امآن الحاسوب وتراخيص البرامج

اخلاق العالم الالكتروني (السلوكيات المهذبة عند استخدام الانترنت)

العالم الالكتروني اخلاق تكاد تكون تشبه العالم التقليدي، فضلاً عن بعض الاداب التي يتطلبها هذا العالم الجديد، وينبغي الالتزام بمجموعة من الاخلاق والاداب العامة عند استخدام الانترنيت، ومن اهمها:

1. احترام الطرف الاخر.
2. الالتزام بعدم الاضرار بالاخرين.
3. الايجاز في طرح الافكار ومحاورة الاخرين.
4. الالتزام بالقانون.
5. احترام الخصوصية الشخصية للاخرين.

تذكر دائماً أن الإنترنت وسيلة للاتصال، إذ يمكنك عن طريقها إرسال الرسائل ومحاورة الآخرين وعرض أفكارك وآرائك والاطلاع على أفكار الآخرين آرائهم، فهي وسيلة للتفاعل والتعامل بين الأشخاص والمؤسسات والهيئات المختلفة، وعند استخدام أي وسيلة اتصال، ينبغي الالتزام بمجموعة من الأخلاق والآداب العامة، ومن هذا المنطلق، جاء مفهوم آداب الإنترنت Netiquette المشتق من التعبير الانجليزي net Etiquette، أي السلوكيات المهذبة عند استخدام الإنترنت، ومفهوم أخلاق الإنترنت.

اشكال التجاوزات في العالم الرقمي

هي مخالفات قانونية في عالم الانترنيت والحاسوب، التي تصدر من المستخدمين لغرض الوصول الى اهداف تخالف القانون والخلق العام والتجاوزات عل خصوصية الغير، وتشمل:

- جرائم الملكية الفكرية: تشمل نسخ البرامج بطريقة غير قانونية، وسرقة البرامج التطبيقية، سواء اكانت تجارية او علمية او عسكرية، لان هذه البرامج تمثل جهود تراكمية من البحث.

- الاحتيال: احتيال التسويق، سرقة الهوية الاحتيال على البنوك والاحتيال عن طريق الاتصالات وسرقة الارصدة وسرقة المال من خلال التحويل الالكتروني من البنوك والاسهم.
- سرقة البيانات الخاصة والتشهير بالاخرين وابتزازهم.

امن الحاسوب هي عملية منع واكتشاف استعمال الحاسوب لاي شخص غير مسمح له (مخترق). وهي اجراءات تساعد على منع المستخدمين غير المسموح لهم بالدخول للحاسوب واستعمال ملفاته.

خصوصية الحاسوب

يُستخدم مصطلح خصوصية الحاسوب ليشير إلى الحق القانوني في الحفاظ على خصوصية البيانات المخزنة على الحاسوب أو الملفات المتشاركة.

تظهر حساسية مسألة خصوصية الحاسوب أو البيانات خاصة عندما يتعلق الأمر ببيانات التعريف الشخصية المخزنة والمحفوظة في أي جهاز رقمي (سواءً كان حاسوباً أو غيره). عدم القدرة على التحكم بإخفاء هذه البيانات هو ما يؤدي إلى تهديد خصوصية البيانات في الغالب. أما أكثر المشاكل التي تكون محور خصوصية البيانات فهي:

- المعلومات الصحية
- السجل العدلي
- المعلومات المالية
- معلومات الموقع والسكن
- وفي بعض الأحيان معلومات عن الجنس أو العِرق أو الدين.
- معلومات عن البيانات السرية بشتى أنواعها

تراخيص برامج الحاسوب

رخصة أو ترخيص البرمجيات (بالإنجليزية: Software license): هي وثيقة قانونية تحكم استعمال أو إعادة توزيع البرمجيات المحمية بحقوق النسخ.

لماذا من المهم معرفة رخصة البرنامج أو التطبيق قبل استخدامه؟

1. حتى لا ننتهك القوانين ونسلب حقوق الآخرين.
2. ليزداد وعينا وفهمنا في مسألة إختيار التطبيقات المناسبة لنا.
3. حتى نتجنب بعض الأخطار المحتملة على خصوصية بياناتنا من استخدام بعض الأنواع من البرمجيات.

ما هي أنواع الرخص؟

رخص البرمجيات هي كالتالي:

برمجيات مجانية (Freeware): يمكن استخدامها لفترة غير محدودة من الزمن وبلا تكلفة، بعض برمجيات المجانية تكون مسموحة فقط للإستخدام الشخصي وليس للإستخدام التجاري أو للإستخدام داخل مؤسسة أو شركة ما، مثل مكافح الفيروسات المجانيAvira AntiVir Personal .

