# جـــرائم الانتـــرنت

◁ لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه "جرائم" يمكن أن تنتهك على الشبكة ، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين ومنسوبي الجامعات- لهذا فالشبكة ليست آمنة في تصميمها وبناؤها- لكن مع توسع استخدام الشّبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها.

**والسؤال الذي يطرح نفسه لماذا لا يعاد تصميم الشبكة وبناؤها بطريقة تحد من المخاطر الأمنية ؟- إن حلا جذريا كهذا يصعب تنفيذه من الناحية العملية نظرا للتكلفة الهائلة المتوقعة لتنفيذ أي حل في هذا المستوى.**

**إن شبكة الإنترنت كشبكة معلوماتية ينطبق عليها النموذج المعروف لأمن المعلومات ذي الأبعاد الثلاثة وهي:**

١- سرية المعلومات: وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك-

٢- سلامة المعلومات: يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك-

٣- وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك-

**إن جرائم الإنترنت ليست محصورة في هذا النموذج، بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة- إن أهم الأهداف المقصودة في تلك الجرائم هي كالتالي:**

**١- المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره-**

**٢- الأجهزة: ويشمل ذلك تعطيلها أو تخريبها-**

**٣- الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز- علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة-**

بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها- حيث يستخدم المجرمون أسلحة" تقليدية" ابتداء من المشارط والسكاكين وحتى عبوات متفجرة ، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بنزين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمته- وفيما يلي استعراض لعدد من جرائم الإنترنت-

**أولا: صناعة ونشر الفيروسات: وهي أكثر جرائم الإنترنت انتشارا وتأثيرا- إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف فون نيومن في منتصف الأربعينات الميلادية- لم تكن الإنترنت الوسيلة الأكثر استخداما في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة ، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات-ولا يخفى على الكثير سرعة توغل ما يسمى بـ "الدودة الحمراء" حيث استطاعت خلال أقل من تسع ساعات اقتحام ما يقرب من ربع مليون جهاز في ١٩ يوليو ٢٠٠١م.**

**إن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها و نقلها إلى أجهزة أخرى-**

ثانيا: الاختراقات: تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب الي- إن جل عمليات الاختراقات (أو محاولات الاختراقات) تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة-

**تختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة- وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه ، كأن يقوم المخترق بعمليته بقصد إبراز قدراته "الإختراقية" أو لإثبات وجود ثغرات في الجهاز المخترق-**

من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع (Defacing). إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة-

**ثالثا: تعطيل الأجهزة: كثر مؤخراً ارتكاب مثل هذه العمليات ، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة-تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها-**

من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل الأجهزة المستضيفة للمواقع على الشبكة- إن الأسباب وراء استهداف هذا النوع من الأجهزة تماثل أسباب استهدافها في جرائم الاختراقات والتي سبق ذكرها في "ثانيا"-

**جميع الجرائم التي ذكرناها تستهدف بشكل مباشر معلومات أو أجهزة وشبكات حاسبات-أما جرائم الإنترنت التي تستهدف جهات سواء كانوا أفراداً أو مؤسسات، ففيما يلي عرض لبعضها:**

رابعاً: انتحال الشخصية: هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية- تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى- إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية- وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة-

**خامساً: المضايقة والملاحقة: تتم جرائم الملاحقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة- تشمل الملاحقة رسائل تهديد وتخويف ومضايقة.**

● تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية - تتميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة- من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية لا يعني بأي حال من الأحوال قلة خطورتها- فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية-

**سادساً: التغرير والاستدراج: غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة- حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين- إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر- وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك كثير من الضحايا أنهم قد غُرر بهم-**

سابعاً: التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فرداً أو مجتمع أو دين أو مؤسسة تجارية أو سياسية- تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين-

**ثامناً: صناعة ونشر الإباحية: لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية- إن الإنترنت جعلت الإباحية بشتى وسائل عرضها من صور وفيديو وحوارات في متناول الجميع ، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا السعودي- إن صناعة ونشر الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال- لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة اربع سنوات والتي انتهت في ديسمبر ١٩٩٨م، تتعلق هذه الجرائم بتغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال-**

تاسعاً: النصب والاحتيال: أصبحت الإنترنت مجالاً رحباً لمن له سلع أو خدمات تجارية يريد أن يقدمها، وبوسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق ساحات الحوار-ومن الطبيعي أن يساء استخدام هذه الوسائل في عمليات نصب واحتيال- ولعل القارئ الكريم الذي يستخدم البريد الإلكتروني بشكل مستمر تصله رسائل بريدية من هذا النوع-

