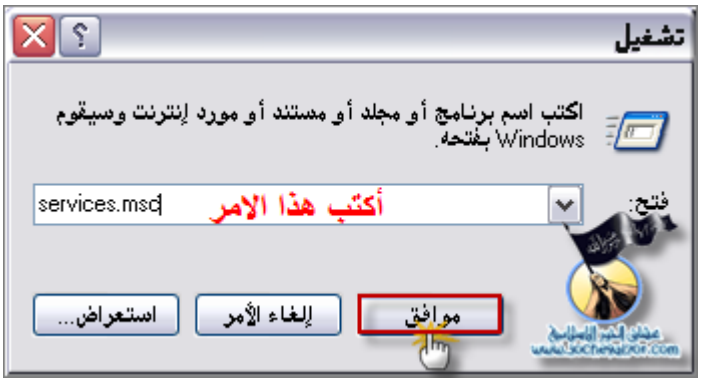
# إجبار المستخدم بوضع كلمه مرور وتحديد اقل عدد مسموح لخانات كلمة المرور






# طريقة حرمان الهاكر الى جهازك ولو كان يعرف كلمة المرور للأدمن



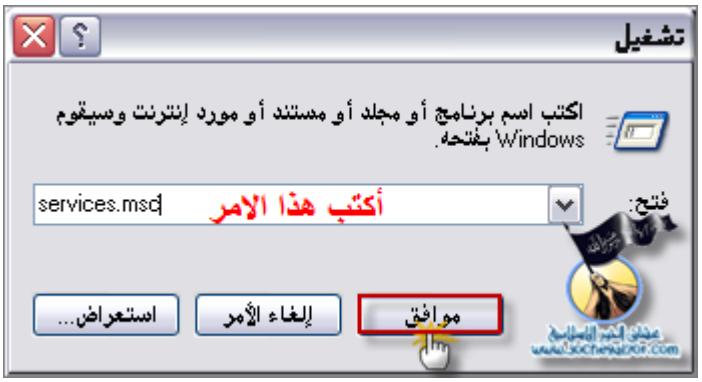


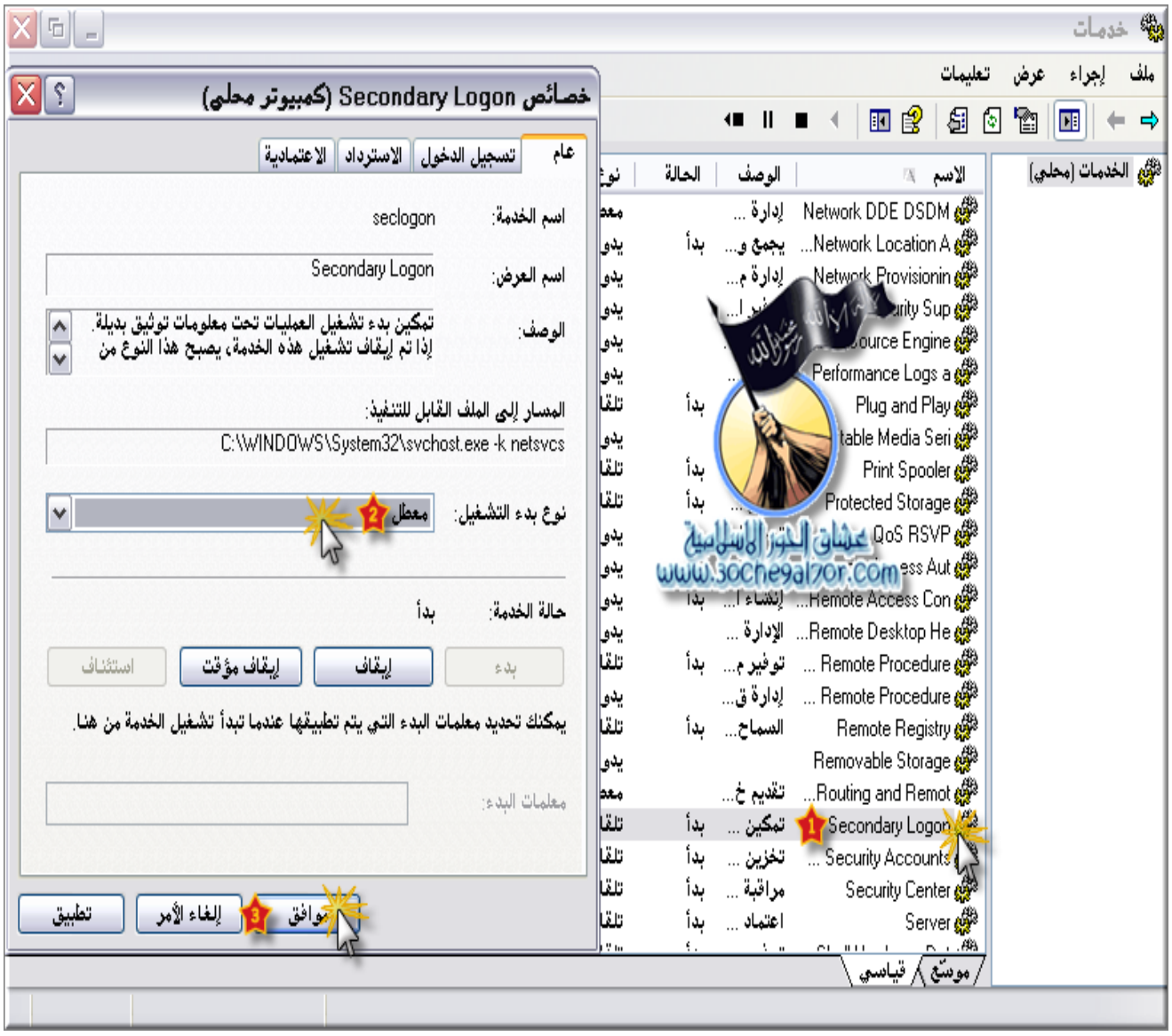


**ملاحظه خدمات Remote Desktop & Run As تتعطل لانها تعتمد على الخدمه Secondary Logon مع العلم بان المستخدم المنزلي .. نادرا ما يستخدمها ..**

للأشخاص الذين لا يملكون شبكات او طابعه او شبكه لاسلكيه ولزيادة الأمان أتبع الخطوات المصورة التالية





- اختر Remote Registry ( تعديل مسجل النظام من بعد )

- اختر Disabled

- اضغط Apply

**واعمل السابق مع هذه الخدمات**

Routing and Remote Access (التوجيه والوصول عن بعد)

Server (للمشاركه بالملفات والطابعات على الشبكه)

Terminal Services (للدخول على الجهاز من بعد)

Wireless Zero Configuration (لشبكة الوايرليس)

Print Spooler (للطابعات)

**للأشخاص الذين يملكون مشاركة ملفات على الشبكه,, وطابعه ,, وشبكه لاسلكيه**

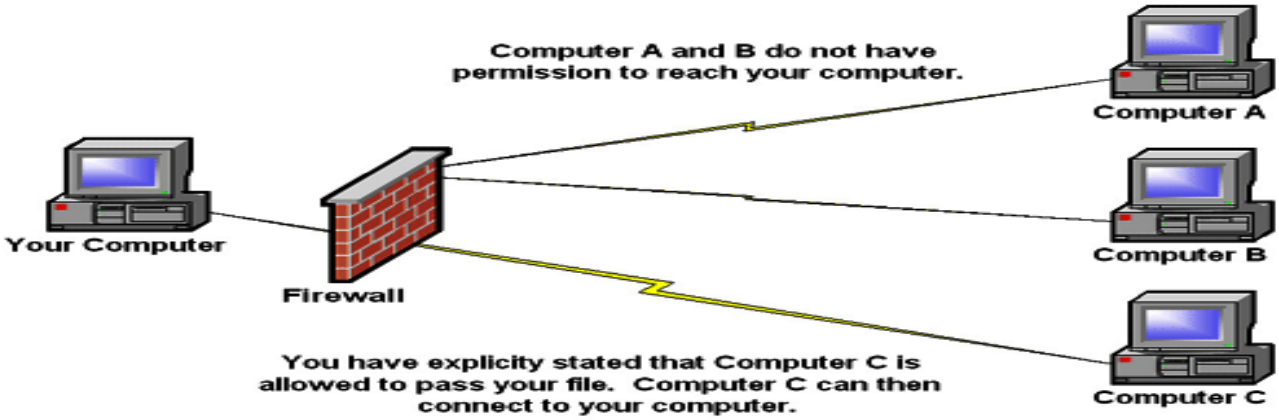
**يعطلون فقط الخدمات التاليه**

Remote Registry (تعديل مسجل النظام من بعد)

Terminal Services (للدخول على الجهاز من بعد)

Routing and Remote Access (التوجيه والوصول عن بعد)

## لماذا ينبغي عليك إستخدام جدار الحماية؟




عبر الأنترنت، يستخدم المتطفلون تعليمات برمجية خبيثة، مثل الفيروسات العادية والمتنقلة وأحصنة طروادة ، في محاولة منهم للعثور على أجهزة كمبيوتر غير محمية.

فبينما بعض الهجمات تؤدي إلى إزعاجات فقط من خلال الدعابات البسيطة، فإن غيرها يتم إنشاؤها بقصد التسبب في الضرر.

قد تحاول هذه الأنواع الخطيرة حذف معلومات من الكمبيوتر، أو تعطيله، أو حتى سرقة معلومات شخصية، مثل كلمات المرور أو أرقام البطاقات الائتمانية.

لحسن الحظ، بإمكانك تقليل خطر الإصابة من خلال استخدام جدار حماية.
كيف اختار جدار الحماية؟

يقوم جدار الحماية بتفحّص المعلومات الواردة من إنترنت والصادرة إليه. ويتعرّف على المعلومات الواردة من المواقع الخطرة أو تلك التي تثير الشك ويوقفها.

إذا أعددت جدار الحماية بشكل صحيح، فلن يتمكن المتطفلون الذين يبحثون عن أجهزة الكمبيوتر التي لا تتمتع بالحصانة من الكشف عن الكمبيوتر الخاص بك.

تتوفر ثلاثة أنواع أساسية من جدران الحماية. الخطوة الأولى عند اختيار جدار الحماية هي تحديد أي منها هو الأفضل لك. وتشمل الخيارات ما يلي:

- جدران الحماية البرمجية.
- أجهزة التوجيه.
- أجهزة التوجيه اللاسلكية.

هذا كل ما في الأمر. أنت الآن جاهز لتبدأ التفكير في نوع جدار الحماية الذي ترغب في استخدامه. هناك عدة خيارات، وكل منها له إيجابياته وسلبياته.

داوم على هذه الخطوات ولن يمسك فايروس أو تروجان أبداً أن شاء الله وقم بتحديث برامج الحماية أول بأول ، وللإطلاع على كل ما هو جديد في هذا المجال، و لإتخاذ الحيطة تابع قراءة الكتاب الألكتروني لنتوصل معاً للحماية القصوى من الأختراقات وملفات التجسس. بأذن الله

الدرس الخامس

## 5 – كيف تحمي بريد الألكتروني:

نلاحظ وبكثر مايسمى بسرقة البريد الألكتروني .وكما نعلم جميعاً أن أكثر المستخدمين يستعلمون بريد الهوت ميل لسهولته وشعبيته وانتشاره بين المستخدمين لأنه يربطهم ببعض عن طريق المسنجر.

