# ماهو البروكسي وطريقة استعماله؟

● قد يتساءل الكثير عند سماعهم بمزود البروكسي عن ماهية هذا المزود؟ وما المقصود به؟ وما هي طريقة عمله ؟ ولماذا يستخدم؟ وما هي علاقته بفلترة المواقع؟

إن أهم ما يجب أن يعرفه مستخدمو الكمبيوتر، ومستخدمو إنترنت على الأخص، أن مزودات البروكسي هي مزودات تعمل كوسيط بين مستخدمي الشبكة و الإنترنت، بحيث تضمن الشركات الكبرى، المقدمة لخدمة الإتصال بإنترنت، قدراتها على إدارة الشبكة، والتحكم بها، وضمان الأمن، وتوفير خدمات الكاش.

● **طبيعة عمل المزودات**

يعمل مزود البروكسي بالتعاون مع مزود البوابات Gateway Server، على عزل شبكة المؤسسات المقدمة للخدمات، عن الشبكة الخارجية، كما يعمل البروكسي كجدار ناري Firewall، يحمي هذه المؤسسات من أي اقتحام خارجي لشبكاتها. يتلقى مزود البروكسي عبر إنترنت طلباً من المستخدم، (كطلب تصفح إحدى صفحات الشبكة)، فتجري العمليات التالية:

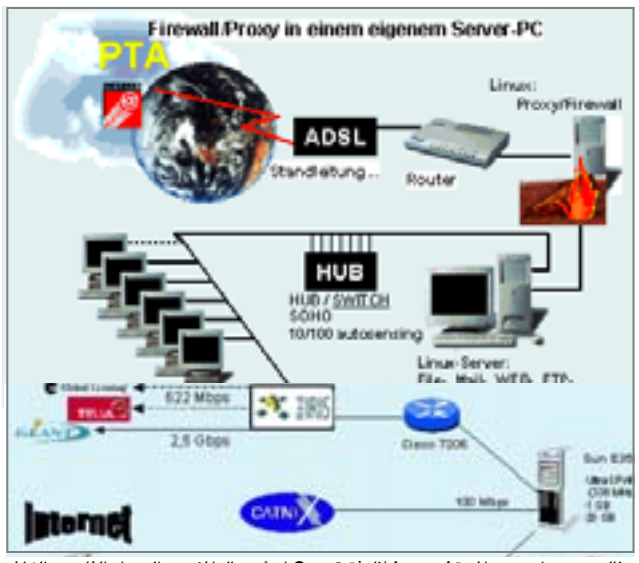
– يمرر الطلب على المرشحات المطلوبة.

– يعمل مزود البروكسي كمزود كاش Cache Server، بحيث يبحث عن الصفحة المطلوبة ضمن الكاش المحلي المتوفر، للتحقق فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك بالفعل، يعيدها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية.

– آما إذا لم يجد مزود البروكسي الصفحة المطلوبة ضمن الكاش، فإنه يعمل كمزود زبون Client Server، بحيث يستخدم أحد عناوين IP الخاصة به، ويرسل الطلب إلى الشبكة العالمية.

– عند يتلقى الصفحة المطلوبة من الشبكة، يقوم مزود البروكسي بربط الرد بالطلب الذي تلقاه من المستخدم سابقاً، ومن ثم يرسل الصفحة المطلوبة إلى المستخدم.

ومن أهم مزايا مزود البروكسي أن الكاش المتوفر لديه يمكنه أن يخدم كل المستخدمين، فإذا كان الموقع المطلوب، ذا جماهيرية كبيرة،




ويطالعه عدد واسع من المستخدمين، خلال فترة زمنية متقاربة، فإن المزود يحتفظ ضمن الكاش بنسخة عن صفحات هذا الموقع، ما يجعل عملية الرد على المستخدم الذي يطلب الصفحة، أسرع، بدون الحاجة لإرسال هذا الطلب إلى الإنترنت مرة أخرى. وهذا بدوره يوفر الوقت على المستخدم، و يؤمن سرعة جيدة في تنفيذ الطلب.

● إن أعمال المزود، والجدار الناري، والكاش، تتم ببرامج مزودات مستقلة، أو مجتمعة في حزمة واحدة ,وهذه البرامج قد تكون في أجهزة كمبيوتر مختلفة، أو أن يجتمع بعضها ضمن جهاز واحد.. أي أن مزود البروكسي و الجدار الناري، مثلاً، قد يجتمعان في جهاز واحد، أو يخصص جهاز مستقل لكل منهما، يجري إرسال الطلبات فيما بينهما.