**● إن كثيراً من صور النصب والاحتيال التي يتعرض لها الناس في حياتهم اليومية لها مثيل على شبكة الإنترنت مثل بيع سلع أو خدمات وهمية، أو المساهمة في مشاريع استثمارية وهمية أو سرقة معلومات البطاقات الائتمانية واستخدامها- وتتصدر المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت- إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعة قدرة مرتكبها على الاختفاء والتلاشي-**

بعد هذا العرض لعدد من أنواع جرائم الإنترنت ، أجد نفسي أمام سؤال مهم يطرح نفسه بقوة ألا وهو: هل من المهم إحداث أنظمة ولوائح تعطي السلطات الأمنية والقضائية الحق في تجريم هذه الأعمال وبالتالي تطبيق عقوبات جزائية على مرتكبيها ، أو يمكن استخدام الأنظمة الموجودة والمستخدمة في تجريم ومعاقبة جرائم السرقة والتعدي والنصب والاحتيال وغيرها من الجرائم التقليدية-في الحقيقة لا يوجد إجماع بين أهل الاختصاص على هذا الرأي أو ذاك ، لكن نظراً لأن الأنظمة الخاصة بالجرائم التقليدية قد لا تغطي جميع جوانب جرائم الإنترنت لذا فإن من المهم في رأيي وجود نظام يجرم الأعمال غير المشروعة على الإنترنت ويعاقب مرتكبيها -

**● والأهم من ذلك هو توعية أفراد السلطات الأمنية والقضائية المعنية بهذه الأنواع من الجرائم على كيفية التعامل معها وتدريبهم على دراسة و تحليل الأدلة ، فلاشك أن طبيعة هذه الجرائم تختلف عن الجرائم التقليدية ولذلك فإنه يتعين على من يتعامل معها أن يمتلك قدرات تقنية ملائمة-**

**د-إياس الهاجري**
موقع الدراسات والبحوث

# الحاسب الالكتروني والجرائم

**● القوانين مرآة المجتمع، ومقياس لحضارة ورقي الدولة، فهي النور الذي يهدي إلى الصواب دون إرهاق، وبقدر ما تكون متطورة، بقدر ما تحقق الغايات التي وجدت لأجلها. رافق الثورة الصناعية منذ منتصف القرن الماضي تطورات وتبدلات بسائر جوانب الحياة في المجتمع فانعكست متطلبات تلك الثورة على المعلومات التي زادت غزارتها وضخامة عدد كتبها ووثائقها لدرجة بات معها أمر حفظها وتخزينها يستلزمان مكتبات كثيرة وأماكن واسعة، وتصنيفها وتبويبها يتطلبان وقتاً وجهداً كبيرين. والرجوع إليها لا يقل عن ذلك جهداً ووقتاً.**

**فكان لا بد من التفكير بوسيلة يتم من خلالها تجاوز هذه المشكلات، إلى أن ظهر الحاسوب وبدأ بالعمليات الحسابية، ثم تطور ليشمل أعمال التخزين واستيعاب كبير للمعلومات، وتجميعها وترتيبها واسترجاعها بسرعة فائقة ودقة متناهية فصارت المعلومات في متناول الأيدي، بجهد بسيط ووقت طويل.**

**هذه الميزات العالية جداً للحاسوب الإلكتروني جعلت الاستعانة به واستخدامه ضرورة لا غنى عنها لدى أجهزة الدولة والأشخاص الاعتباريين والعاديين، مما جعل الحاسوب يفرض نفسه في كافة المجالات.**

**● نتيجة ذلك ظهرت إلى حيز الوجود علاقات استثمارية جديدة، بعضها انصب على تصنيع الحاسبات وآخر على إعداد البرامج اللازمة لمعالجة المعلومات، وإعداد الكوادر الفنية المتخصصة في أعمال الحاسوب إضافة لدخول الحاسوب نفسه كسلعة جديدة في مجال التداول التجاري.**

**ظهور هذه العلاقات رافقه ظهور لعلاقات قانونية جديدة، لم تكن معروفة من ذي قبل، ولدى قيام المنازعات بشأنها، وقفت النصوص القانونية السائدة قاصرة . إن لم تكن عاجزة . عن هذه المنازعات والجرائم، خاصة مع بروز الجريمة المعلوماتية إلى حيز الوجود.**