برمجيات مفتوحة المصدر(Open Source): قد تعمل تحت رخصة جنو العمومية GNU General Public License أو رخصة غيرها تمنح المستخدم إمكانية الإطلاع على شفرتها المصدرية (أو الشفرة البرمجية) للدراسة أو للتغيير أو للتطوير، والكثير من برمجيات المفتوحة المصدر مجانية ولكن ليست كلها.

برمجيات تجريبية غير مجانية (Trial): تعمل لفترة معينة من الزمن أو لعدد معين من مرات الإستخدام، وبعد إنتهاء الفترة التجريبية قد تتوقف عن العمل وتطالب المستخدم بشراء رخصة الإستخدام، عادةً تمتد فترة التجربة من 15 يوما إلى 90 يوم.

برمجيات تجريبية غير مجانية (Demo): مشابهة للبرمجيات التي تعمل بنوع الترخيص Trial أي أنها تعمل لفترة معينة ولكن تختلف عنها بأنها تعمل فقط بوظائف محدودة وتضع قيودا على استخدامها، ولا تعمل بكافة وظائفها إلا بعد شراء رخصة الإستخدام.

Adware: برمجيات دعائية، قد تقوم بالعديد من الأمور المزعجة، مثل: عرض إعلانات، تغيير صفحة البداية في المتصفح، تغيير محرك البحث الإفتراضي في المتصفح، فتح صفحات ويب عند تشغيل أو إغلاق الحاسوب، وتشكل خطورة على خصوصية المستخدم، ويعتبر Messenger Plus! Live الشائع الإستخدام من برمجيات الـ Adware.

ملاحظة ننصح ابنائنا الطلبة بعدم اقتناء وتنصيب نسخ البرامجيات غي الاصلية والتي تباع بالاسواق

- هذا العمل يتنافى مع الشريعة السماوية التي حرمت سرقة جهد الغير وتسويق منتجاتهم بدون علمهم .
- اغلب هذه البرامج عادتا ما تحمل فايروسات او برامج التجسس والقرصنة.

البديل

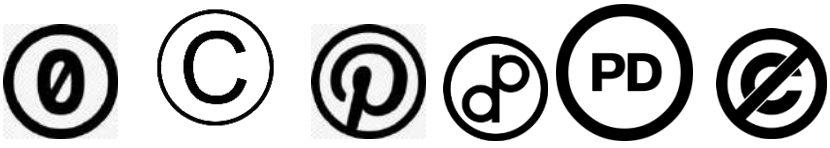
- البحث عن مراكز التسويق لهذه البرمجيات داخل العراق.
- التحول للبرمجيات ونظم التشغيل المفتوحة والامنية.

الملكية الفكرية

هي اتفاقية قانونية تكون موثقة في دوائر عدلية مثل المكتبات العامة او الدوائر الملكية الفكرية(حالها حال الملكية للاراضي او السيارات او الاموال)، مجموعة من الحقوق التي تحمي الفكر الانساني وتشمل براءات الاختراع والعلامات التجارية والرسوم والنماذج الصناعية وحق المؤلف وغيرها.

حقوق النسخ والتأليف(COPY RIGHT)

مجموعة من الحقوق الحصرية التي تنظم استعمال النصوص واستخدام عمل ابداعي جديد. تشكل هذه الحقوق نوع من الحماية للمبدع ليتقاضى اجرا عن ابداعه لفترة محددة تختلف حسب البلد والاتفاقية. الاعمال التي تنتهي مدة حمايتها تدخل ضمن الملكية العامة تصبح بمتناول الجميع.



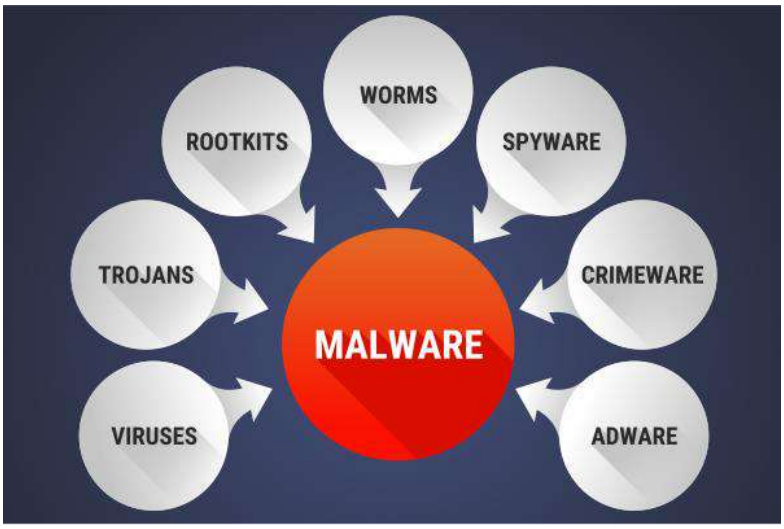
الاختراق الالكتروني

قيام شخص غير مخول او اكثر بمحاولة الدخول (الوصول) الكترونياً الى الحاسوب او الشبكة عن طريق الانترنيت بغرض الاطلاع والسرقة، التخريب، التعطيل باستخدام برامج متخصصة.

