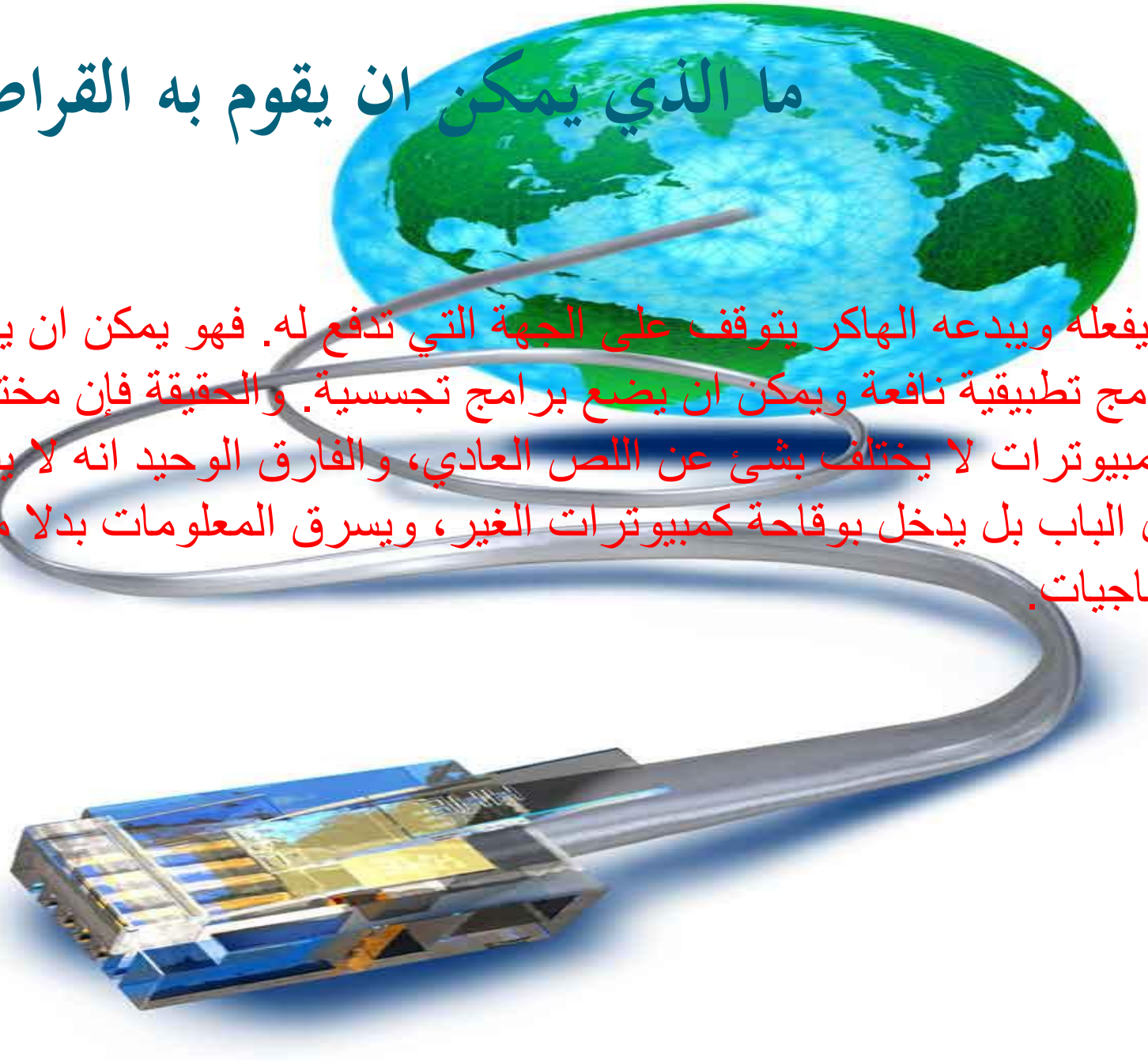
الفصـــل الأول : مشـــروع حاســوب

..الأمـــــن الالـــــــكتروني..