وأخيراً، فإن مزود البروكسي يعمل في الخفاء، أي أن الطلبات والردود تظهر وكأنها ترتبط مباشرة مع عناوين إنترنت المطلوبة ,ولكن على المستخدم، لكي يضمن اتصال برامجه بالشبكة، أن يحدد Configure في متصفحه (أو في أي برنامج بروتوكول آخر)، عنوان IP الخاص بمزود البروكسي.

**أما بخصوص الفلترة، فهي ليست من مهمات البروكسي الأساسية. إلا أنه، بالتعاون مع برامج أخرى، وقواعد بيانات، يمنع وصول المستخدمين إلى مواقع محددة، وفق قواعد مختلفة، ولأسباب متنوعة.**

## ماهو البروكسي إذا؟

● البر وكسي هو الاتصال بالانترنت ويتم عن طريق سيرفر فأنت تعتبر زبون او كلاينت بالنسبة له والبر وكسي..عبارة عن حائط يحيط بالسيرفر لا يسمح بإدخال أي شخص إلا بعد التأكد من انضمامه لمجموعة الزبائن التي يخدمهم هذا البر وكسي ,لذلك عندما يتم الاتصال بأي عنوان فإن هذا البر وكسي يتأكد من هذا العنوان الذي تريد الدخول إليه وهل هو من ضمن القائمة المحظورة أم لا ؟

**فإذا كان من ضمنها تظهر لك رسالة**

BLOCKED BY PROXY

**أو تظهر رسالة أخرى مثل هذه**

UNABLED TO LOCATE THE SERVER

وهذا يعني أن المكان محظور أو قد تظهر لك رسائل عدة أخرى حسب برمجة الشركة للرسالة المراد ظهورها عند الدخول إلى هذه المواقع.

● **اغلب بعض الأشخاص لا يعرف ان اشتراكه مربوط مع بروكسي الشركة ولكن اتصالك مع السير فر يمررك من خلال البر وكسي بدون الحاجة إلى وضع عنوان البروكسي وفي هذه الحالة فانه سهل جدا كسر هذا البر وكسي وذلك بوضع عنوان آخر .. من البروكسيات الأخرى والمنتشرة في هذا الموقع وبهذا سيمررك السير فر إلى الموقع مباشرة.**

**إعداد / منصور الحرازي**

# اختر الصورة المفضلة بدلاً من كلمة السر؟

● إذا أردت فتح بريدك أو التعامل مع الصراف الآلي فتذكر الصورة بدلا من كلمة السر..فقد أصبحت كلمة السر جزءا من حياتنا لفك شفرة كمبيوتر العمل أو المنزل أو استخدام السيارة أو التعامل مع أنظمة المنزل الأمنية أو التعامل مع الأعمال المصرفية أو فتح البريد الإلكتروني مما يعكس حالة من الرتابة والملل خاصة في تذكر كلمة السر وكتابتها بشكل صحيح وإذا تهاون المستخدم في اختيار كلمة السر سيكون عرضة لسرقة اللصوص والعبث في خصوصياته ،الأمر الذي جعل الباحثين والمهتمين بشفرة الكمبيوتر يتجهون لاستخدام صور كبديل سهل لكلمة السر, فقد اتجهت بعض الشركات وعلى رأسها مايكروسوفت العملاقة في استبدال كلمات السر بصور يسهل تذكرها مقارنة بالأرقام والأسماء التي غالبا ينساها المستخدمون ,كما يطور حاليا مجموعة من الباحثين أشكالا من الصور للاستعمال بدلا من الكلمات وتكون أسهل في حفظها أصعب في اختراقها على لصوص الكمبيوتر .

ويرى أدريان بيريج الباحث ضمن فريق " يو سي بيركيلي " المتخصص في إعداد دراسات عن عادات مستخدمي الكمبيوتر أن الناس تتهاون في اختيار كلمات السر حيث تميل بشدة إلى استعمال كلمات سر مألوفة خاصة أسماء أفراد العائلة أو الحيوانات الأليفة .