المخاطر الامنية الاكثر انتشاراً

1. الفايروسات
2. ملفات التجسس(Spywares): هي برامج مصصمة لجمع المعلومات الشخصية مثل المواقع الالكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الالكترونية، وغيرها
3. ملفات دعائية(Adware): هي برامج مصممة للدعاية والاعلان وتغير اعدادات العامة للحاسوب.
4. قلة الخبرة في التعامل مع بعض البرامج.
5. اخطاء عامة

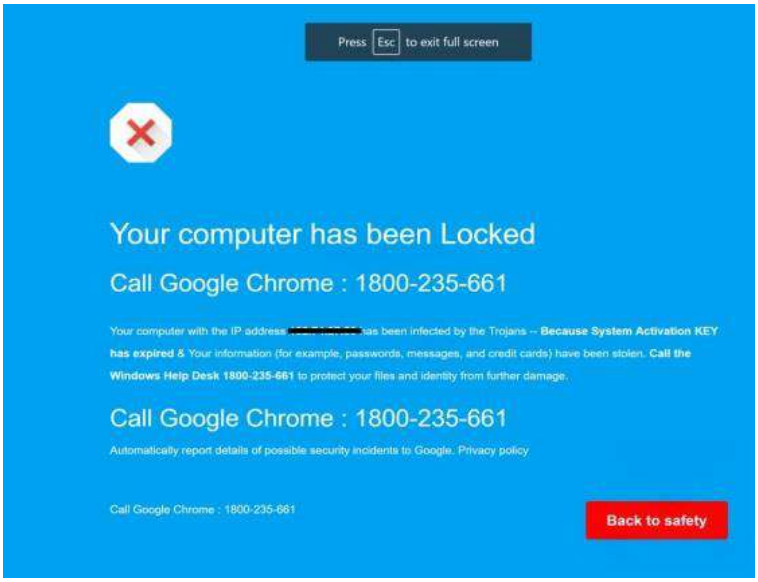
برامجيات خبيثة: اختصار لكلمتين(Malicious Software) هي برامج مخصصة للتسلل لنظام الحاسوب او تدميره بدون علم المستخدم

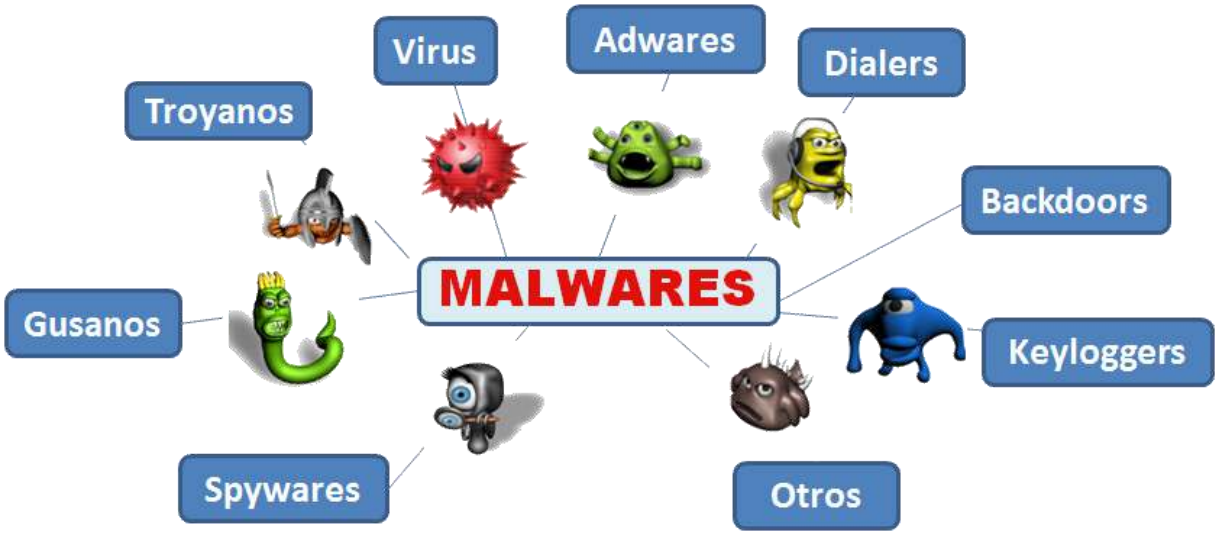


فايروسات الحاسوب: برامج صغيرة خارجية صممت عمداً لتغيير خصائص الملفات التي تقوم ببعض الاوامر التنفيذية اما بالحذف اوالتعديل او التخريب وفقاً لاهدف صممت لاجلها، ولها القدرة على التخفي، ويتم خزنها باحدى الطرق لالحاق الاذى به والسيطرة عليه.