الأمن الإلكتروني

تقوم الاجهزة الامنية لمختلف البلدان بالبحث عن العباقرة في مجال الحاسوب بهدف الصراع ضد الارهابيين والمجرمين. حتى ان ممثلي اجهزة الامن في الولايات المتحدة الامريكية شاركوا خلال الصيف الماضي باجتماع دولي لقراصنة الانترنيت في مدينة لاس فيغاس. ان التهديد باستخدام الشبكة العنكبوتية اصبح اكثر فاكثر امرا واقعيا.

ما الذي يمكن ان يقوم به القراصنة؟



- ما يفعله ويبدعه الهاكر يتوقف على الجهة التي تدفع له. فهو يمكن ان يضع برامج تطبيقية نافعة ويمكن ان يضع برامج تجسسية. والحقيقة فإن مخترق الكمبيوترات لا يختلف بشئ عن اللص العادي، والفارق الوحيد انه لا يفتح قفل الباب بل يدخل بوقاحة كمبيوترات الغير، ويسرق المعلومات بدلا من الحاجيات.

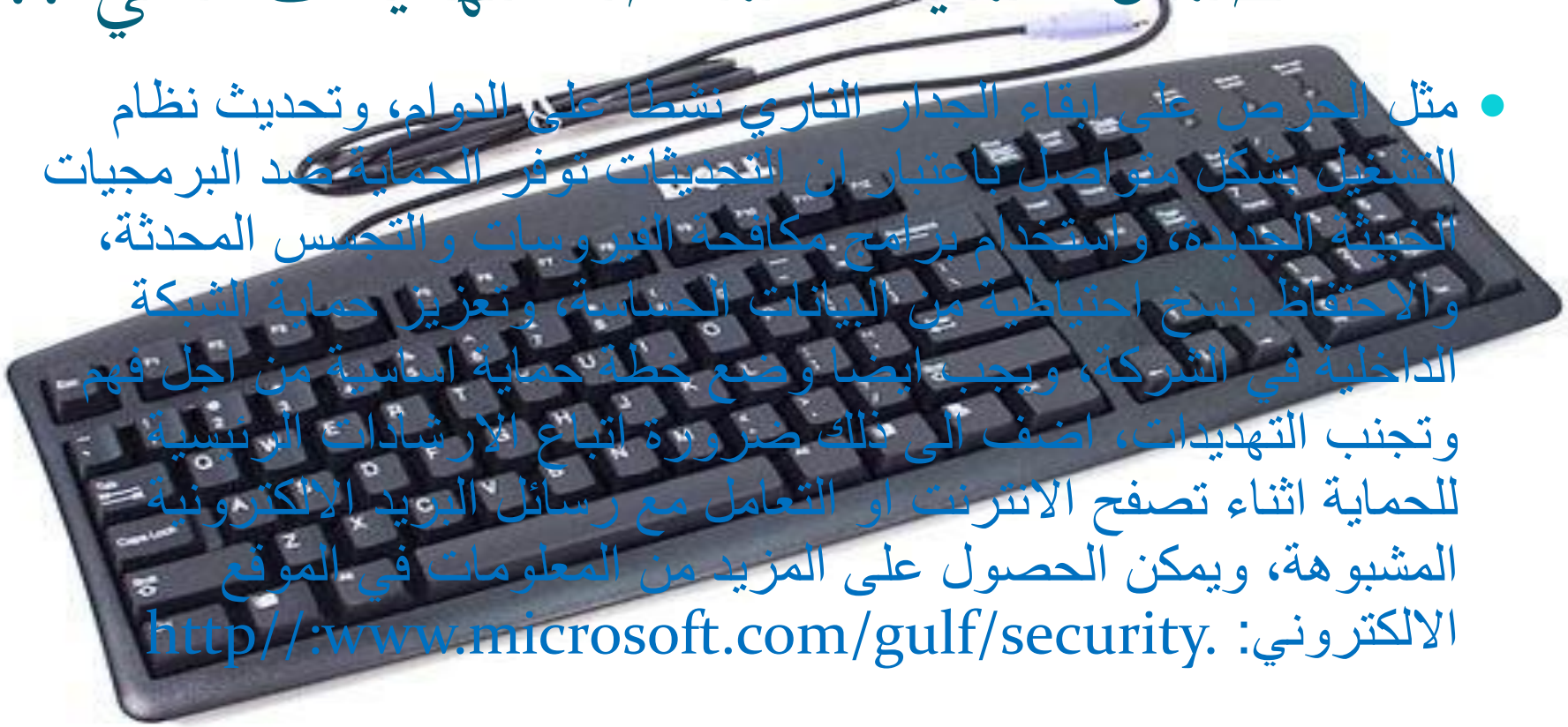
ما هي رؤية «مايكروسوفت» للحماية الإلكترونية؟