ونلاحظ أيضاً أنه تتم سرقته بسهولة كبيره لذلك سوف أشرح لكم كيف تتم عملية سرقه بريد الهوت ميل أو أي بريد أالكتروني.

نجد أن أكثر الأشخاص الذي يُسرق ايميلاتهم هم الذين يرتادون مقاهي الأنترنت لأنه وكما نعلم أن أكثر الأجهزه تعريضاً للأختراق هي أجهزه المقاهي لأن الجهاز لا نعرف من جلس عليه قبلك ومن سوف يجلس عليه بعدك , وهنا يكمن الخطر والتهديد وسرقة البريد الألكتروني.

كل ماعليك عمله وقبل أن تستعمل أي جهاز في مقهى أنترنت هو أن تقوم بالتشييك على وجود برنامج الديب فريز deepfreeze واذ تبين انه موجود فقط قم بأعادة تشغيل الجهاز قبل وبعد جلوسك عليه , هدف هذا البرنامج هو مسح أي اعمال قام بها اي شخص جلس عليه قبلك ليقوم بسمح ملفات الأنترنت المؤقتة وملفات التجسس من قام قبلك بزرعها لك في الجهاز او تأكد من PORTS المتصلة بالجهاز وما اذا كان هناك برامج او فيروسات غير مرغوب فيها بالجهاز.

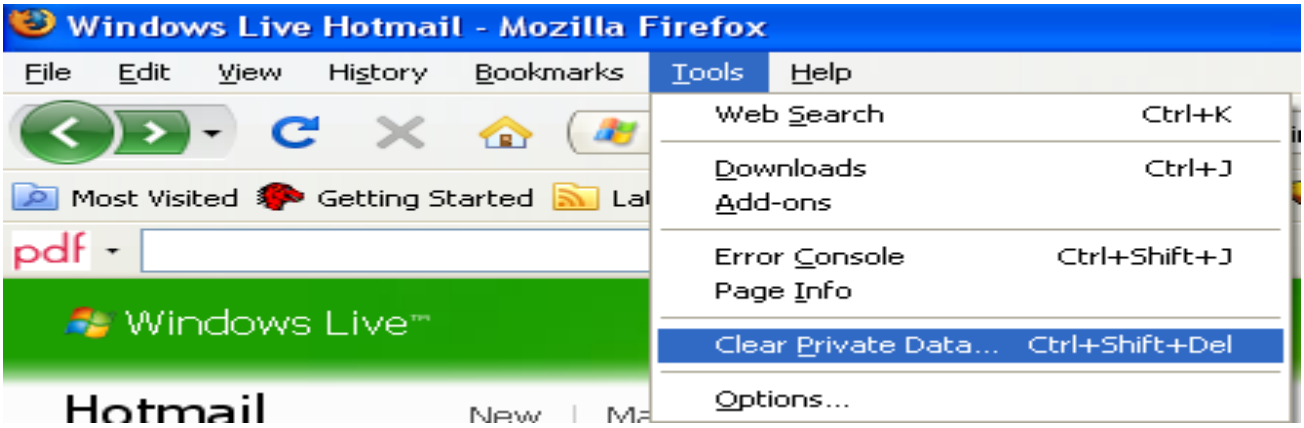
لذا فعليك أن تقوم بفحص الجهاز قبل ان تستعمله.

الأن ماذا بعد الأنتهاء من أستعمال الجهاز؟

بعد الأنتهاء عليك أن تقوم بتنظيف الجهاز من ملفات الأنترنت المؤقتة Cookies لأن أي بريد الكتروني يقوم بحفظ صفحة Inbox Email الخاصة بك في ملفات الأنترنت المؤقته.

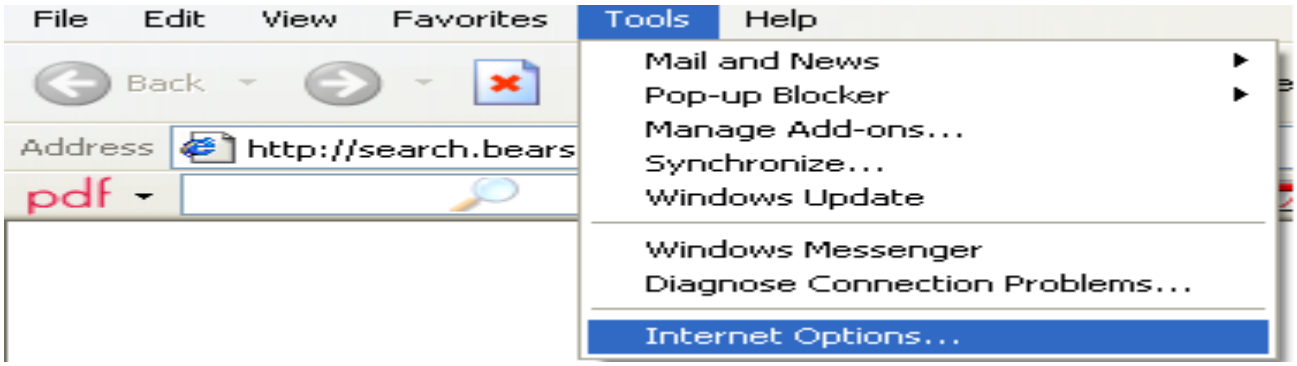
من FireFox

Tools >> Clear Private Data..




او من Internet Explorer

Tools >>> Internet Options ..




ثم

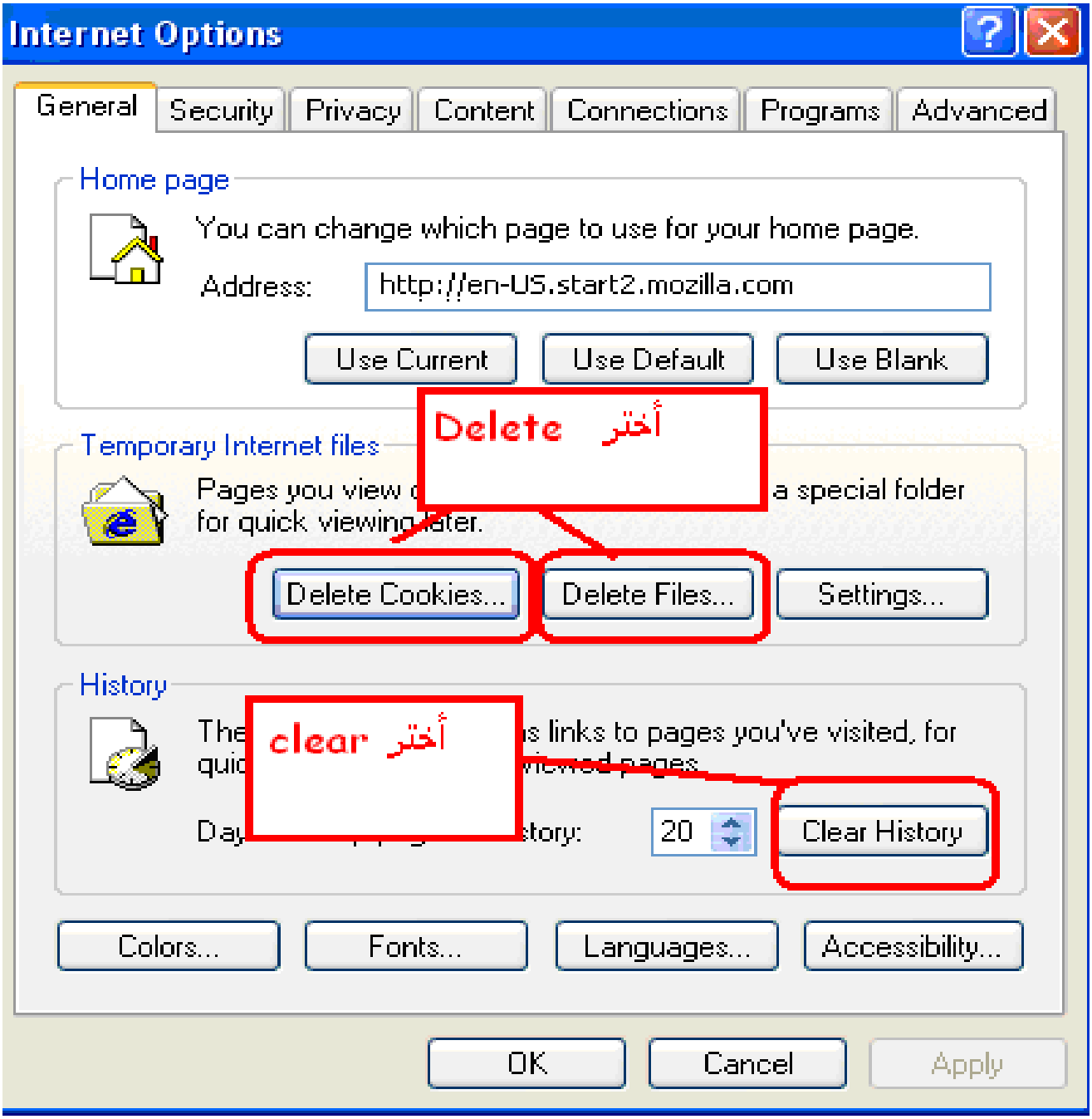
أمسح ملفات الكوكيز وملفات الأنترنت المؤقتة

Delete Cookies

Delete Files

ثم أحذف History الملفات المؤقتة

Clear History




لحذف جميع الملفات الأنترنت المؤقتة والتي يتم فيها تخزين صفحة بريدك الألكتروني.

قد تكون مهتماً جداً بلإحتمال إعتراض بريدك الإلكتروني وقراءته من قبل الآخرين، وكذلك يهتم العديد من مستخدمي الإنترنت بذلك. وبشكل فعلي، فهذه الأشياء القليلة التي تحدث ضمن الإنترنت، إذا، هل يستطيع الآخرون اعتراض بريدي الإلكتروني؟

والجواب ببساطة هو "نعم" ولكن

هل يستطيع الآخرون اعتراض بريدي الإلكتروني بسهولة؟؟

والجواب هو "لا"

فإعتراض البريد الإلكتروني ضمن الإنترنت يحتاج إلى الجهد والتخطيط المسبق. إن بيانات البريد الإلكتروني يتم نقلها عبر الإنترنت ضمن رزم Packets وهذا يعني أن رسالة البريد الإلكتروني يتم إرسالها غالباً ضمن مجموعات متعددة ولزيادة التعقيد، فلا يتم إرسالها كل رزمة بنفس المسلك الفعلي للرزم الأخرى. لذلك فأي شخص يريد اعتراض البريد الإلكتروني، يجب أن يمتلك خبرة تقنية عالية إضافة إلى خبرته في الوصول إلى الكمبيوترات وخطوط البيانات التي تتعامل مع الرسائل الإلكترونية، كما أنه يجب عليه أن يبذل مزيداً من الجهد لتعقب الرزم واعتراضها وإعادة تجميعها وهذا يشار إليه عادة بالمصطلح:

Packet-sniffing

وهو بحد ذاته تطبيق متوفر بالأنترنت يستغله المخترقون وهنا هو عامل الخطورة لأنه مع وجود التطبيقات المناسبة وانتشارها بالإنترنت، يتوفر عامل يدعم عمليات اعتراض البريد الإلكتروني ويسهل هذه المهمة فلا تحسبن أن الجهد والمشقة سيكونان مضنيين على الراغب بقوة في اعتراض بريدك الإلكتروني واحرص في ذلك على حماية منطقتك الأمنية...

