## مصادر الاختراق الالكتروني:

1- **مصادر متعمدة:** ويكون مصدرها جهات خارجية تحاول الدخول الى الجهاز بصورة غير مشروعة. ومن الامثلة على المصادر المتعمدة للاختراق الالكتروني:
- المحترفون والهواة لغرض التجسس دون الاضرار بالحاسوب.
- اختراق شبكات الاتصال والاجهزة الخاصة بالاتصال للتنصت او الاتصال المجاني.
- اختراق لنشر برنامج معين او لكسر برنامج او لفك شفرتها المصدرية (Crackers).
- اعداء خارجيون وجهات منافسة.
- مجرمون محترفون في مجال الحاسوب والانترنت.

2- **مصادر غير متعمدة:** وهي تنشأ بسب ثغرات موجودة في برامجيات الحاسوب والتي قد تؤدي الى تعريض الجهاز الى نفس المشاكل التي تنتج عن الاخطار المتعمدة.

## المخاطر الامنية الاكثر انتشارا:

a- **الفيروسات (Viruses):** وهي برامج مصممة للانتقال الى اجهزة الحاسوب بطرق عدة وبدون اذن المستخدم وتؤدي الى تخريب وتعطيل عمل الحاسوب او اتلاف البيانات والملفات.ولها القدرة على التخفي ويتم خزنها داخل الحاسوب باحدى طرق الانتقال لالحاق الضرر به والسيطرة عليه.

b- **ملفات التجسس:** هي برامج مصممه لجمع المعلومات الشخصية مثل المواقع الالكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الالكترونية.

c- **ملفات دعائية :** وهي ملفات مصممة للدعاية والاعلان وتغيير الاعدادات العامة في اجهزة الحاسوب.

d- **قلة الخبرة في التعامل مع بعض البرامج:** مع ازدياد استخدام الانترنت من عامة الناس غير المتخصصين واستخدامهم وتعاملهم مع برامجيات متطورة وبدون خبرة كافية قد يفتح ثغرة في جهاز الحاسوب تمكن الاخرين من اختراق الجهاز.

e- **اخطاء عامة:** مثل سوء اختيار كلمة السر او كتابتها على ورقة مما يمكن الاخرين من قراءتها او ترك الحاسوب مفتوح مما يسمح للاخرين بالدخول لملفات الحاسوب او تغيير بعض الاعدادات.

## برامجيات خبيثة Malware :

هي اختصار لكلمتين Malicious software وهي برامج مخصصة للتسلل لنظام الحاسوب او تدميره دون علم المستخدم. وما ان يتم تثبيت البرمجية الخبيثة فأنه من الصعب ازالتها. وبحسب درجة البرمجية من الممكن ان يتراوح ضررها من ازعاج بسيط الى اذى غير قابل للاصلاحيتطلب اعادة تهيئة القرص الصلب.

من الامثلة على البرامجيات الخبيثة هي الفيروسات وحصان طروادة.

## الاضرار الناتجة عن فيروسات الحاسوب:

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

## صفات فايروسات الحاسوب:

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

## مكونات الفيروس:

**يتكون الفيروس بشكل عام من اربعة اجزاء رئيسية تقوم بالاتي:**

1- الية التناسخ: تسمح للفيروس بنسخ نفسه.
2- الية التخفي: تخفي الفيروس عن الاكتشاف.
3- الية التنشيط: تسمح للفيروس بالانتشار.
4- الية التنفيذ: تنفيذ الفايروس عند تنشيطه.

## انواع الفايروسات:

**تقسم الفايروسات الى ثلاثة انواع:**

1- **الفايروس (Virus)** برنامج تنفيذي (ذات الامتداد com, exe, bat, pif, scr) يعمل بشكل منفصل ويهدف الى احداث خلل في الحاسوب وينتقل بواسطة نسخ الملفات من حاسوب يحوي ملفات مصابة الى حاسوب اخر عن طريق الاقراص المدمجة (CD) والذاكرة المتحركة (Flash Memory).
2- **الدودة (Worm):** تنتشر فقط عبر الشبكات والانترنت مستفيدة من قائمة عناوين البريد الالكتروني ( مثل تطبيق برنامج التحدث الماسنجر Messenger).
3- **حصان طروادة (Trojan Horse):** فايروس تكون الية عمله ملحقا مع احد البرامج اي يكون جزءا من برنامج دون ان يعلم المستخدم. سمي هذا البرنامج بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة اذ اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.

## أهم الخطوات اللازمة للحماية من عمليات الاختراق:

الحفاظ على جهاز الحاسوب من هذه الملفات بشكل كامل صعب جدا ما دام الجهاز مربوط بشبكة الانترنت. ولكن يمكن حماية الحاسوب بشكل كبير وتقليل خطر الاصابة بالاختراقات الالكترونية والبرامج الضارة بأتباع الخطوات التالية:

1- استخدام نظم تشغيل محمية من الفيروسات كنظم يونكس ولينكس ومشتقاتها. تم بناء هذه النظم بحيث لايمكن ان يدخل اليها اي برنامج خارجي الا بموافقة المستخدم.
2- تثبيت البرامج المضادة او المكافحة للفيروسات (Antivirus) مثل Norton, Avira, Kaspersky (McAfee).

3- الاحتفاظ بنسخ للبرامجيات المهمه مثل نظام التشغيل ويندوز وحزمة الاوفيس ونسخة من ملفات المستخدم.
4- عدم فتح اي رسالة او ملف ملحق بريد الكتروني من شخص غير معروف.
5- تثبيت كلمة سر Password على الحاسوب.
6- عدم الاحتفاظ بأية معلومات شخصية في داخل الحاسوب ( الرسائل الخاصة، الصور، الملفات المهمه، والمعلومات المهمه مثل ارقام الحسابات او البطاقات الائتمانية).
7- عدم تشغيل برامجيات الالعاب على نفس الحاسوب الذي يحتوي البيانات والبرامجيات المهمه.
8- ايقاف خاصية مشاركة الملفات الا للضرورة.
9- ثقافة المستخدم وذلك من خلال التعرف على الفيروسات وطرق انتشارها وكيفية الحماية منها.
10- فك الارتباط بين الحاسوب والموديم (Modem) او الخط الهاتفي عند الانتهاء من العمل.
11- تفعيل عمل الجدار الناري بتفحص المعلومات الواردة من الانترنت والصادرة اليه.

## ***اضرار الحاسوب على الصحة:***

الجلوس لفترات طويله امام الحاسوب، الجلوس الخاطئ امام شاشة الحاسوب، والتعرض للاشعة الصادرة من هذه الشاشة الذي يؤثر في العين والابصار والبشرة والجلد. وافضل وقاية منه هو التاكد من صحة الجلو س امام الحاسوب مع الحفاظ على وضع الشاشة بشكل مناسب.

- اثار بدنية ونفسية قصيرة المدى: وتشمل توتر واجهاد عضلات العين والقلق النفسي.
- اثار بدنية ونفسية بعيدة المدى التي تأخذ فترة اطول لظهورها مثل الام العضلات والمفاصل والعمود الفقري وحالة من الارق والقلق النفسي والانفصال النفسي والاجتماعي عن عالم الواقع والعيش وسط افتراضي والعلاقات الخيالية لمن يدمنون الانترنت. وافضل وقاية لذلك هو التوقف من حين لاخر عن العمل بالحاسوب وبسط الساقين والقيام ببعض التمارين الرياضية الخفيفة لتسريع جريان الدم وتحديد ساعات العمل بالحاسوب في الليل.