**فالجريمة المعلوماتية قوامها أحد السببين التاليين:**

**- أن تكون المعلوماتية، وسيلة للغش والتحايل والاعتداء.**

**- أن تكون المعلوماتية نفسها محلاً للاعتداء.**

**● هذه الجرائم تمس حقوق مرافق حيوية هامة للدولة، وأشخاص اعتباريين وعاديين، وهي جرائم لا يستهان بها لمساسها بمصالح المجتمع، خاصة فيما يتعلق بالبنوك بتعاملاتها الإلكترونية من سحب للأرصدة وإيداع عن طريق البطاقة المغنطة، وكذلك تقليد برامج الحاسوب والمساس بالحياة الخاصة للأفراد عن طريق التسجيل وغيرها من المجالات التي يستعمل فيها الحاسوب الإلكتروني.**

**والجريمة المعلوماتية ذات طبيعة خاصة، لتعلقها بأساليب المعالجة الإلكترونية للبيانات، من تجميع وتجهيز للبيانات، بغية الحصول على معلومات، وبأساليب معالجة الكلمات أو النصوص والوثائق المخزنة في الحاسوب بطريقة أوتوماتيكية تمكن المستخدم من الاطلاع على وثائق الحاسوب، ومن إجراء التعديلات عليها من محو أو إضافة، كما في حالات التقليد والتزوير.**

**من هذا يتراءى لنا أن الفاعل في جرائم المعلوماتية أو ما يسمى (بالمجرم المعلوماتي) ليس شخصاً عادياً إنما شخصاً ذو مهارات تقنية عالية، قادراً على استخدام خبراته في اختراق الكود السري لتغيير المعلومات، أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسب بشكل غير مشروع.. وهذا يعني تطور أعمال الإجرام، وانتقالها من عالم المجرمين البؤساء إلى عالم مجرمي المهارات المعلوماتية من ذوي الياقات البيضاء والسمات الخاصة..ويبين لنا أيضاً أن جهاز الحاسوب على الرغم من قدرته العالية، بالإمكان التأثير عليه والتلاعب فيه من خلال نسخ برامجه أو إدخال معلومات غير حقيقية أو تعديل أو حذف المعلومات والبرامج بأشكال غير مشروعة.**

**● ومن مراجعة النصوص القانونية الحالية المتعلقة بالتزوير والسرقة والاحتيال وتقليد العلامات الفارقة وغيرها من النصوص المشابهة، نجد أنها رغم أهميتها قاصرة عن تغطية الحالات الجرمية المستجدة نتيجة لظهور هذه التقنيات، وانتشار المعلوماتية وتوسع نطاقها على مختلف الصعد والمجالات.**

**هنا تظهر الحاجة ملحة لوضع تشريع، لحماية البرامج المعلوماتية الإلكترونية، وحماية الحاسبات الإلكترونية نفسها من كل فعل يلحق الضرر بها او بمضامينها..فالقاضي عند نظره بدعوى مطروحة لديه، مقيد بما هو نافذ من نصوص قانونية، ومهما حاول الاجتهاد والقياس والتفسير والتأميل، فإن حكمه غير محصن من الطعن فيه، خاصة وأنه لا عقوبة على جرم، لم يأت عليه نص قانوني.**

**المحامي عدنان فيومي**
دمشق . سورية

# كيف تعمل وصلة الناقل العام

● تقوم وصلة الناقل العام بنقل البيانات بشكل تفاضلي عبر زوج واحد من الأسلاك بينما يقوم الزوج الآخر بتزويد ملحقات الكمبيوتر والأجهزة ذات الاستهلاك البسيط للطاقة بالطاقة الكهربائية في بعض الأحيان. يتميز الإصدار الأولي ١ من وصلة الناقل العام USBبنقله للبيانات بسرعة ١٢ ميغابت بالثانية، ولكن هذه السرعة لم تعد تنفع مع التطور الهائل في ملحقات الكمبيوتر وازدياد سرعاتها، فتم تطوير الإصدار ٢,٠ من الناقل العام في عام ٢٠٠٢ والذي تفوق على الإصدار ١ بسرعته لنقل البيانات والبالغة ٤٨٠ ميغابت بالثانية. وإذا كنت من محبي إضافة الكثير من الملحقات للكمبيوتر، فستجد ضالتك في وصلة الناقل العام ٢,٠ التي تمكّن المستخدم من إضافة العديد من الملحقات للكمبيوتر (١٢٧) ملحق أو أداة مما يجعل من الكمبيوتر المزود بوصلة الناقل العام كمبيوترا مميزا قابلا للترقية.