- ـ يشهد العالم الرقمي تطورا متسارعا، وبات المستخدمون ينجزون بواسطة الكمبيوتر أشياء أكثر من السابق، الأمر الذي افرز تحديات أمنية جديدة ينبغي على القطاع أن يستبقها ويكون مستعدا لمواجهتها. وتتمثل رؤية «مايكروسوفت» للحماية الإلكترونية في ايجاد بيئة تتيح للافراد والشركات استخدام الاجهزة المتنوعة للوصول إلى المعلومات والخدمات والتواصل مع الاشخاص المهمين بالنسبة لهم، بشكل آمن. وبناء على ذلك، طرحت الشركة في ابريل 2008، رؤية جديدة لتوسيع نطاق «الحوسبة الموثوقة» ليشمل الإنترنت، تحت عنوان «الحماية الإلكترونية الشاملة».

ما الخطوات التي تتخذها مايكروسوفت في مجال مكافحة البرامج الخبيثة Malware؟

- ــ تهدف مايكروسوفت إلى توفير أعلى مستويات الحماية الشاملة والمتواصلة للمستخدمين في جميع أنحاء العالم، ضد التهديدات الإلكترونية والمستقبلية. ويتولى مركز مايكروسوفت للحماية من البرامج الخبيثة Microsoft Malware Protection Center، مسؤولية إجراء الأبحاث والتصدي للتهديدات الجديدة وتوفير التقنيات والبنية التحتية الأمنية الضرورية لحماية المستخدمين. ومع تطور التهديدات الأمنية الإلكترونية، تؤكد مايكروسوفت التزامها المتواصل بمواجهة هذه المخاطر في جميع أنحاء العالم، باسلوب دقيق وموثوق ووفقا لأعلى معايير الكفاءة والفعالية، وكذلك توفير الجيل التالي من تقنيات الحماية التي تلبي متطلبات العملاء المتجددة.

هناك عدد من الخطوات الرئيسية التي يجب اتباعها لضمان الحماية الدائمة ضد التهديدات ماهي ؟؟



- مثل الحرص على ابقاء الجدار الناري نشطا على الدوام، وتحديث نظام التشغيل بشكل متواصل باعتبار ان التحديثات توفر الحماية ضد البرمجيات الخبيثة الجديدة، واستخدام برامج مكافحة الفيروسات والتجسس المحدثة، والاحتفاظ بنسخ احتياطية من البيانات الحساسة، وتعزيز حماية الشبكة الداخلية في الشركة، ويجب ايضا وضع خطة حماية اساسية من اجل فهم وتجنب التهديدات، اضف الى ذلك ضرورة اتباع الارشادات الرئيسية للحماية اثناء تصفح الانترنت او التعامل مع رسائل البريد الالكترونية المشبوهة، ويمكن الحصول على المزيد من المعلومات في الموقع الالكتروني: http//:www.microsoft.com/gulf/security.