● **وبلغة الأرقام يقول بيريج أن نتائج استطلاع أجريت بشركة تسجيل اسم الملكية البريطانية " سينترالينك " وجد أن ٤٧٪ من مستعملي الكمبيوتر يختارون أسماء العائلة في كلمة السر أو أسماء كلبهم أو قطتهم ويضيفون عليها رقم ظنا منهم أن هذا يحميهم من لصوص الكمبيوتر .**

**بينما ٣٢٪ من مستعملي الكمبيوتر يختارون الألعاب الرياضية أو موسيقى البوب أو نجوم السينما أو الأسماء الشهيرة في أفلام الكارتون أو أسماء الفريق الرياضي الذي يشجعونه ,لكن ٩٪ فقط هم الذين يختارون كلمات غامضة وأكثر صعوبة بها أرقام وأسماء مجهولة لمنع اختراق أجهزتهم .**

ويؤكد بيريج أن التهاون في اختيار كلمات السر تجعل الناس فريسة سهلة للصوص الكمبيوتر حيث يمكن معرفة كلمة السر في ظرف دقائق معدودة باستعمال برنامج أشبه بقاموس يستعرض كافة الكلمات الشائعة والوارد استخدامها وبسهولة يمكن التخمين لمعرفة كلمة السر عن طريق تشكيل متوالية حسابية بها أرقام وأسماء وبعملية حسابية بسيط تكتمل كلمة السر ليسهل اختراق الكمبيوتر .

● **كما أن نسيان كلمة السر أمر شائع بين مستخدمي الكمبيوتر خاصة في الشركات الكبرى التي يجب أن تضع خدمة لتذكر المستخدمين بكلمة السر على مدار اليوم مما يكلفها ملايين الدولارات بسبب ضياع الوقت في تذكر كلمة السر وكتابتها دون تغيير ,بينما لو استخدمت الصور كبديل لكلمات السر ستستطيع هذه الشركات توفير المال والجهد والوقت الضائع لتضائل فرصة نسيان الصورة وسهولة التعرف عليها .**

وأضاف بيريج أن ٩٠٪ من مستخدمي الكمبيوتر الذين تم اختبارهم من الباحثين في استخدام الصورة كبديل سهل لكلمات السر كانوا قادرين على تذكر الصورة والتعامل معها بيسر في حين وصلت نسبة المستخدمين الذين يتذكرون كلمات السر إلى ٧٠٪ من مستخدمي الكمبيوتر .

● **من ناحية أخرى تختلف الشركات في طريقة استعمال الصور حيث ترى شركة" ديجا فو بريج "أن استعمال صورة بسيطة وواضحة ومميزة الألوان على شاشة الكمبيوتر يعظم من فرص التعرف عليها بيسر في حين ترى شركة مايكروسوفت أن تكون الصورة معقدة مثل الأجزاء المختلفة لهيكل عظمي في جسم الإنسان من خلال استعراض لعدة وجوه عشوائية تكمل الصورة المطلوب التعرف عليها .**

حيث يقول باسفاس باريت أحد مصممي الصور يجب على المستخدم أن يتعرف على خمسة وجوه مختارة بشكل عشوائي ليتمكن من الدخول الصحيح للكمبيوتر وهو ما يحتاج إلى خمسة دقائق فقط هي المدة التي تظهر فيها الوجوه المختارة على شاشة الكمبيوتر ليتعرف المستخدم على الصورة المطلوبة .

● **ويضيف باريت أن نسبة نسيان المستخدمين للصور ضئيلة جدا فقد أثبتت الأبحاث أن شخص واحد من ٨ مليون مستخدم لا يستطيع تذكر الوجوه المختلفة التي تكون الصورة وهو ما يقلل من ظاهرة نسيان كلمات السر ويعيق عمل لصوص الكمبيوتر.**

في حين تختلف راتشنا دامجا الباحثة في فريق بيركيلي مع الباحثين في استخدام الصور كبديل لكلمات السر حيث تقول أن استخدام الصور ليس بديل سهل لإعاقة اختراق الكمبيوتر حيث يمكن للصوص الكمبيوتر فك شفرة الصور خاصة لو رجعوا لطبيعة المستخدمين فمن البديهي أن يميل الرجال إلى استخدام صور متعارف عليها مثل السيارات ,الجسور ,عملات معدنية .. الخ في حين تميل المرأة إلى استخدام الصور الرومانسية مثل الصور الطبيعية وما شابهها .

● **كما يرى مارك بوروديتسكاي رئيس شركة باسلوجيكس التجارية أن استخدام صور كبديل سهل لكلمات السر سيلزم الشركات بتنظيم دورات تدريبية للعاملين بها للتدريب على استخدام النظام الجديد وهو ما يعني معدل إنتاج مفقود بسبب جلسات تدريب العاملين .**

ويضيف لقد اتبعت شركته نظاما أفضل من ذلك حيث اختارت كلمة سر واحدة تتميز بالتعقيد والصعوبة في حل شفرتها وهذه الكلمة تقوم بفتح برنامج يقوم بدوره بفتح جميع أجهزة الكمبيوتر الخاصة بالشركة وهو ما يقلل فرص نسيان كلمة السر أو اختراق أجهزة الكمبيوتر.