## خطوات مهمة لحماية بريدك الألكتروني من السرقة:

- غير رقمك السري بأستمرار:

تأكد من تغيير رقمك السري بأستمرار.. تأكد من أستخدام أرقام سرية قوية بأن يتكون الرقم السري من أرقام و حروف معاً بأستخدم زر SHIFT ليصبح هكذا مثلا:

!@#$%^&*

الرقم الأصلي

12345678

بأستطاعك اضافة حروف في وسط الأرقام وينصح ان يكون الرقم السري مكون من أثنى عشرة حرفاً ورقماً بأستخدام زر SHIFT على الأقل حتى يصعب كسره.

- لاتعطي رقمك السري لأي كان:

تأكد من أن لا تعطي اي شخص كان رقمك السري .. حتى لو وصلتك رسالة من مقدم بريدك تطلب منك ارسال رقمك السري.. مثلا لو كان لديك بريد على شركة الهوتميل ووصلتك رسالة من جهة تدعي انها إدارة الهوتميل مثلاً:

Livehotmail-server@hotmail.com

بأرسال الرقم السري لهم لا ترسله لهم في اي حال من الأحوال فإن الشركة المقدمة لن تطلب منك ذلك ابداً و هي حيلة قديمة لإستغفالك و أخذ رقمك السري.

وعدم وضع الباسورد بملف وحفظه داخل الجهاز لانه لا سمح الله اذا دخل هاكرز جهازك سيجدها على طبق من ذهب.

- لا تفتح أي ملف مرفق من أي كان:

لا تفتح أي ملف مرفق من أي كان حتى لو كان من صديقك لا تفتحه إذا لم يكن هناك وصف او شرح لنوعية الملف المرفق أو لم تكن تعلم ما هو.

هناك بعض ملفات التجسس ممكن ان يزرعها الهكرز بجهازك عن طريق البريد الألكتروني وهذه الملفات تتولى ارسال له جميع الأرقام السرية التي تدخلها في جهازك او كل ما تكتبه على لوحة التحكم "الكيبورد" من كلمات سرية وهذا الملف خطير جدا واسمه:

Key logger

لذلك ينصح ان لا تقبل اي ملف من اي شخص لا تعرفه.

- تأكد من الخروج من حسابك البريدي log Out :

تأكد دائما من الخروج من بريدك باختيار Log Out فهذا قد يجعل أقتحام بريدك صعب جدا جدا و مقتصر على المحترفين.

كما تأكد من إغلاق المتصفح بعد الخروج من البريد خاصة لو كنت تطالع بريدك من خارج منزلك او من مقهى الأنترنيت وحفظ ملفات الأنترت المؤقتة.

حاول بأن تقوم بحفظ كلمة السر في الماسنجر بعد ذلك قم بحذف ملفات الأنترنت المؤقتة والكوكيز حتى يتم مسح login لكلمة السر الخاصة بك في ملفات الأنترنت ولا يعرفه المخترق.

- لا ترد على الرسائل التي تأتيك بغرض الدعاية او التي تدعوك لمواقع إباحية مثلا Spam

فهذا يدلهم على انه بريد ما زال قيد الاستخدام و سيعرضك لمضايقات اكثر . توجد في بعض انواع البريد المقدمة ما يسمى الفلتر Filter حيث يمكنك ان تعطي اسماء العناوين التي لا تريد استقبال بريد منهم .

- كن ذكيا :

أنا متأكد من أنك كذلك ..و لكن على تنبيهك على أي حال في الغالب يطلب منك عند تسجيل بريدك سؤال حتى يتمكن النظام من تذكيرك برقمك السري عند فقدانه . قد يقوم البعض بوضع سؤال كالتالي .. Where do I live? مثلا أين اعيش أجعل الجواب ليس له علاقه بالسؤال حتى اذا قام المخترق بالتخمين يصعب عليه ذلك , وتأكد من وضع سؤال غريب و جواب أغرب , أهم خطوة هي أن تتأكد من أيميلك البديل Alternate Email ان يكون الرقم السري مختلف عن الرقم السري الخاص بالأيميل الأول , حتى إذا نسيت رقم المرور و طلبت أسترجاع كلمة المرور من إيميلك البديل Alternate Email وحتى إذا تم سرقة ايميلك لا سمح الله لا يكون المخترق قد قام يتغيير الرقم السري الخاص بأيميلك البديل Alternate Email , سوف اقوم بشرح هذه الخطوة المهمة في الخطوات القادمة من الكتاب ان شاء الله.

- جدد دائما :

لو كنت تستخدم برنامج لأستقبال البريد الالكتروني تأكد دائما من تجديد برنامجك و تطويره حتى تكون كل إجراءات الأمن بحوزتك.

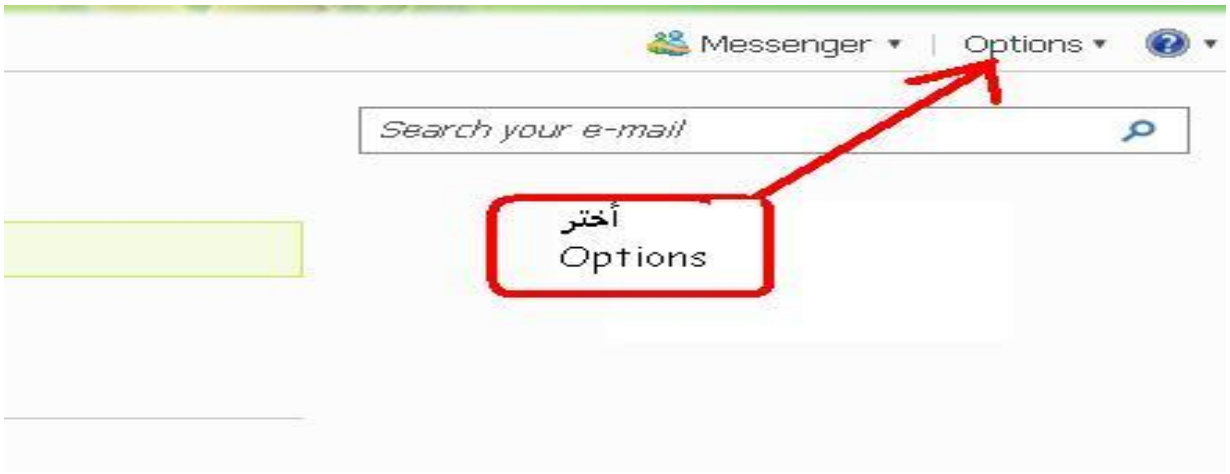

الملاحظ هذه الفترة كثرت الاختراقات للمواقع وأيضا سرقة الايميلات ... والبعض منها يتعرض الى التدمير بواسطة برامج خاصة مثل BOMB او SPAM وهي عملية أغراق البريد الألكتروني بالرسايل حتى يتم غلق البريد من قبل الشركة وهذا يعتبر عمل تخريبيي.

**طريقة حماية البريد الألكتروني من هذه الرسائل التدميرية او السبام:**

إليكم الطريقة التالية :

أدخل الى بريدك في الهوتميل

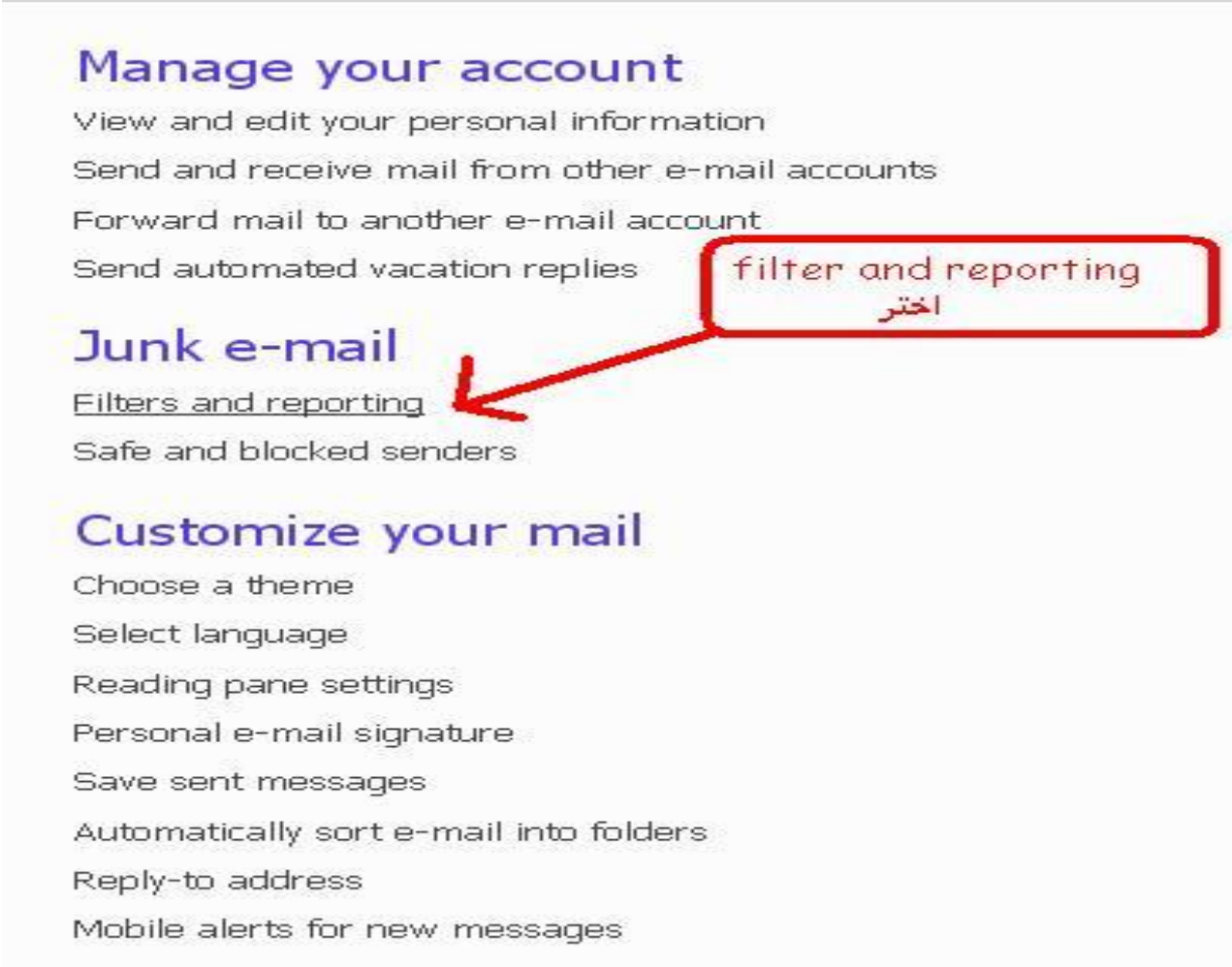
2- بعد دخولك الى بريدك الألكتروني .....أذهب الى OPTIONS .