لماذا تستغرق مايكروسوفت وقتا طويلا لإصدار تحديثات الحماية؟

- ـ تعمل مايكروسوفت بشكل دائم على رصد الثغرات الامنية الحالية والمحتملة بهدف حماية المستخدمين، وهناك العديد من العوامل التي تلعب دورا في تحديد المدة الزمنية بين اكتشاف الثغرة واطلاق التحديث الامني الخاص بها، فكل ثغرة تفرض تحديات خاصة بها. ويعد تطوير التحديثات الامنية القادرة على اصلاح العيوب بكفاءة وفعالية، عملية واسعة النطاق ، تستلزم عددا من الخطوات، فمثلا: عندما يتم الابلاغ عن ثغرة محتملة، يبدأ الخبراء المتخصصون بحماية المنتج المعني، العمل على تحديد نطاق التهديد، واثره على المنتج، وعند معرفة حجم الثغرة، نعمل على تطوير التحديث للنسخ المدعومة كافة المصابة بها، ولدى اكتمال التحديث، نقوم باختباره على مختلف انظمة التشغيل والتطبيقات المتأثرة، ومن ثم نترجمه الى لغات مختلفة بحسب كل سوق في انحاء العالم كافة.

كيف تميزون عادة بين أنواع التهديدات المختلفة، مثل «الديدان» Worms وملفات (تروجان) و«الفيروسات»، وهل هي ذات طبيعة متشابهة؟

- ـ يطلق على هذه التهديدات غالبا اسم «البرامج الخبيثة»، فالفيروسات تصيب بعض الملفات التنفيذية والتي عند تشغيلها ينتقل الفيروس الى ملفات اخرى. بيد ان الديدان تعتبر برمجيات خبيثة ذاتية النسخ، وتستغل الشبكة المحلية او الانترنت لارسال نسخ منها الى اجهزة اخرى بسرعة فائقة. واما «التروجان»، فيظهر على صورة برنامج قادر على تأدية وظيفة مرغوب فيها، ولكنه في الواقع يخفي وراءه عمليات خبيثة او ضارة.

ما التدابير التي تتخذها مايكروسوفت للحد من الثغرات الأمنية الالكترونية؟

- ـ تعد «دورة تطوير الحماية» Security Development Lifecycle، جزءا من مبادرة «الحوسبة الموثوقة» وهي عملية طورتها الشركة لتزويد العملاء ببرمجيات فائقة الجودة مصممة بدقة متناهية وخاضعة لأقسى الفحوص والتجارب، والتي من شأنها ان تساعد على التصدي للهجمات الخبيثة. و تخضع جميع منتجات الاتصال بالانترنت والمنتجات الخاصة بالمشاريع لهذه الدورة التي يتم تحديثها بانتظام من خلال الخبرات والممارسات المكتسبة عبر جميع مراحل دورة تطوير المنتج، الامر الذي يؤدي الى تحسينات قابلة للقياس على صعيد الأمن وحماية الخصوصية. وتدعو مايكروسوفت الى استخدام عملية «دورة تطوير الحماية» في جميع المنتجات المستخدمة او المطبقة بالمشروع المعني، وكذلك في اي منتج يقوم عادة بتخزين ومعالجة ونقل المعلومات المالية او اي بيانات حساسة خاصة بالعملاء، وكل المنتجات التي تحتك من قريب او بعيد بالانترنت.

عـــــرفي الفـــيروسات:☺

- هي برامج صغيرة تصيب الأجهزة وتتسبب في الكثير من المشاكل الخطيرة كمسح الذاكرة الصلبة أومسح بعض الملفات الهامة في أنظمة التشغيل أوالقيام بإصدار الأوامر لبعض البرامج دون علمك أوتدخل مباشر منك مثل ما عمل فيروس الحب. ولمزيد من المعلومات عن أنواع الفيروسات وكيفية عمل البرامج المضادة يمكن الاطلاع على التفاصيل المتوفرة في موقع شركات برنامج الحماية من الفيروسات مثل نورتن ومكافي وغيرها.