الاضرار الناتجة عن فايروسات الحاسوب

1. تقليل مستوى اداء الحاسوب.
2. ايقاف تشغيل الحاسوب واعادة تشغيل نفسه تلقائيا كل بضع دقائق او اخفاقه في العمل بعد ايقاف العمل بعد اعادة التشغيل.
3. تعذر الوصول الى مشغلات الاقراص الصلبة والمدمجة (وحدات الخزن) وظهور رسالة تعذر الحفظ لوحدات الخزن.
4. حذف الملفات وتغيير محتوياتها.
5. ظهور مشاكل في التطبيقات المنصبة وتغيير النوافذ التطبيقات والقوائم والبيانات.
6. تكرار ظهور رسائل الخطأ في اكثر من تطبيق.
7. افشاء معلومات وأسرار شخصية هامة.


Press Esc to exit full screen
Your computer has been Locked
Call Google Chrome : 1800-235-661
Your computer with the IP address [redacted] has been infected by the Trojans -- Because System Activation KEY has expired & Your information (for example, passwords, messages, and credit cards) have been stolen. Call the Windows Help Desk 1800-235-661 to protect your files and identity from further damage.
Call Google Chrome : 1800-235-661
Automatically report details of possible security incidents to Google. Privacy policy
Call Google Chrome : 1800-235-661
Back to safety


Virus
Adwares
Dialers
Troyanos
Backdoors
MALWARES
Gusanos
Keyloggers
Spywares
Otros

صفات فايروسات الحاسوب

- القدرة على التناسخ والانتشار.
- ربط نفسها ببرنامج اخر يسمى الحاضن (المضيف Host)
- يمكن ان تنتقل من حاسوب مصاب لاخر سليم.

مكونات الفايروسات

- الية التناسخ تسمح للفايروس ان ينسخ نفسه.
- الية التخفي تخفي الفايروس عن الاكتشاف.
- الية التنشيط تسمح للفايروس بالانتشار.
- الية التنفيذ تنفيذ الفايروس عند تنشيطه.

انواع الفايروسات

1. الفيروسات Virus : برنامج تنفيذي.ذات الامتداد scr. , pif., bat. , exe. , com. وتتراوح خطورته حسب المهمة المصممة لاجلها فمنها البسيطة ومنها الخطيرة، يعمل بشكل منفصل ويهدف الى احداث خلل في الحاسوب، ينتقل بواسطة نسخ الملفات من حاسوب يحوي ملفات مصابة الى اخر عن طريق الاقراص المدمجة (CD) والذاكرة المتحركة(Flash Memory) .
2. حصان طروادة: فايروس تكون الية عمله مرفقاً مع احد البرامج المفيدة وغرضه الاساسي جمع المعلومات مثل اسمك وكلمة السر ثم يبعث بهذه المعلومات لصاحبة وانت متصل بالشبكة والاسوء من ذلك انه يسمح للهاكر بتصفح جهازك او يتحكم بملفاتك تحكم كاملا، سمي هذا البرنامج بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة، اذ أختبأ الجنود اليونان واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.
3. الفيروسات فئة الديدان Computer Worms تنتشر فقط عبر الشبكات والانترنت مستفيدة من عناوين البريد الالكتروني، فعند إصابة الحاسوب يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في قائمة العناوين ويرسل نفسه الى كل الاشخاص في القائمة، مما يؤدي الى انتشاره وبسرعة عبر الشبكة