ثم

أختر


3- بعد دخولك الى OPTIONS ....اذهب الىJunk Mail Filter .




4- بعد دخولك الى Junk Mail Filter .....سوف تجدون عدة خيارات ..كالتالي:

Low

Standard

Exclusive

قم بأختيار LOW .....


5- اضغط على OK ....لحفظ التغييرات.

سوف تلاحظون ان هناك فولدر FOLDER جديد..

قد تم تكوينه في بريدك وهو Junk Mail على اليسار.

هذا الفولدر هو امنك وامانك.....يعني.....اي قنبله بريديه تستهدف بريدك...فسوف تدخل الى هذا الفولدر...ولن تذهب اي قنبله الى ال INBOX.

هذه الطريقه تهدف الى تحصين بريدك ضد القنابل البريديه SPAM انصح الجميع باتباعها

, ايضاً أنتشرت برامج تخمين كلمات السر , تستطيع أن تتكفل بالمهمة وخصوصاً اذا كانت الرقم السري قصير او عبارة عن أرقام على شكل حركات او أسامي معروفة ومن اشهر هذه البرامج :

munga bunga

e-mail crack

http port

menhaten

girl friend

وهذه البرامج تكمن مهمتهم في تخمين قائمة كبيرة من كلمات السر على بريدك وللوقاية من جميع هذه البرامج ينصح أن يكون الرقم السري مكون من أثنى عشرة حرفاً ورقماً ورمزاً بأستخدام زر SHIFT على الأقل حتى يصعب تخمينه وكسره بسهولة.

اما بالنسبة للماسنجر فإذا طلب منك أي شخص محادثة صوتية لا تقبلها الا اذا كنت تثق به حيث عن طريق المحادثة الصوتية يستطيع بسهولة الحصول على الأي بي الخاص بك ويخترق الجهاز ببرنامج مستكشف الأيبي الاصدار الاخير.

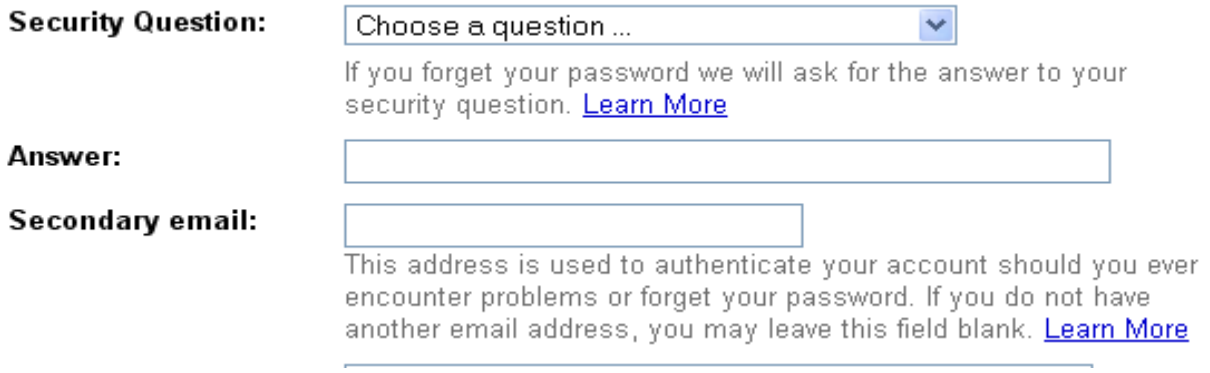
وبذلك تكون قد حميت بريدك من كل أنواع السرقة.

ماذا لو قد تم سرقة ايميلك وتغيير السؤال السري؟؟؟ هل من الممكن إستراجع الأيميل؟؟؟

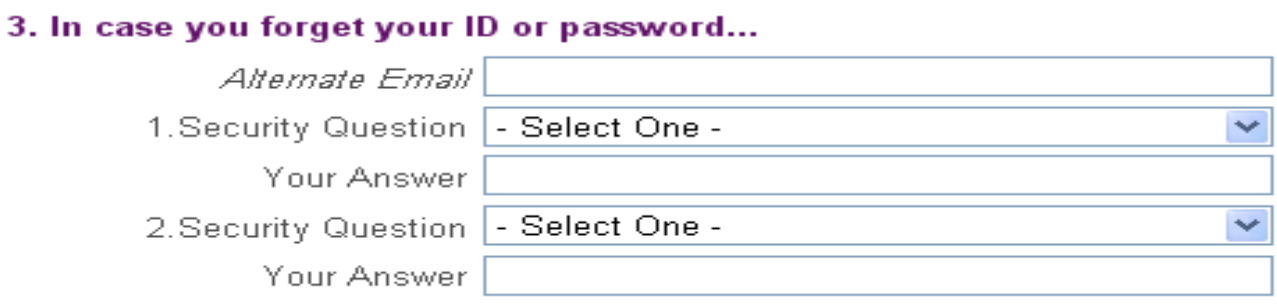
الجواب "نعم" ممكن وهذا على حسب قوة المخترق وطريقة تفكيره وعدم تغييره للأيميل البديل.

في كل بريد إلكتروني وعند التسجيل لأول مرة يسألك عن Alternate Email أو Secondary email هذا البريد الألكتروني هو بمثابة ضمانة في حال تم تغيير الرقم السري الخاص بأيميلك وتغيير السؤال السري كذلك او لم تتذكره او تم سرقته , تستطيع من خلال هذا الأيميل البديل استرجاع الرقم السري وبدون استخدام الجواب والسؤال السري اذ تم تغييره عن طريق رابط وصلة أنترنت تابع معي الصور التالية:

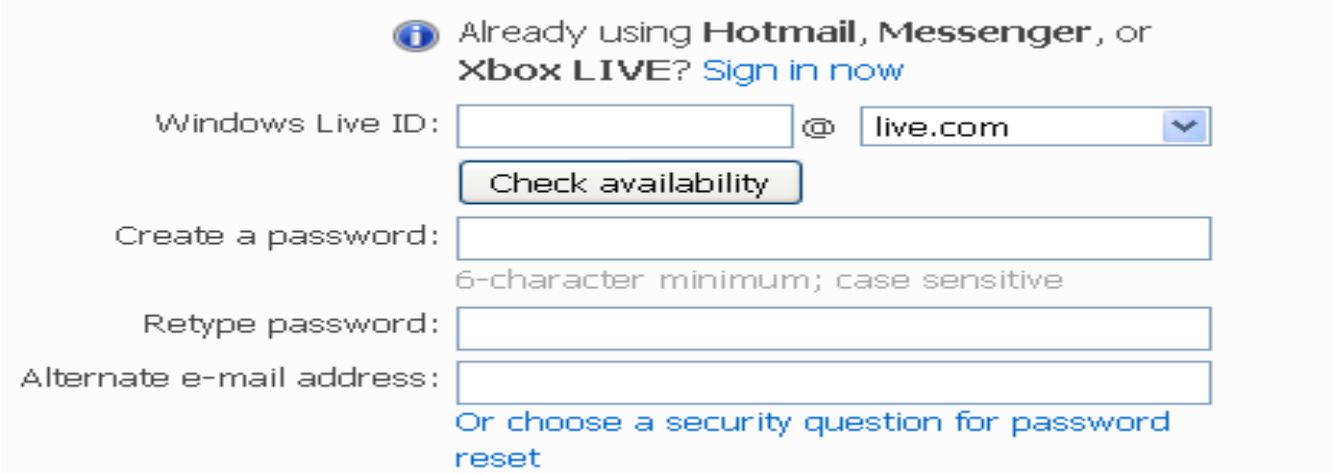
عند التسجيل لأول مرة في بريد Gmail تجده هنا بأسم Secondary email




وفي بريد Yahoo موجود هنا Alternate Email

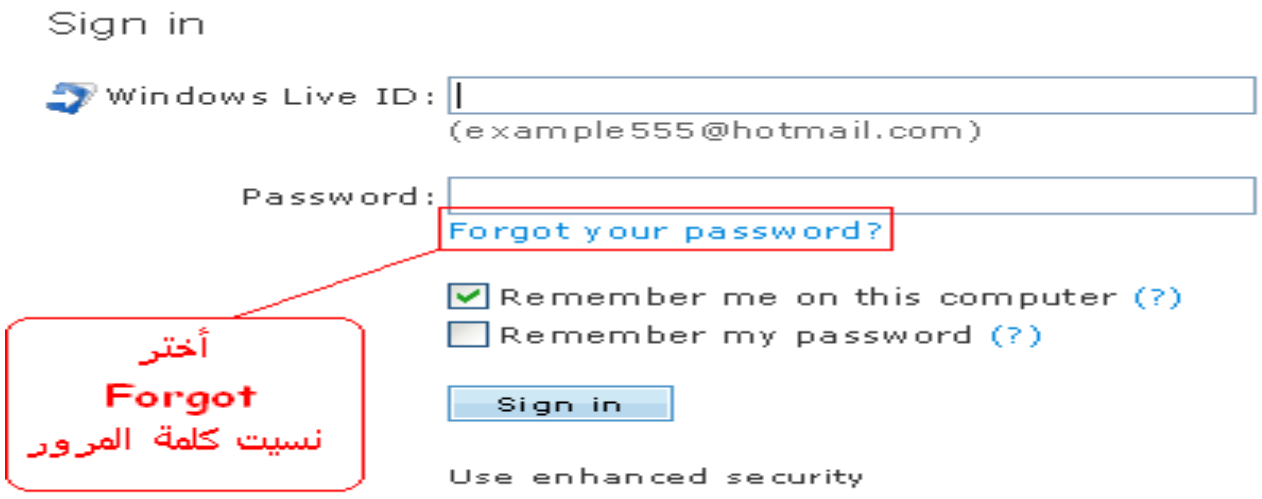


وفي بريد hotmail موجود هنا Alternate Email




اذا فقدت كلمة مرورك والسؤال والجواب السري كل ما عليك فعله هو أن تذهب إلي الصفحة الرئيسية للدخول Sign in في Hotmail

ثم أختر Forget your password

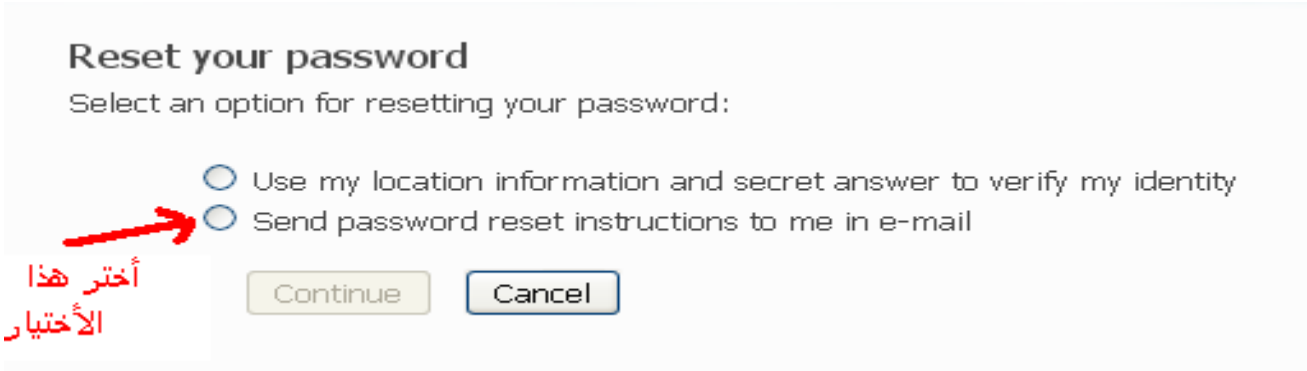



بعد الضغط على Forget your password سوف تذهب إلي صفحة

Reset Your Password

ثم اتبع الصورة التالية:


ثم أضغط Continue سوف تذهب إلي هذه الصفحة:




Use my location information and secret answer to verify my identity

هذا الأختيار لوضع كلمة المرور والجواب السري.