من هم الهاكرز ؟

- هم الأشخاص الذين يخترقون جهازك فيستطيعون مشاهدة ما به من ملفات أو سرقتها أو تدمير جهازك أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت ..

جواسيس البريد الإلكتروني

- وهم عادة من المخترقين السابقين لجهازك أوممن يشاركونك الجهاز فعليا سواء في المنزل أوالعمل. أو مستخدم آخر للجهاز خاصة إذا كنت في مقهى للإنترنت ولم تخرج من برنامج البريد بشكل صحيح أولم تقم بالخروج من برنامج المتصفح.
راصدو لوحة المفاتيح
وهم من أخطر مصادر التهديد الأمني حيث إنهم قادرون على رصد أي ضغطة على لوحة المفاتيح وبذلك يتمكنون من رصد كل ما يتم كتابته على لوحة المفاتيح خاصة اسم المستخدم وكلمات العبور وذلك حتى قبل أن يتمكن جهازك أوبرنامجك من اخفاء وتشفير الكلمة

- ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة لأنها تتطلب الوصول الى جهازك فعليا. ويكثر استخدام هذه البرامج من قبل النساء (الزوجات) لمراقبة دردشة الأزواج على الشبكة ! كما يستخدمها بعض ضعاف النفوس لرصد معلومات الغير في مقاهي الإنترنت والأجهزة العامة في المكتبات وغيرها من الاماكن الأخرى. ولذلك يتردد الكثير من المستخدمين ممن يعتمدون على الأجهزة العامة كمقاهي الإنترنت (ولا يمتلكون أجهزة خاصة بهم) من الشراء المباشر من الإنترنت واستخدام بطاقات الائتمان ويفضلون التحويل البنكي أوالاتصال لإملاء الرقم بالهاتف أما إذا كنت تتسوق من جهازك الخاص فلا داعي للقلق

خطوات وإجراءات بسيطة

- هنالك عدة إجراءات بسيطة ينبغي التعود عليها أثناء تصفحك للإنترنت. علما بأن هذه الإجراءات لا تغنيك عن اقتناء برنامج حماية متخصص ولكنها كافية لكي تبدأ ببناء خط دفاعي أول وقوي يصعب من مهمة اللصوص والمتطفلين خاصة اذا كنت تعمل من جهاز شخصي متصل بالإنترنت عن طريق مودم. أما إذا كنت متصلاً بالإنترنت بطريقة أسرع كالخطوط الرقمية فأنت بحاجة فورية لبرنامج متخصص للحماية والسبب هو حصولك على رقم أي بي (عنوان بروتوكول الإنترنت) ثابت مخصص لك. ما يسهل عملية تتبعك على الإنترنت. أما لوكنت تستخدم فاكس مودم عاديا للاتصال بالإنترنت فإن مزود الخدمة لا يخصص لك رقم أي بي محددا ولكنك تحصل على رقم مختلف كلما قمت بالاتصال على الشبكة. أما لوكنت تملك شبكة من الكمبيوترات المتصلة مع بعضها البعض وجهازك يعتبر جزءا من هذه الشبكة المتصلة بالإنترنت فإنك بحاجة فورية لبرنامج حماية متخصص (جدران اللهب) وذلك لأن المخارج المخصصة لمشاركة الملفات تكون مفتوحة وجاهزة ومواتية لدخول الهاكرز.

نصائح

مصادر التهديد الأمني في الرسائل الإلكترونية

- أولا: الملفات المرفقة التي تتطلب الفتح والتحميل: عليك بالحذر الشديد عند فتح الملفات الملحقة بالرسائل الإلكترونية لأنها أكثر الطرق استخداما من قبل أشرار الإنترنت. ولذلك ننصحك بعدم فتح الملفات المرفقة اذا كانت من أحد الأنواع التالية. وخاصة إذا لم تكن من شخص معروف لديك. وهذه الملفات الملحقة الخطيرة تنتهي بأحد هذه الاختصارات:
((Command Files.)=(COMوهذا يعني وجود ملف به أوامر للتنفيذ مرتبطة بأي جزء من الملف وتبدأ بالعمل بعد مرور وقت معين أوحين الضغط على جزء معين.
((Batch Files.) =(BATوهذا يعني وجود أمر معين موجه لأحد ملفات نظام التشغيل في جهازك.
((Application) =(APPوهذا يعني وجود ملف به برنامج تطبيقي وهي خطيرة لأنها ممكن أن تكون أحدبرامج التجس.