ولا تحتاج إضافة وصلة الناقل العام كمبيوترا متطورا بل يمكنك إضافة وصلة الناقل العام للكمبيوتر بنظام التشغيل ويندوز ٩٥ والإصدارات اللاحقة منه لكن الإصدار ٢,٠ من الناقل العام USBيستدعي تأمين دعم خاص له في الأجهزة وفي نظام التشغيل.

× تشمل وصلة الناقل العام ثلاثة أجزاء: المضيف ( الكمبيوتر)، وملحقاته ووحدة الوصل المركزية. تتميز وصلة الناقل العام بتصميمها المثالي المناسب لوصل كافة ملحقات الكمبيوتر بالناقل العام. توفر وصلة الناقل العام للمستخدم فوائد كثيرة فهي تقلل من أسلاك الوصل الخاصة بملحقات الكمبيوتر، فمع وصلة الناقل العام لم يعد من الضروري وصل الملحقات مباشرة بالكمبيوتر بل يمكن وصلها بالمفرّع والتي تتصل بدورها بوحدات وصل أخرى ومن ثم توصل بالكمبيوتر. وعند إضافة وصلة الناقل العام يظهر الكمبيوتر تغيرا واضحا في الفولتات ثم يطلب من المستخدم معلومات عن الملحق الجديد كنوعه واسم الشركة المصنّعة، يعطي الكمبيوتر للملحق الجديد عنوانا خاصا يتم بعدها تحميل السواقة من قبل نظام التشغيل.

وبشكل مماثل يكتشف الكمبيوتر إلغاء ملحق ما من الجهاز فيحمّل الكمبيوتر البرنامج المناسب ويلغي السواقات الأخرى. وتتميز معظم الكمبيوترات بوصلة الناقل العام من الطراز المعروض في وسط الصورة، وتأتي نهايات كابلات الناقل العام بنوعين الأول يتصل بالكمبيوتر والثاني بالملحقات الأخرى مثل الطابعات والكاميرات، تسمى بعضها وصلات ميني . Mini USBستلاحظ عند مقارنة المنتجات مع بعضها أن مجموعة منها تدعم الإصدار ١,١ فقط من الناقل العام والذي يوفر معدل تبادل بيانات بسرعة ١٢ ميغابت بالثانية، في حين أن مجموعة أخرى منها تدعم أيضا الإصدار ٢,٠ الأحدث من الناقل العام والذي يوفر معدل نقل بيانات بسرعة ٤٨٠ ميغابت بالثانية يرمز له أيضا بالسرعة العالية High Speedولكن الاستفادة من هذه السرعة مشروطة بتوفر منفذ الناقل العام ٢,٠ في كمبيوترك. وانتبه من سرعة تعرف باسم السرعة الكاملة Full Speedللناقل العام ٢,٠ الجديد وهي توفر معدل نقل بيانات بسرعة ١٢ ميغابات بالثانية، وبالتالي فإن الفارق كبير بين هذه السرعات وعليك الانتباه إليها عند شراء هذه الأقراص.

## سؤال & جواب

# جدار الحماية في XP

**● محمد رياض جبران**
MOHAMDY@HOTMAIL.COM

**● ما هو جدار الحماية المتوفر في ويندوز XP؟ و كيف يتم تفعيله ؟**

- إن جدار الحماية هو نظام الأمان الذي يعمل كحد وقائي بين شبكة الاتصال والعالم الخارجي. إن جدار حماية اتصال إنترنت (ICF)هو برنامج جدار الحماية المستخدم لتعيين قيود على نوعية المعلومات المتبادلة بين جهازك الشخصي أو شبكتك المنزلية أو المكتبية الصغيرة وإنترنت.

يعتبر ICFجدار حماية "مصحوب بالحالة". جدار الحماية المصحوب بالحالة هو الجدار الذي يراقب كافة أوجه الاتصالات التي تعبر مساره ويختبر عنوان الوجهة والمصدر لكل رسالة يعالجها. لمنع حركة المرور غير المطلوبة من الطرف العام للاتصال من دخول الطرف الخاص، يحتفظ ICFبجدول لكافة الاتصالات التي تم إجراؤها من كمبيوتر .ICF في حالة الكمبيوتر المفرد، يتتبع ICFحركة المرور الخاصة بالكمبيوتر. عند استخدامه في حالة مشاركة مجموعة أجهزة لإتصال الإنترنت ICS، يتتبع ICFكامل حركة المرور الخاصة بكمبيوتر ICF/ICSوالخاصة بأجهزة كمبيوتر شبكة الاتصال الخاصة. تتم مقارنة حركة المرور الواردة من إنترنت مع الإدخالات في الجدول. ويتم السماح لحركة مرور إنترنت الواردة بالوصول إلى أجهزة الكمبيوتر الموجودة على شبكة الاتصال عند وجود إدخال مطابق في الجدول الذي يظهر بدء تبادل الاتصال من ضمن الكمبيوتر أو شبكة الاتصال الخاصة.