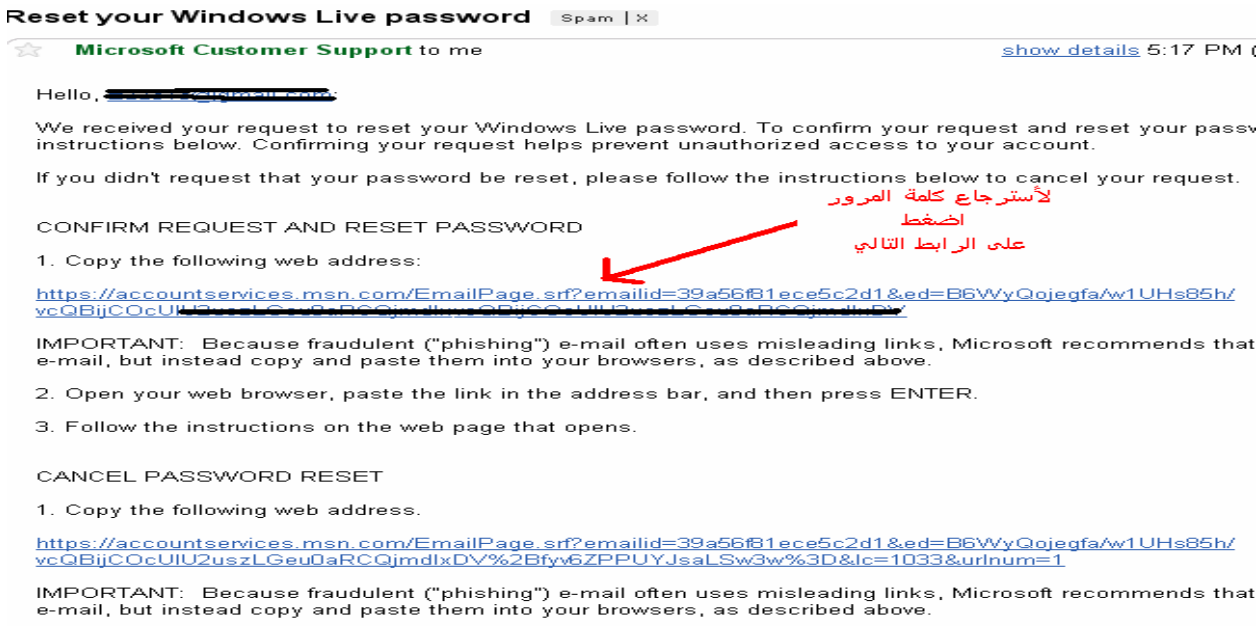
Send password reset instructions to me in e-mail

هذا الأختيار لأرسال رسالة الي الأيميل فيها كلمة المرور الجديدة.

وفي حالتنا سوف نختار الأختيار الثاني بما انه قد تم نسيان الرقم السري والجواب السري لتقوم الشركة بأرسال رسالة الي بريدنا الألكتروني الذي وضعناه في أول التسجيل Alternate e-mail بالرقم الجديد الذي سوف نقوم نحن بكتابته **اذا لم يتم تغييره سابقاً**.

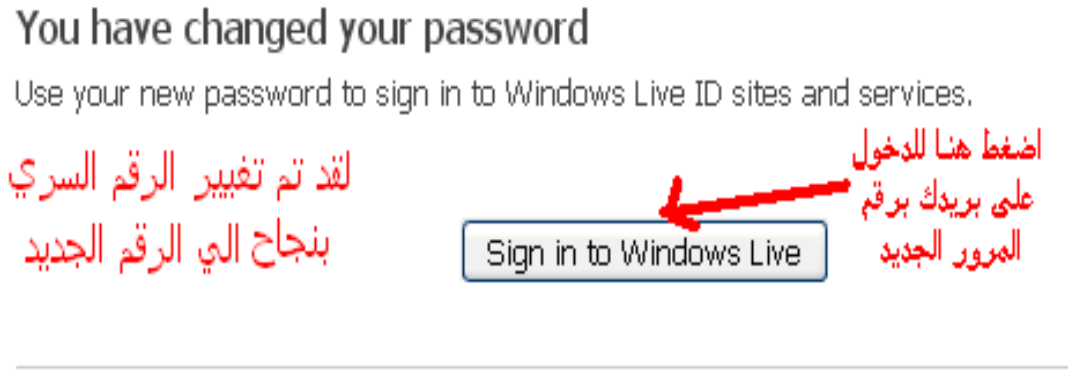

تستطيع تغيير Alternate e-mail في بريد Hotmail من Options ثم More Options ثم أختر View and edit your personal information ثم Alternate e-mail address وأختر Change وسوف يتم تغييره.

بعد الضغط على Continue في الصورة السابقة سوف يتم إرسال كلمة المرور الجديدة على الأيميل الذي وضعته في Alternate e-mail اثناء التسجيل وهذا هو نص الرسالة:



بعد الضغط على الرابط أعلاه سوف تذهب الي صفحة وضع كلمة المرور الجديدة وتكرارها مرة أخرى:


ثم أضغط Continue سوف تذهب الي هذه الصفحة:



الأن يخبرك أن تم تغيير الرقم السري وبأمكانك أستعمال الرقم السري الجديد الأن في الدخول على صفحة بريدك الألكتروني , أضغطٍ Sign in to windows live ثم أدخل على بريدك الأن برقم المرور الجديد ومبروك عليك تم أسترجاع إيميلك بخطوات سريعة وبسيطة جدا جدا.

ويمكنك ايضاً فحص جهازك أونلاين للتأكد من خلوه من الفيروسات عبر هذه المواقع:

وهي طريقة جيدة لتفادي تلف مكافح الفيروسات بسبب ضربه بواسطة فايروس ، فالفحص الخارجي عادة اكثر دقة وقوة.

وفيما يلي اشهر المواقع التي تتيح فحص الجهاز من الشبكة

سواء فيروسات او آدوير او سباي وير وتروجان

((اضغط على الصورة للشركة المختارة))

TREND MICRO

http://housecall65.trendmicro.com

فحص ملف مفرد

http://www.kaspersky.com/scanforvirus/

فحص الجهاز كاملا

http://www.kaspersky.com/virusscanner

McAfee®

http://home.mcafee.com/Downloads/FreeScan.aspx

ca Transforming IT Management

http://cainternetsecurity.net/entscanner/

SCAN ONLINE NEW

http://www.bitdefender.com/scanner/online/free.html

F-SECURE ONLINE SCANNER
scan your computer for viruses
F-SECURE

http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/online-scanner/index.html

symantec.

http://security.symantec.com/sscv6/WelcomePage.asp

PANDA SECURITY | One step ahead.

http://www.pandasecurity.com/homeusers/solutions/activescan


http://onlinescan.avast.com/

http://www.eset.com/onlinescan/

http://www.xblock.com/references.php

Addware & SpyWare((اضغط على الصورة للشركة المختارة))

http://www.noadware.net/?hop=adwords101

http://www.webroot.com/En_US/land-freescan-ent.html

http://www.tenebril.com/scanner/main_start.php


http://www.process.com/spycatcher/scan.html

/http://www.windowsecurity.com/trojanscan

مع العلم بان كل تلك المواقع تتطلب تثبيت عنصر التحكم

ActivX بجهازك لكي يتمكن من فحص الجهاز من الموقع

# التصنيف العالمي لأقوى برامج الحماية بحسب الموقع toptenreviews.com

| Rank | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Excellent / Very Good / Good / Fair / Poor | BitDefender Antivirus | Kaspersky Anti-Virus | Webroot Antivirus | G DATA AntiVirus | ESET Nod32 | ParetoLogic Anti-Virus PLUS | AVG Anti-Virus | Vipre Antivirus + Antispyware | F-Secure Anti-Virus | Trend Micro |
| Reviewer Comments | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW | READ REVIEW |
| Lowest Price | BUY $24.95 | BUY $39.95 | BUY $39.95 | BUY $29.00 | BUY $39.99 | BUY $39.95 | BUY $34.99 | BUY $29.95 | BUY $39.99 | BUY $10.96 |
| Overall Rating | | | | | | | | | | |
| Ratings | | | | | | | | | | |
| Ease of Use | | | | | | | | | | |
| Effectiveness | | | | | | | | | | |
| Updates | | | | | | | | | | |
| Feature Set | | | | | | | | | | |
| Ease of Installation | | | | | | | | | | |
| Help/Support | | | | | | | | | | |
| View Specifications | Go! | Go! | Go! | Go! | Go! | Go! | Go! | Go! | Go! | Go! |
| View Screenshots | | | | | | | | | | |

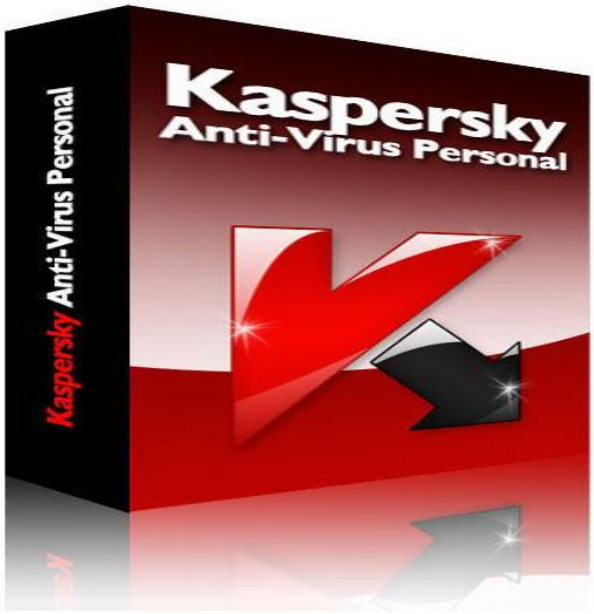


رابط الموقع والتصنيف

http://anti-virus-software-review.toptenreviews.com/

## أهم برامج الحماية:

### العملاق الروسي KasperSky Anti-Virus Personal من أقوى برامج الحماية بالعالم:




برنامج مضاد للفيروسات بشكل فائق الجودة و لايمكن مقارنته بأي برنامج آخر سواء نورتون أو مكافي **فهذا البرنامج لديه من الإمكانيات ما تجعله الأفضل على الإطلاق.**
ويعطيك البرنامج خمس اختيارات لمستوى الحمايه تستطيع ان تقوم باختيار المناسب لك وذلك لصد الهكرز وملفات التجسس.