ثانيا: الملفات المرفقة ذاتية التشغيل:

- وهي قادرة على أن تقوم بالعمل حال فتحك لبرنامج البريد الإلكتروني ودون الحاجة لفتح المرفقات وتقوم بإعادة تحميل نظام التشغيل لديك ومن ثم العمل في الخفاء. وتقوم بإضافة نفسها في كل رسالة ترسلها دون علمك لتصيب بها بقيةالمستخدمين. ومن أهم الأمثلة على ذلك ملف: WScript.kakوالطريقة الوحيدة لحماية نفسك من مثل هذه النوع هوإلغاء وحجب خاصية Alow Scriptingمن متصفحك.

ثالثا: بقة نظام التشغيل دوس:

- هذا مصدر تهديد يسمح لمرسل الرسالة أوالصفحة من تخريب وتعطيل جهازك حال فتحك لرسالته. التي يتم فيها استخدام لغة الترميز اتش تي إم إل. لأنه من الممكن زرع تعليمات وبرامج مستخدمة في نظام التشغيل القديم وهو مايعرف بنظام دوس. ليتم تعطيل نظام ويندوز. وأكثر نظم التشغيل التي يمكن أن تتأثر بها هي نظام التشغيل ويندوز 95 و98 لأنهما يعتمدان على دوس 16 بت. وفي هذا النظام القديم توجد بعض الأوامر التي تمكن نظام التشغيل من التعامل مع بقية المكونات.

- ومنها على سبيل المثال للتعامل مع الطابعة والمودم وهي: LPT1 for printerCOM1. COM2 for communication and Fax modem.وتكمن المشكلة في تعرف نظام التشغيل ويندوز على هذه الأوامر القديمة والتي لا تستخدم في ويندوز حاليا ولكنها في نفس الوقت تتعرف على البرامج والأوامر القديمة إذا ما تم زرعها في لغة الترميز وهي تسبب بعض المشاكل لأنها تجعل نظام ويندوز يتبادل المعلومات والأوامر مع المكونات مثل الفاكس مودم والطابعة بدلا من القرص الصلب وبالتالي يتوقف الجهاز عن العمل ولذلك ينصح كل من يستخدم ويندوز 98 او95 بالقيام بتحديث الملفات من موقع الشركة لتغطية هذا العيب.

أشهر الفيروسات

من أشهر الفيروسات التي تنتشر عن طريق الرسائل الإلكترونية:

I Love You
Meet Melissa
Buble Boy
Yaha
Nimda
Kletz

وأخـــــيراًاًاًًًًًًً

وللوقاية والحماية أثناء استخدام البريد الإلكتروني يجب اتباع الآتي:

- استخدام برامج مضادة للفيروسات وبرامج حماية وبرامج التشفير المتخصص.
استخدام كلمات عبور سهلة التذكر ولكن صعبة التخمين كأن تكون مكونة من حروف وأرقام أوخليط من الأحرف الكبيرة والصغيرة.
غلق المتصفح حال ابتعادك عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح.
عدم استخدام خاصية تذكر اسم المستخدم وكلمة العبور.
عدم استخدام خاصية الإكمال الآلي والتلقائي للاسم وفراغات النماذج في المتصفح.
عدم استخدام خاصية تذكر الصفحات التي تقوم بزيارتها لفترات طويلة وتقليل هذه المدة على قدر المستطاع.
عدم فتح الملفات المرفقة اذا كانت من أحد الأنواع التي تم ذكرها في البداية.
عدم تحويل الرسائل المشبوهة الى أصدقائك ومعارفك.