يتم إسقاط الاتصالات الناتجة من مصدر خارج كمبيوتر ICF، كإنترنت مثلاً، من قبل جدار الحماية إلا إذا تم إنشاء إدخال في التبويب الخدمات للسماح بالمرور. وعوضاً عن إرسال إعلامات حول النشاط، يقوم ICF بصمت بتجاهل الاتصالات غير المطلوبة، مع إيقاف المحاولات الشائعة للقرصنة مثل مسح المنفذ. إذ أنه يمكن إرسال هذا النوع من الإعلامات بشكل متكرر مما يؤدي إلى تعطيك عن العمل. عوضاً عن ذلك، يمكن أن يقوم ICF بإنشاء سجل أمان لعرض النشاط المتتبع من قبل جدار الحماية.. تحقق ICFمن كافة الاتصالات الواردة، لذلك قد تتصرف بعض البرامج، وخاصة برامج البريد الإلكتروني بشكل مختلف عند تمكين .ICFتقوم بعض برامج البريد الإلكتروني وبشكل دوري باستقصاء ملقم البريد الإلكتروني الخاص بها للاستعلام عن البريد الجديد، بينما تنتظر بعض برامج البريد الإلكتروني وصول الإعلام من ملقم البريد الإلكتروني.

● يقوم مثلاً Outlook Expressبالتحقق تلقائياً من البريد الإلكتروني الجديد عندما يخبره ضابط الوقت الخاص به بالقيام بذلك..وعند وجود بريد إلكتروني جديد، يطالب Outlook Expressالمستخدم بإعلام بريد إلكتروني جديد.لذلك لن يؤثر ICFعلى سلوك هذا البرنامج ، بسبب صدور إعلام البريد الإلكتروني الجديد من داخل جدار الحماية. كما يقوم جدار الحماية بإنشاء إدخال خاص بالاتصال الصادر في جدول. وعند إرسال استجابة البريد الإلكتروني الجديد من قبل ملقم البريد، يعثر جدار الحماية على إدخال مقترن في الجدول ويسمح بمرور الاتصال، بعدها يتلقى المستخدم إعلام يفيد بوصول البريد الإلكتروني الجديد.. بالمقابل، يتصل Office 2000 Outlookالذي يستخدم بملقم Microsoft Exchange لاستدعاء الإجراء البعيد ( RPCلإرسال إعلامات البريد الإلكتروني الجديدة للعملاء. لا يقوم Office 2000 Outlookبالتحقق تلقائياً من البريد الإلكتروني الجديد عند اتصاله بملقم التبادل. يعلم ملقم Exchange برنامج Office 2000 Outlookبوصول البريد الإلكتروني. يتم البدء بإعلام RPCمن ملقم التبادل الموجود خارج جدار الحماية وليس من قبل Office 2000 Outlook، الموجود داخل جدار الحماية، لذلك لا يتمكن ICFمن العثور على الإدخال الموافق في الجدول، ولا يتم السماح لرسائل RPC بالعبور من إنترنت إلى الشبكة المنزلية. يتم إسقاط رسالة إعلام .RPCيمكن للمستخدمين إرسال البريد الإلكتروني وتلقيه، ولكن عليهم التحقق من رسائل البريد الإلكتروني الجديدة يدوياً..توفر ميزة تسجيل أمان ICFطريقة لإنشاء سجل الأمان لنشاط جدار الحماية. لدى ICFالقدرة على تسجيل كل من حركة المرور المسموحة وحركة المرور المرفوضة، يمكنك تعيين الحجم المسموح به لسجل الأمان لمنع التجاوز المحتمل والذي قد تتسبب به هجومات رفض الخدمة.