التقييم : ممتاز جدا جدا

يعمل مع Windows 2000, 9x, XP

### البرنامج الرائع والقوي جداً Bit defender


البرنامج الرائع للحماية ضد الفايروسات والسبايوير من أقوى وأذكى البرامج في هذا المجال ضد الفيروسات رزمة متفوقة فريدة، محركات قوية مدمجة ضد الفيروسات بتقنيات ترشيح انترنت متقدمة بالإضافة الى الحمايةً ضد الفيروسات سرية للبيانات سيطرة راضية نشيطة وترشيح الإنترنت. يجري البرنامج بشكل صامت في الخلفية ويضمن الحماية المثالية لمعلوماتك الحيوية، يستعمل محركات قوية لترشيح كل طرق الوصول المحتملة من الفايروسات أَو الرموز الخبيثة التى يمكن أَن تستعمل لدخول نظامك. الفيروسات:أكثر من الحماية ضد الفيروسات، ليصبح برنامج حماية شخصي حقيقي..
وهو أقوى من Antivirus

التقييم : ممتاز جدا جدا

يعمل مع Windows 2000, 9x, XP

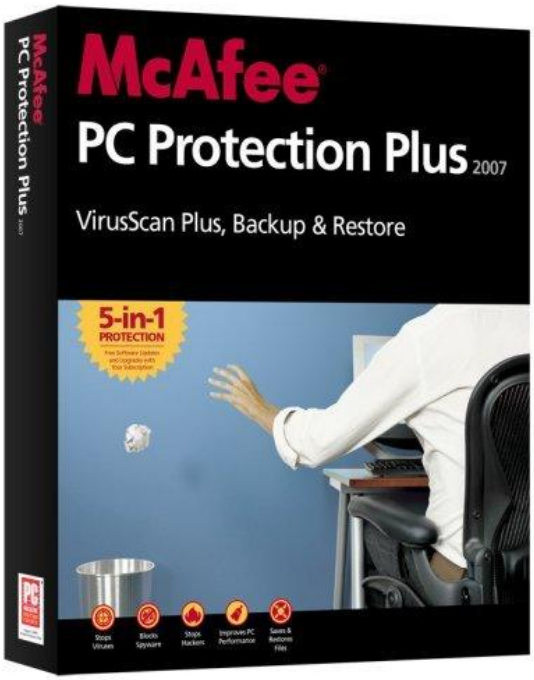
## برنامج Zone Alarm حماية (وجدار ناري) قوي وفعال جداً:


من أقوى البرامج لحماية جهازك من إختراق المخربين حيث يقدم أربع أنواع من الحمايات بحيث يمنع أي أختراق لجهازك , ويدعم ايضاً جدار ناري قوي جداً Firewall لصد أي هجوم على جهازك برنامج قوي ولا غنى عنه.

التقييم : ممتاز جدا جدا

يعمل مع Windows 2000, 9x, XP

## برنامج Mcafee




حماية للجهاز من الاختراق يقوم البرنامج بحماية جهازك الخاص من الغزاة والمتطفلين بمراقبة نشاطات الشبكة لا شيء يدخل جهازك او يغادره بدون اذنك ولذلك يمكنك حماية ملفاتك بشكل مستمر ويحتوي على انظمة حماية اخرى والتي تزيد من مستوى الامن لجهازك

التقييم : جيد جداً

يعمل مع Windows 2000, 9x, XP

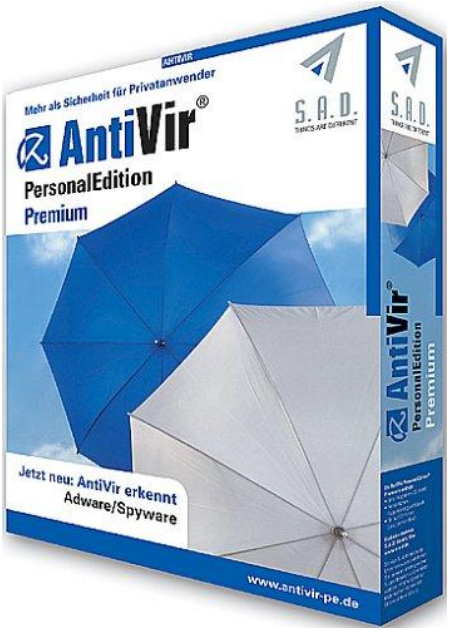
## برنامج NOD32


يعد هذا البرنامج من أقوى برامج مكافحة الفايروسات
به 32 ميزه للحمايه وهو خفيف على الجهاز ..
من عيوبه حذف الفيروس مع الملف المحتوى
على الفيروس مما يعني انه قد يحذف
ملف مهم يؤثر على اداء الجهاز.

التقييم : ممتاز جداً

يعمل مع Windows NT/2000/2003/XP/ x64

## برنامج AntiVir




نسخه حديثه من هذا البرنامج المجاني الذي يقوم بحماية
جهازك من الفايروسات ... فهو يقوم بكشف وازالة اكثر
من 50 الف فايروس كما يمكن تحديثه عن طريق
الإنترنت مباشرة ... وهو متوافق مع كل إصدارت
الويندوز

التقييم : جيد جداً

يعمل معWindows 2000, 9x, XP

ملحوظة: تستطيع تثبيت برنامجين حماية في جهاز واحد هذا اذا لم يحدث تضارب بين البرنامجيين واذ حدث بأمكانك تفعيل واحد منهم فقط Enable والثاني يكون غير مفعل disable وذلك عند بداية الأقلاع للجهاز Start >> Run >> msconfig ثم اذهب الي Start up وقم بإلغاء برنامج منهم عند بداية التشغيل , حتى لا يحدث تضارب بين البرنامجيين وتستطيع أستخدامهم في البحث عن ملف واحد بواسطة البرنامجيين في أن واحد.

اداة

# Windows Worms Doors Cleaner

**لتقفيل وبشكل تاااااام المنافذ (( الخطيره )) 135 و 445 و 137 و 138 و 139 و 5000**

**وذلك بتعطيل الخدمات ( الغير مستخدمه ) التي تستخدم هذه المنافذ**

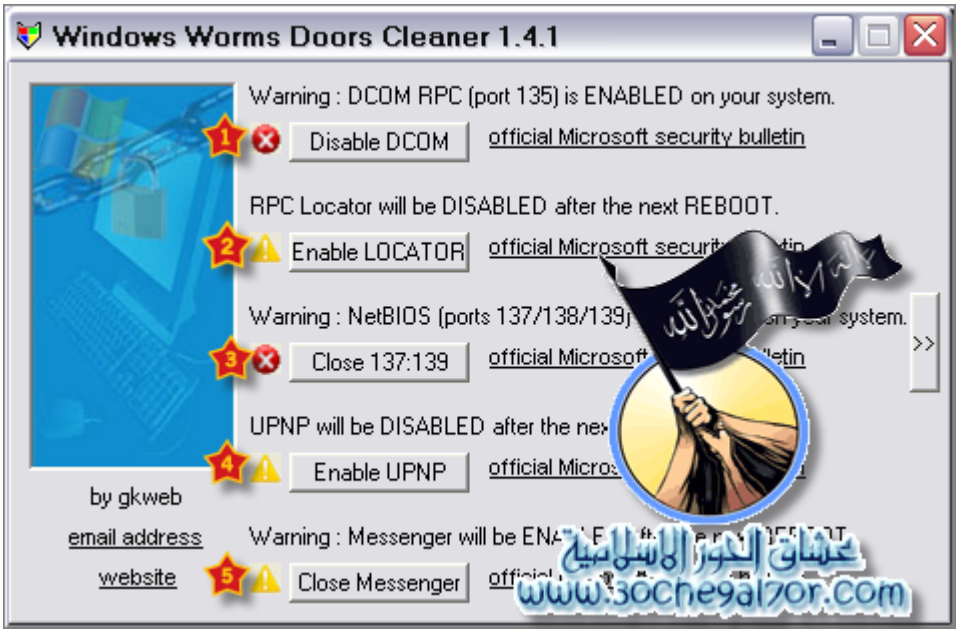
**وهذا شرح لعملية اغلاق المنافذ الخطيره**

**كما بالصوره اضغط على المفتاح**

**(( Close ))**

**لكل منفذ**

**بعدها اعد تشغيل الجهاز**



الدرس السادس

# 6- الحمـــايـــة القـــصوى

في هذا القسم سأقوم بشرح خطوات بسيطة تجعل جهازك الشخصي يصل الي الحماية القصوى من الأختراق بطريقة فعالة وقوية جداً جداً.

لماذا أخترت هذا الأسم "الحماية القصوى" ؟

لأن في الحقيقة هذا اخر ما توصلت اليه شخصيا في حماية ولن تجد في أي مكان في العالم شيءً كاملاً ومعنى هذا الكلام إنك لن تجد حماية كاملة لذلك لن تجد حماية 100% بل هناك 99.9% حماية , لأن الكمال لله وحده لا شريك له ولا كامل إلا وجه الله تعالى سبحانه وتعالى.

هناك مثل أنجليزي يقول:

Security is a Big Lie

معنى هذا الكلام ان الحماية هي اكبر كذبة ان لا يوجد حماية كاملة 100% **ولكن**.....

ليس معنى هذا الكلام انه لا يوجد حماية لا بل و **بالعكس** هناك حمايات وحمايات قوية جداً جداً ايضاً ومثل ما ذكرت سابقاً عن أاقوى برامج الحماية التي تقوم بكشف ملفات الفيروسات والتروجان وملفات التجسس والتي احياناً يصعب تشفيرها عن هذه الحمايات القوية وحمايتها احياناً تصل الي 99.9% وأستخدام الجدار الناري مهم جداً وكل شيء يعتمد عليك في البداية.

ولكن في الأول والأخير لهذه البرامج ثغرات يتم اختراقها مثل المواقع ليس هناك موقع يصعب اختراقه ولا تنسى انه تم إختراق سابقاً موقع البنتاجون الأمريكي , لذلك لن تجد حماية كاملة ولن تجد مخترق كامل فالحماية امراً سهلاً وليس أمراً صعباً , وفي الأول والأخير نحن نسعى الي تحقيق أقصى درجات الحماية في هذا القسم إن شاء الله لأجهزتنا لذلك قمت بعمل هذا القسم بأسم "**الحمـايـة القصـوى**" لأشرح بعض الخطوات التي نسعى فيها الي تحقيق أقو ى درجات الحماية وتخطي المتخرقون بشكل خاص وعام.

كما قلت في الصفحات السابقة من الكتاب يجب عليك بتحميل برنامج حماية ويكون أخر إصدار وتقوم بتحديثه أول بأول وأنصح ببرنامج Kaspersky برنامج رائع وفعال جداً وبرنامج Zone Alarm الجدار ناري القوي جداً , هذه أول خطوة يجب ان تتخذها كبداية للطريق الي "**الحماية القصوى** " يجب عليك ان تقوم بتحديث برامج الحماية قبل عملية البحث والفحص للجهاز, وان تتأكد كل التأكد انك قمت بعمل فحص كامل لجميع الأقراص وملفات الريجيستري في جهازك بعد عملية التحديث لبرامج الحماية , قم بتفعيل الجدار الناري وقد ارفقت في الكتاب بعض المواقع الأونلاين لفحص الجهاز من الفيروسات وملفات التجسس , يجب ان تتأكد ان يكون الجهاز نظيفاً من اي ملفات ضارة , أو يمكنك حفظ بياناتك المهمة في قرص خارجي وعمل فورمات وتقسيم جديد للقرص الصلب , ولذلك لتضمن خلو جهازك من اي نوع من الملفات الضارة قبل البدأ في الخطوة التالية ان شاء الله خطوة الحماية القصوى.