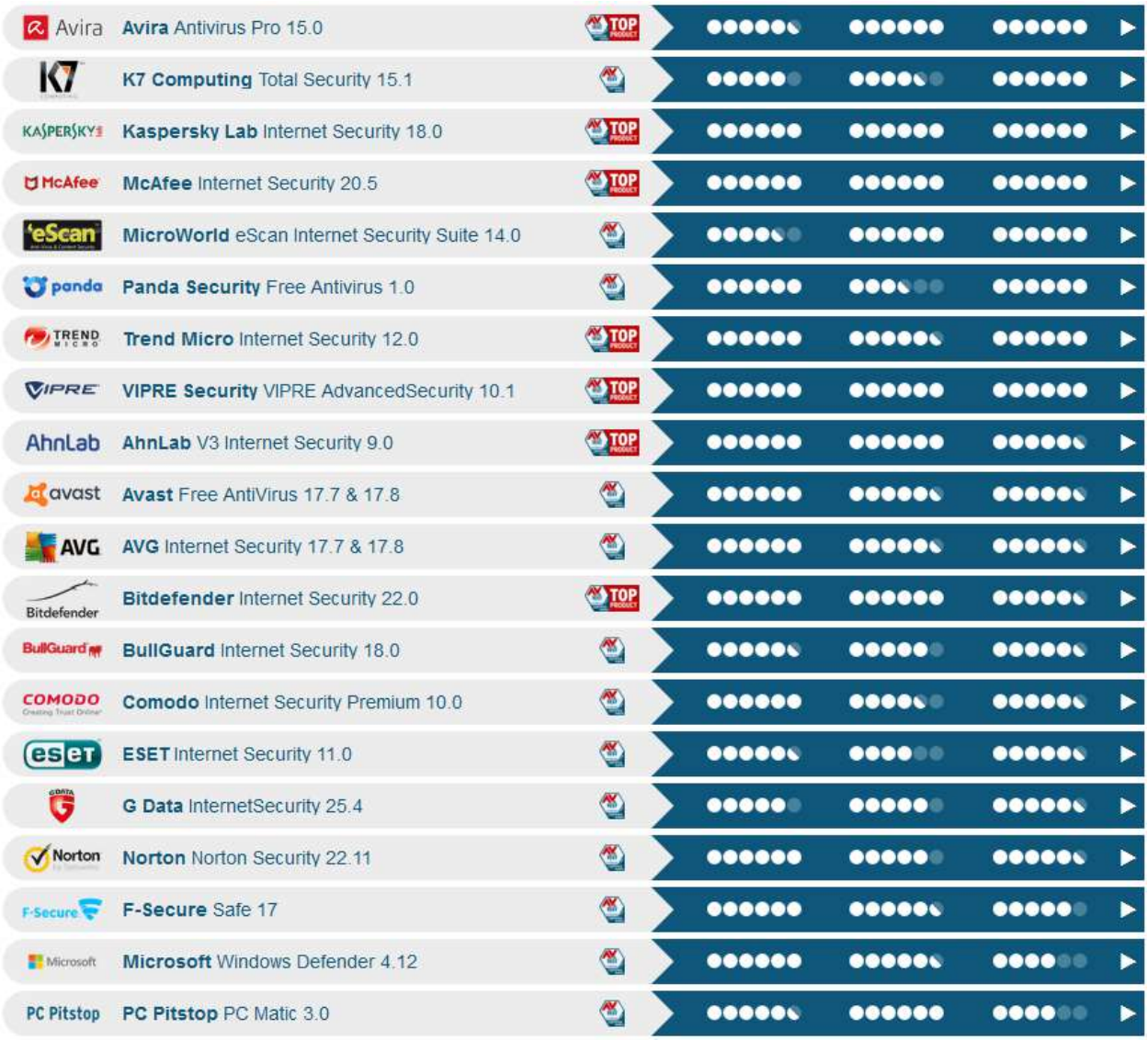
اهم الخطوات اللازمة للحماية من عمليات الاختراق

الحفاظ على جهاز الحاسوب ضد هذه الملفات بشكل كامل صعب جداً مادام الجهاز مربوط بشبكة الانترنت، لكن يمكن حماية الحاسوب بنسبة كبيرة وتقليل خطر الاصابة بالاختراقات الالكترونية والبرامج الضارة بأتباع الخطوات الاتية:

1. استخدام نظم تشغيل محمية من الفايروسات كنظم التشغيل يونكس ولينكس ومشتقاتها

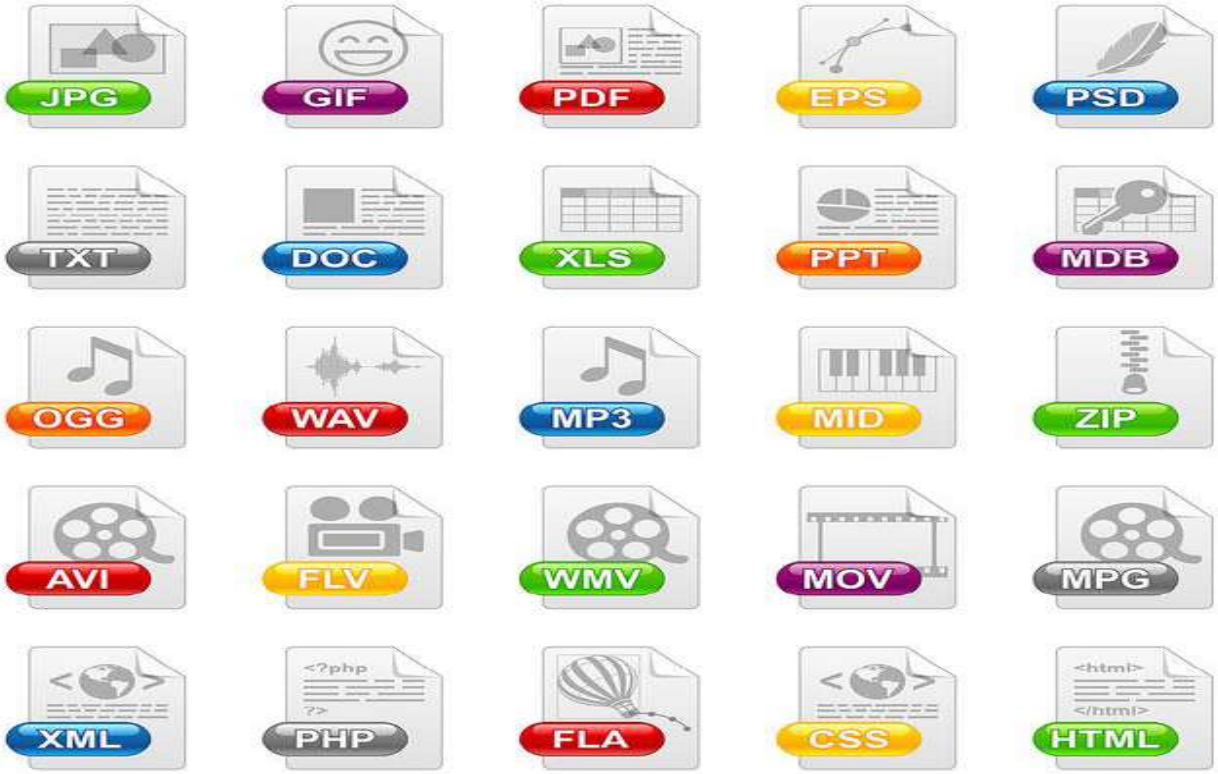
تم بناء هذه النظم بحيث لايمكن ان يدخل اليها اي برنامج خارجي الا بموافقة وعلم المستخدم بشكل واضح وصريح، كما ان ملفات النظام الاساسية تكون محمية من اي تلاعب او تغير حتى عن طريق الخطأ غير المتعمد.

2. تثبيت البرامج المضادة او المكافحة للفايروسات (Antivirus) وبرامج مكافحة ملفات التجسس (Antispyware) ذات الاصدارات الحديثة وتحديث النسخة.



The title of best antivirus 2018-2019 (No doubt, Bitdefender & Kaspersky has continued win)

3. الاحتفاظ بنسخ للبرمجيات المهمة مثل نظام تشغيل الويندوز وحزمة اوفيس ونسخة من ملفات المستخدم.
4. عدم فتح اي رسالة او ملف ملحق ببريد الكتروني وارد من شخص غير معروف للمستخدم او الملفات ذات الامتدادات غير المعروفة.



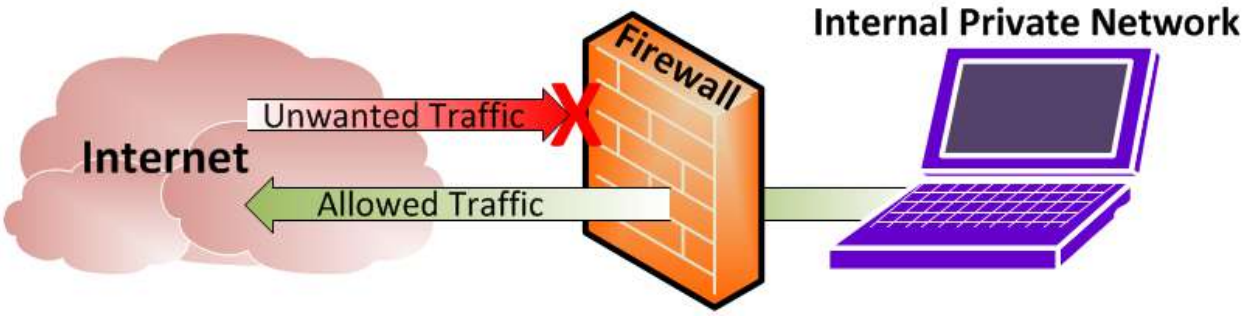
امتداد الملف (بالإنجليزية: extension) هو لاحقة تلحق اسم ملف حاسوب لتوضيح تكويد أوترميز محتويات الملف (صيغة الملف).