لتمكين الجدار الناري و تفعيله قم بما يلي:

انقر فوق أبدأ، انقر فوق لوحة التحكم، انقر فوق اتصالات شبكة الاتصال وإنترنت، ومن ثم انقر فوق اتصالات شبكة الاتصال.. ثم انقر فوق الطلب الهاتفي، أو فوق شبكة الاتصال المحلية أو فوق اتصال إنترنت عالي السرعة الذي تريد حمايته، ثم تحت مهام شبكة الاتصال، انقر فوق تغيير إعدادات هذا الاتصال.. في التبويب خيارات متقدمة، تحت جدار حماية اتصال إنترنت، حدد واحد مما يلي:

لتمكين جدار حماية الاتصال بإنترنت ((ICF، حدد خانة الاختيار حماية الكمبيوتر وشبكة الاتصال وذلك بمنع الوصول إلى هذا الكمبيوتر من إنترنت أو الحدّ منه.لتعطيل جدار حماية الاتصال بإنترنت، امسح خانة الاختيار حماية الكمبيوتر وشبكة الاتصال وذلك بمنع الوصول إلى هذا الكمبيوتر من إنترنت أو الحدّ منه.

توقف النظام

● نصر محمد سلام
salam_78@maktoob.com -

● يتوقف النظام لدي عن العمل دائماً وخاصة عندما أحاول تحميل أي برامج ثلاثية الأبعاد هل أستطيع إصلاح النظام دون الرجوع إلى تهيئة القرص وإعادة التحميل ؟

الصيانة في طبيعة الحال هي معالجة المشكلة والتأكد من سببها فقد يكون السبب هو الذي يجعلك تكرر تحميل النظام في كل مرة .. ولذا في المهندس الصحيح والذي يطلع عليه هذه العبارة بأنه لا يلجأ إلى عملية for-mat أي تهيئة الأقراص إلى كحل نهائي لأن عواقب تهيئة القرص يعني فقدان بياناته .. وقد يتم إنقاذ البيانات لكن تتبقى البرامج والتجهيز النظام على طبيعته وحسب رغبة المستخدم .. وليس كل شخص يتقن التهيئة يعني أنه مهندساً فهذا يعني وبعبارة أوضح أعدم النظام... فهناك طرق يمكن للمهندس الاستعانة بها لإنقاذ النظام ولنفترض لدينا نظام win xpأو نظام meفهذا النظامين يمكن من خلالهما استعادة النظام لوقت سابق.. فهذه الميزة التي تتوفر في الأنظمة والتي من خلالها يمكن أستعادة نظامك إلى وقت سابق وبحسب الأحداث التي سجلت من خلال الريجستيري تلقائياً .. أما الطريقة لاستعادة النظام فهي طريقة سلها للغاية .. فيمكن اختيار من قائمة إبدأ والبرامج الملحقة ومن قائمة أدوات النظام قم باختيار أستعادة النظام .. قم بعدها بمتابعة الرسائل التي ترد على شاشتك .. سوف تلاحظ خيارين الخيار الأول هو إنشاء نقطة استعادة وهذا يعني بأنك سوف تقوم بتسجيل نقطة استعادة لنظامك لكي تتمكن مستقبلاً الرجوع إليها.. أما عملية الاستعادة فهي تعني استعادة النظام لوقت سابق.

لكن بعض الأحيان قد يصادفك عدم تشغيل النظام نهائياً لكي تتمكن من استعادة النظام أو الدخول إلى سطح المكتب فتستطيع من خلال الوضع الآمن الدخول على نظامك وذلك بالضغط على F8عند بدء النهوض واختيار safe Modeثم قم باستعادة النظام من خلال النافذة في الوضع الآمن ..

أما إذا كان لديك ويندوز آخر سواء ٩٨ أو ٩٥ أو ٢٠٠٠ فتستطيع استعادة النظام وذلك بالدخول إلى المحث dos \>c:عن طريق قرص بدء التشغيل ومن ثم كتابة الأمر SCANREG /RESTOREفهذا الأمر يعني أنه سيتم استعادة النظام لوقت سابق حينها سوف تظهر أمامك على الشاشة نقاط الاستعادة وبالتاريخ حسب الحدث لتغييرات النظام أما طريقة تسجيل النظام عن طريق dosفيمكنك كتابة الأمر scanregثم متابعة الرسالة الواردة لتسجيل نقطة النظام ..أما في حالة ظهور رسائل خطأ في النظام أو عدم نهوض النظام فيمكنك التأكد من الرسائل الواردة على الشاشة ومن ثم معرفة الملف الناقص أو المحذوف .. ثم يتم نقله من جهاز آخر ليتم حينها نهوض النظام بالشكل الصحيح.

**م/ بشير عبدالله العواضي**
awadybashir@hotmail.com