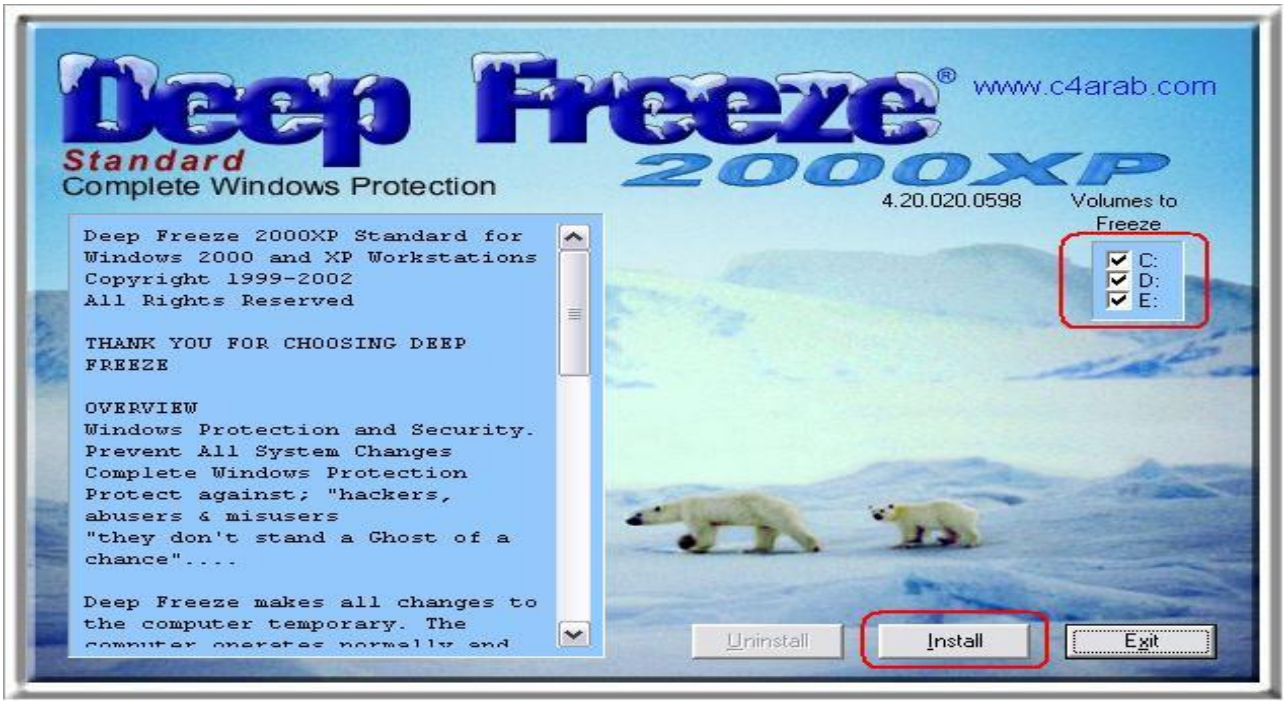

ثالث نقطة وأهم نقطة في هذا الدرس والتي أنصح بها الجميع وهي تثبيت برنامج **Deepfreeze**العملاق والقوي جداً جداً فعال في الأمن والحماية, يقوم بتجميد القرص الصلب C الي أخر وضعية قمت بطلب البرنامج بعمل تجميد له لذلك اذا لا سمح الله اذا قمت بتشغيل ملف تجسسي او قمت بفتح فايروس وتم تخطي هذا الفايروس او ملف التجسس برنامج الحماية في جهازك و الجدار الناري ايضا Zone Alarm Firewall فيكون برنامج الديب فريز له بالمصد الثالث لأنه سوف يرجع كل شيء كما كان بعد اعادة تشغيل الجهاز **وحتى بعد عملية الأختراق.**

تخيل معي لا سمح الله دخلت موقع وكان فيه ملف تجسس او قمت بأستقبال ملف من أحد الأصدقاء عن طريق الخطأ وكان ملف تجسسي يستطيع التحكم في جهازك او تخريبيه , وعند استقبال هذا الملف التجسسي قمت بعمل بحث عنه ببرنامج الحماية لديك فلم يجد شيئاً والجدار الناري لم يجد شيئاً كذلك ولكن وأنت جالس شعرت بتغير في سرعة الجهاز او ببطء او تغير غير طبيعي فما عليك إلا ان تستأذن صديقك دقيقة وتقوم بعمل Restart للجهاز لن يستطيع المخترق في هذه الفترة الزمنية القصيرة بأخذ أي شيء من جهازك او تخريب الجهاز لأنك في وقتها سوف تقوم بعمل Restart اذا شعرت بأي شي غير طبيعي لتجد جهازك عاد نظيفاً كما كان ليقوم بحذف هذا الملف الذي قمت بأستقباله وبفتحه سابقاً عن طريق الخطأ وعلى المخترق أن يقوم بأرسال الملف لك مرة اخرى ووقتها فلن تستقبله. لأنك علمت سابقاً محتوى هذا الملف برنامج قوي قوي قوي وأنصح الجميع بتثبيته الأن.

يأتي لي شخص يسألني انا الأن اريد ان أحفظ ملف في جهازي او اثبت برنامج جديد فكيف احفظ الملف في جهازي اذ قمت بتثبيت برنامج الديب فريز فبمجرد عمل Restart سوف يذهب كل ما قمت بحفظه؟؟؟؟؟.

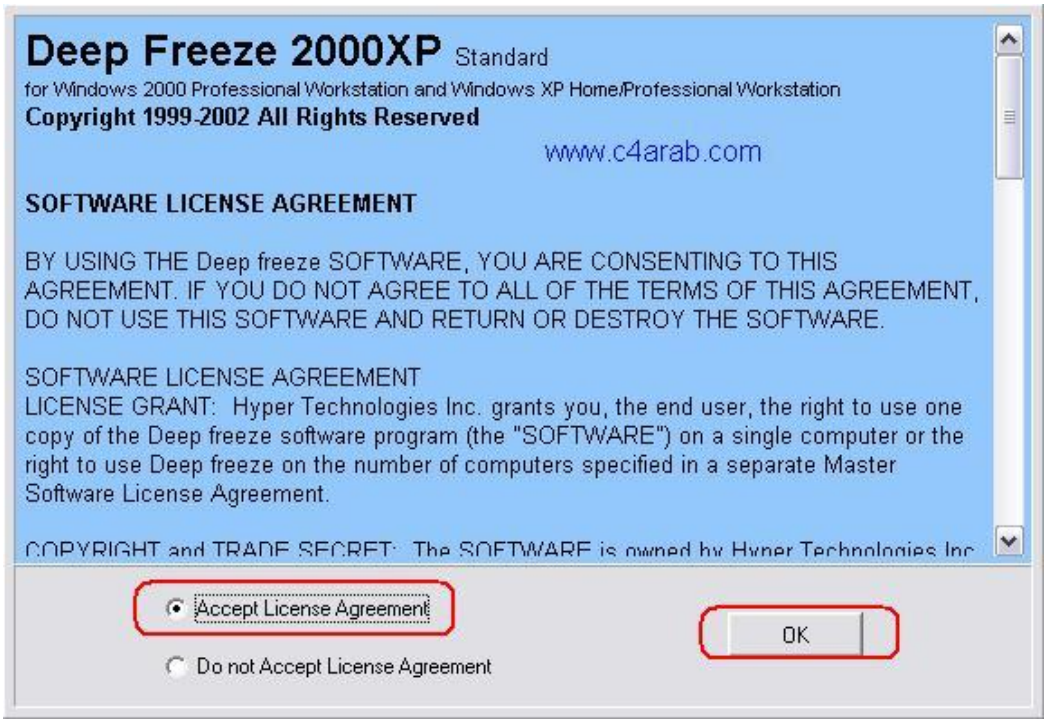
أرد وأقول له ان هذا البرنامج رهيب وله ميزة قوية وهو انك تستطيع عمل Freeze أو تجميد للقرص الصلب الذي تختاره أنت بنفسك , سواء قرص صلب C , Dأو F ولكي تصل الي أقصى درجات الحماية القصوى قم بعمل تجميد للقرص C لأنه القرص الأهم في أقراص الهارد ديسك جميعاً ولأنه يحتوي على ملفات النظام التي من خلالها يستطيع المخترق تخريبها والتحكم في جهازك واستخراج كلمات سر الإيميلات ولأن التروجان او الباكدور او ملف التجسس ينشأ نفسه في ملف System32 في القرص C ويقوم بتشغيل نفسه تلقائياً عند بداية كل تشغيل للنظام , تستطيع حفظ ما تريد من ملفات على D أو F أو E , **ولكن يجب عليك اولاً ان تقوم بتنظيف الجهاز وان تتأكد كل التأكد انه لا يحتوي على اي برامج تجسس او فايروسات قبل ان تقوم بتثبيت البرنامج وعمل تجميل للقرص C** , بعد ذلك قم بتثبيت **deepfreeze** وقم بأختيار تجميد القرص C , يجب ان يكون التجميد للقرص على نظافة وأمان من أي فيروسات أو ملفات تجسس , واذا قمت بفتح ملف تجسس او فايروس لا سمح الله ولم يكتشفه برنامج الحماية وتخطى الجدار الناري ZoneAlarm لديك ايضاً وشعرت ببعض البطء في النظام أو شيء غير إعتيادي فقط كل ما عليك أن تقوم بعمل Restart وقد يستغرق ثانيتين فقط لإعادة التشغيل ولكن في الحقيقة هذه الثانيتين قد قاموا بتأمين جهازك ضد اي أختراق مستهدف, يقوم بتنظيف الجهاز اذ قمت بتحميل فايروس او ملف تجسس بدون قصد او علم فسوف يتم حذفه تلقائياً بمجرد Restart قبل أن ينتشر بالجهاز. وإذا اذا شعرت بأي شيء غير طبيعي بالجهاز فقط قم بعمل Restart للجهاز ليرجع لسابق عهده ولزيادة الأطمئنان , فهذه العملية لا تستغرق ثانيتن على حسب سرعة جهازك صراحتن برنامج أكثر من رائع وقوي جدا وأنصح الجميع بأستعماله وأتباع الخطوات التالية في الشرح وان شاء الله سوف **يكون جهازك في أمن دائم حتى ولو تخطى برامج الحماية والجدار الناري.**

شرح بسيط لطريقة تثبيت البرنامج اخر اصدار:



في النافذه السابقه يظهر لك البرنامج جميع محركات الأقراص لديك ويعطيك الخيار بأنه هل تريد أن يقوم البرنامج بحماية جميع الاقراص C-D-E **في هذه الخطوة أنصح بأختيار الخيار C فقط وأجعل D و E غير مفعلين وذلك لحفظ الملفات التي قمت بتحميلها من الأنترنت مثل أغاني أو مقاطع فيديو على هذه الأقراص** لأن اذا قمت بحفظه على C فعند قيامك بعمل إعادة تشغيل الجهاز فسوف يتم حذف اي شيء قمت بحفظه بالقرص C:> لذلك ينصح بجعل البارتشن E أو D لحفظ الملفات في جهازك من الأنترنت , وفي حالة رغبت في تثبيت برنامج جديد يجب عليك من اغلاق برنامج الديب فريز ليتم تثبيت البرنامج الجديد وسوف اشرح هذه الخطوة بعد عملية تثبيت البرنامج أختر القرص C وتابع شرح تثبيت البرنامج:

بعد أختيار القرص :C والضغط على Install في الصورة السابقة:

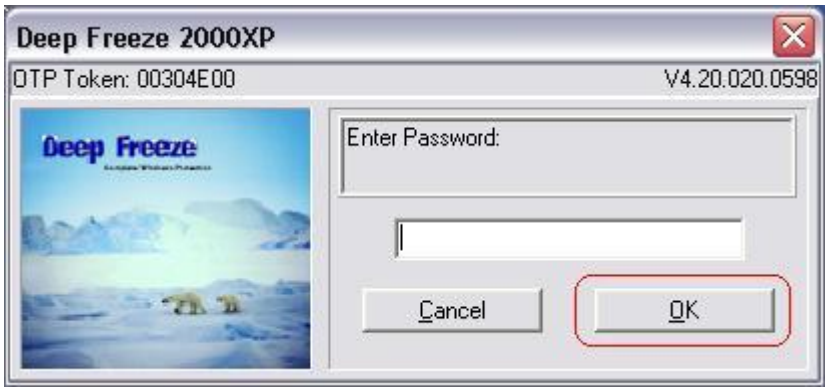



أضغط على OK

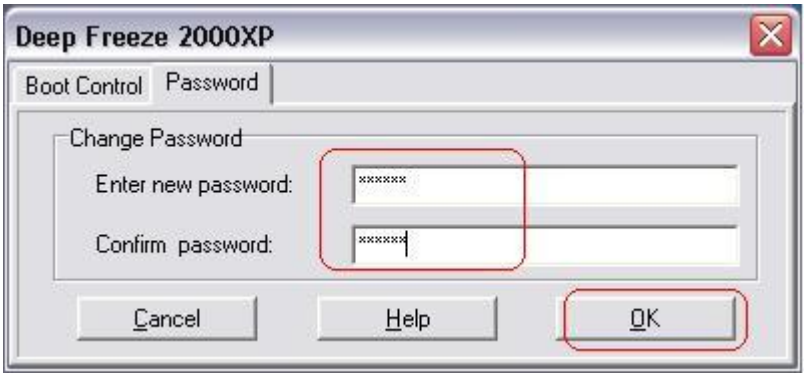


عملية التثبيت جارية وهي تأخذ عدة ثواني بعدها سيتم إعادة تشغيل الكمبيوتر تلقائياً.

بعد تثبيت البرنامج بنجاح ستجد أيقونة البرنامج في شريط الأدوات بجانب ساعه الكمبيوتر أضغط عليها أو قم بالضغط على الأزرار التاليه في الكيبورد ctrl+alt+shift+F6 بيظهر لك التالي:

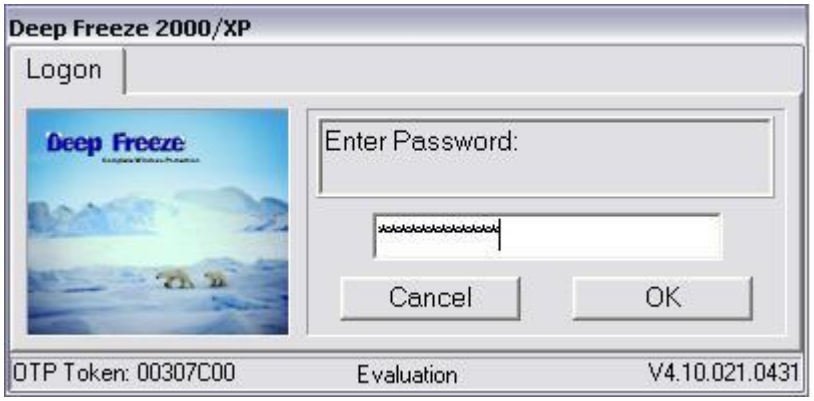




بما اننا لم نقم بوضع كلمة سر للبرنامج فقم بالضغط على Ok

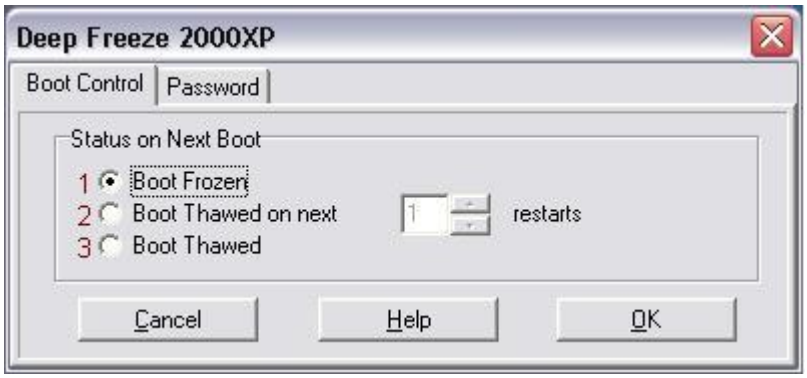



نقوم بإختيار التبويب Password ثم ضع الرقم السري المخصص للبرنامج في الخانتيين:

طريقة عملية إيقاف البرنامج تتم بالشكل التالي:



بعد كتابة كلمة السر والضغط على Ok ستظهر لدينا هذه النافذة:




في النافذة السابقه سنجد أن لدينا في التبويب Boot Control ثلاثة إختيارات:

## الإختيار الأول Boot Frozen

هذا الخيار لعمل تجميد او Freeze للجهاز.

## الإختيار الثاني Boot Thawed on Next

هذا الخيار لتحديد للبرنامج لوقف عملية التجميد بعد عدد معين انت تحددها بنفسك من إعادة تشغيل النظام. "غير مهمة".

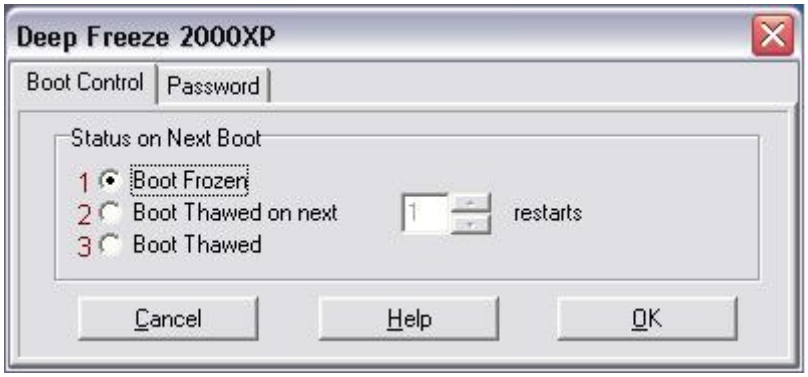
## الإختيار الثالث Boot Thawed

هذا الخيار لوقف عمل البرنامج او الغاء الـ Freeze , في حالة إذا رغبت في تغيير او تثبيت برنامج جديد في الجهاز وينصح بفصح الملف والتأكد من خلوه من اي ملفات تجسسية او فيروسات قبل هذه العملية.

دعونا نختار الاختيار الثالث , نضغط OK لعمليه ايقاف البرنامج , اذ رغبت مثلاً في تثبيت برنامج جديد على النظام كما قلت سابقاً.

قم بإعادة تشغيل الجهاز restart وستجد أن أيقونه البرنامج تغيرت في شريط الأدوات وقد تحولت إلى الشكل التالي:

بعد أن تنتهي من عمل التغييرات التي تريدها في جهازك قم بفتح البرنامج ثم إختيار الخيار الأول لعمل freeze او لتفعيل عمل البرنامج وتجميد القرص C ولحمايته من العبث بعد التغييرات التي قمت بها في الجهاز من هذا الأختيار وهو الخيار الأولBoot Frozen:




ثم قم بعمل إعادة تشغيل للجهاز حتى يكون شكل ايقونة البرنامج بهذا الشكل:


وبذلك تقوم قد ضمنت جهازك من العبث والتخريب وملفات التجسس والفايروسات التي قد تصيب جهازك , **حتى واذا قمت بفتح ملف تجسس او فايروس لا سمح الله من اي شخص كان بدون قصد او بقصد في جهازك او قمت بتحميل ملف او فايروس من موقع مشبوه وكان ملف تنفيذي "داونلودر" فايروس , واذا تخطى الملف التجسسي هذا او الفايروس برنامج الحماية او الجدار الناري , فيكون الديب فريز بمصد ثالث للمخترق ويعيق عملية الأختراق عليه ويحذف الملف التنفيذي التجسسي من الجهاز نهائياً , يستطيع هذا البرنامج حذف كل هذه الملفات التخريبية بمجرد إعادة تشغيل الجهاز** , برنامج رائع ولا غنى عنه , لإن ملف التجسس او الفايروس يتم زرعه بملف system32 وهذا الملف موجود بالقرص C ثم تقوم بالأنتشار الي بقية الأقراص الصلبة اذا لم تقم بحذفها في الوقت المناسب , وقرص C هو أهم قرص بالجهاز , وهوالذي يجب حمايته من العبث والفيروسات وبرامج التجسس هذه , لذلك ينصح بظبط اعدادت البرنامج على القرص C وقد قلت سابقاً انه عند تثبيت البرنامج تقوم بأختيار هذا القرص C في برنامج deepfreeze ليقوم بتجميده وحمايته من التخريب , وبالطبع بعد أن تتأكد من خلو الجهاز من اي فيروسات او ملفات تجسس او عبث بملفات النظام الأصلى قبل عملية التثبيت , حتى اذا حدث اي شيء غير اعتيادي او شعرت بشيء غير طبيعي في الجهاز , فكل ما عليك هو ان تقوم بعمل Restart لتجد جهازك عاد كما كان في سابق عهده , نظيفاً وجديداً!!! كما تركته لا يوجد ملفات تجسس او فيروسات.

# 7- المراجع

شكر خاص

منتديات الحاسب في حياتنا
http://www.pcintv.com

منتديات العاصفة
http://www.3asfh.net

الموسوعة العربية للكمبيوتر والأنترنت
http://www.c4arab.com

منتديات المعرفة
http://www.almarefa.net

ويكيبيديا الموسوعة الحُرة
http://ar.wikipedia.org/wiki

منتديات المشاغب
http://www.absba.com

شبكة مكتوب
http://www.maktoob.com

توب تن ريفيو
http://www.toptenreviews.com

# تم بحمدالله

إعداد وتقديم:\\ عزالدين إبراهيم
جمهورية مصر العربية
Ezz313[at]gmail[dot]com