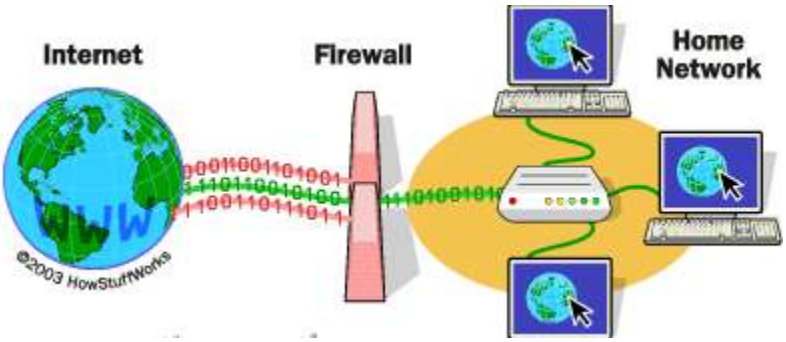
5. تثبيت كلمة السر (Password) على الحاسوب والشبكة اللاسلكية الخاصة بالمستخدم مع تغيرها كل فترة، وعدم السماح إلا للمستخدمين الموثوقين بالاتصال واستخدام الحاسوب

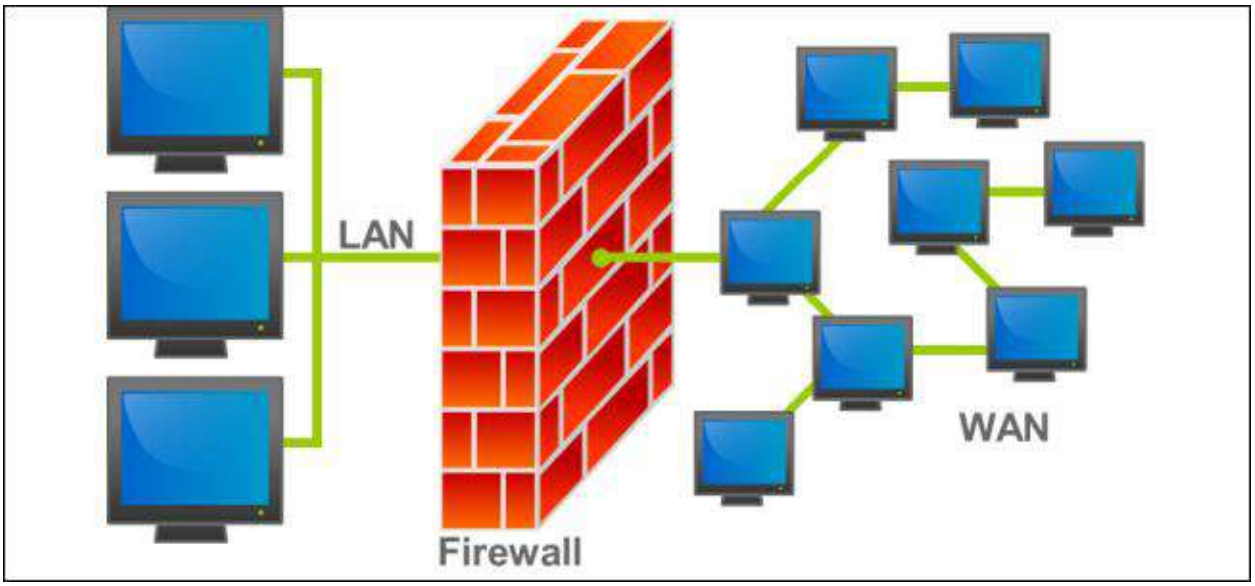
6. عدم الاحتفاظ بأي معلومات شخصية في داخل الحاسوب كـ(الرسائل الخاصة، الصور الفوتوغرافية، الملفات المهمة، والمعلومات المهمة مثل اقام الحسابات او البطاقات الائتمانية)، وخزنها في وسائط تخزين الخارجية.

7. عدم تشغيل برامجيات الالعاب على نفس الحاسوب الذي يحتوي البيانات والبرمجيات المهمة، لانها تعد من اكثر البرامجيات تداولا بين الاشخاص والتي تصاب بالفايروسات.
8. ايقاف خاصية مشاركة الملفات إلا عند الضرورة وعمل نسخ احتياطية من الملفات المهمة والضرورية.

9. ثقافة المستخدم وذلك من خلال التعرف على الفايروسات وطرق انتشارها، وكيفية الحماية منها، والاثار المترتبة حال الاصابة بها. من خلال التواصل المستم بزيارة المواقع التي تهتم بالحماية من الفايروسات.
10. فك الارتباط بين الحاسوب والموديم او الخط الهاتفي عند الانتهاء من العمل، فذلك يمنع البرامج الخبيثة التي تحاول الدخول الى الحاسوب.
11. تفعيل عمل الجدار الناري(Firewall) يقوم الجدار الناري بتفحص المعلومات الواردة من الانترنت والصادرة اليه، ويتعرف على المعلومات الواردة من المواقع الخطرة او تلك التي تثير الشك فيعمل على ايقافها. فما عليك الان تقم بأعداد جدار الحماية بالشكل الصحيح لكي لايتمكن المتطفلون من الدخول والاطلاع الاجهزة الحاصة بك.



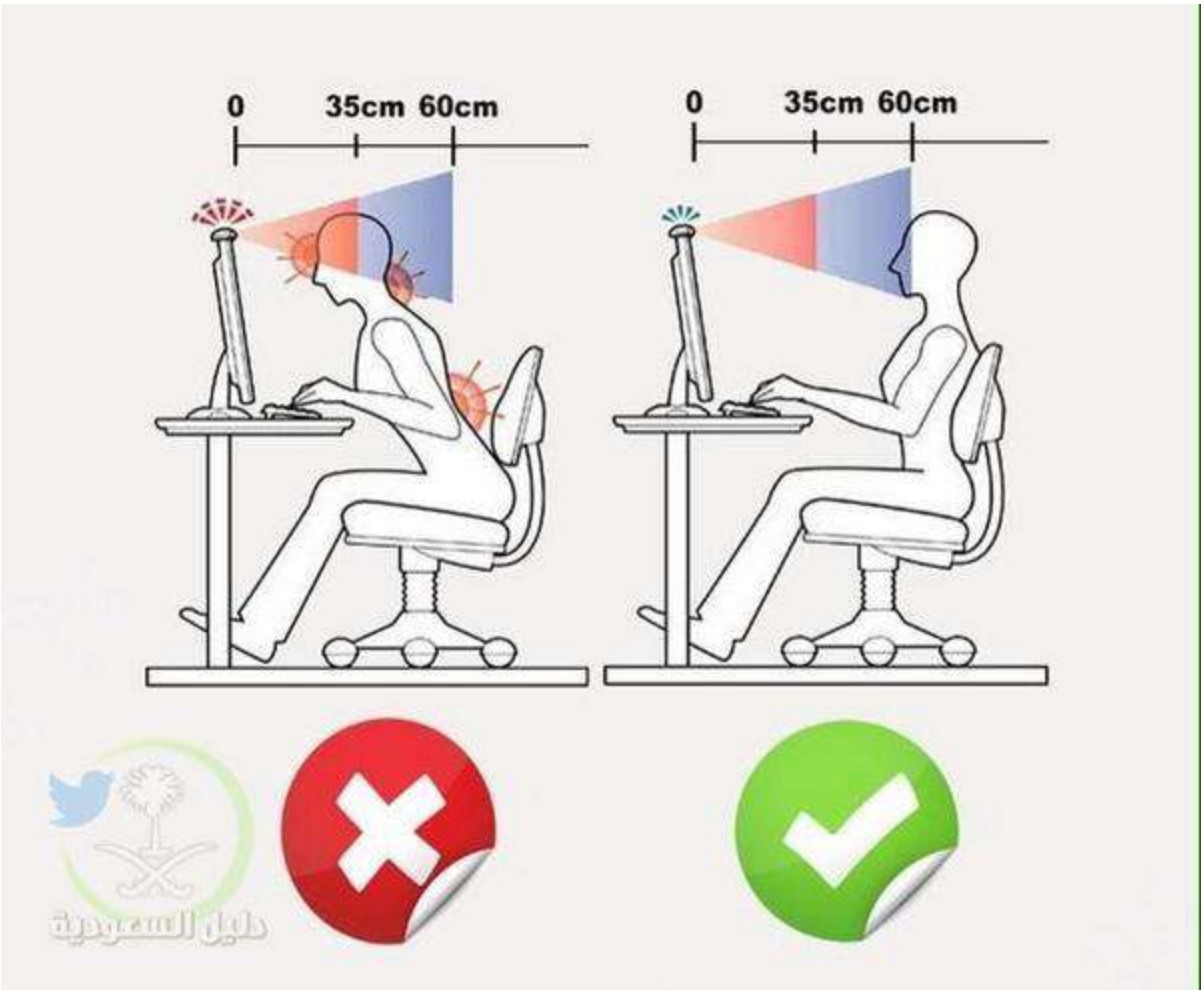




اضرار الحاسوب على الصحة

يعد استعمال الحاسوب ضرورة لغالبية الأفراد ولكن قليلًا من يراعي فعلياً الاعتبارات الطبية التي يمكن أن يتسبب فيها التعامل مع الحاسوب؛ مثل ضعف البصر والأمراض الناتجة عن وضع الجسم السيء والتهاب مفاصل الأصابع وإصابات ضغط الكمبيوتر التي يمكن أن تنتج بسبب الجلوس في وضع واحد لمدة زمنية مطولة.

م. رشا عبد الحسين علي النعيمي



تمرين التمطط نحو الأعلى

تمرين عطف القدم وبسطها

تمرين تدوير الكتف

تمرين التمطط الجانبي

تمرين حني الظهر

تمرين مد الساق وعطف القدم وبسطها

تمرين رفع الساق