**إيهاب سلطان**

## دقائق او اقل فكيف استطيع التخلص من هذه المشكلة ؟

– هذا يعني أن اللعبة ليست متوافقة مع الكمبيوتر أي أن العتاد الموجود لا يتوافق مع أداء اللعبة فمثلا كرت العرض VGA CARD والذي قد لا يدعم ثلاثي الأبعاد ٣ Dبينما اللعبة التي تقوم بتشغيلها قد تتطلب كرت عرض يدعم هذه الخاصية أي ٣ .. Dأما الاحتمال الآخر فقد تكون هناك مشكلة في SOFTWAREأي لا توجد برامج داعمة لهذه اللعبة ..

## وحدة القياس المناسبة

● **كيف أستطيع اختيار وحدة قياس مناسبة في برنامج وورد ؟**

– عندما نتعامل مع البرامج والتطبيقات علي الحاسب فإننا نفضل أن نختار وحدات القياس التي سنستخدمها لتحديد بيانات الملف الذي نتعامل معه. فعلي سبيل المثال عندما نتعامل مع برنامج Word لمعالجة الكلمات فنحن نحدد للبرنامج مساحة الصفحة والمسافة التي سيتركها للهوامش وتحديد المسافات بين السطور وغيرها من القيم التي يتم تحديدها باستخدام أحد وحدات القياس. عادة ما يستخدم البرنامج البوصة كوحدة للقياس وهذه الوحدة غير منتشرة في بعض البلدان ويفضل معظم المستخدمين التعامل مع وحدة السنتيمتر بدلا منها. يمكنك أن تقوم بتغيير وحدة القياس لكي تستخدم الوحدة التي تفضلها وسوف نتعرف معا على كيفية إجراء هذا التغير مرة واحدة فقط وسوف يحتفظ البرنامج بوحدة القياس التي اخترتها لكي تستخدم بعد ذلك بطريقة تلقائية.

● أولا: سنقوم بتشغيل برنامج Word لمعالجة الكلمات ثم نفتح قائمة الأدوات Tools ونختار منها خاصية الاختيارات Options بالضغط عليها بمؤشر الفأرة. من نافذة الاختيارات سنضغط على الاختيارات العامة Generalوسنجد في نهاية هذه النافذة خاصية تسمى وحدات القياس Measurement Units وهي الخاصية التي نريد التعامل معها. بجوار هذه الخاصية سنجد قائمة بها وحدات القياس التي يمكن للبرنامج التعامل معها مثل البوصة والسنتيمتر والمليمتر والنقطة. أختر وحدة القياس التي تريدها ثم اضغط على مفتاح Ok لتأكيد الاختيارات، معظم البرامج والتطبيقات الأخرى التي تتعامل معها على الحاسب توجد بها خاصية مشابهة لتلك التي توجد في برنامج Wordويمكننا ضبطها بطريقة مشابهة لكي نحدد وحدة القياس المطلوبة.

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

# سؤال & جواب

## الملف BOOT.INI

● **نصر جبران - عدن**
**NASR_GU_810@HOTMAIL.COM**

● **ما هو عمل الملف boot.ini وكيف يمكن الاستفادة منه ؟**

– هو الملف المسئول عن إظهار قائمة أنظمة التشغيل عند بدء التشغيل، هذا الملف يوجد في المجلد الرئيسي للنظام مثلا: c:\boot.iniو يمكن تحريره بأي محرر نصوص مثل المفكرة و ذلك بالذهاب إلى ابدأ ثم تشغيل و كتابة c:\boot.ini ثم موافق، كما يمكن الوصول إليه بالذهاب إلى لوحة التحكم ثم النظام ثم تبويب خيارات متقدمة ثم النقر على الإعدادات في قسم بدء التشغيل و الاسترداد و من ثم النقر على زر : تحرير .

عندما تفتح هذا الملف تجد أنه ينقسم إلى قسمين:

الأول: [boot loader]وفي هذا القسم بارا مترين :

Timeoutوهو المسئول عن تحديد الزمن بالثواني اللازم لتشغيل النظام الافتراضي.

Defaultو هو يحدد النظام الافتراضي الذي يتم تشغيله تلقائيا في حالة عدم اختيار أي نظام من القائمة.

الثاني : [operating system]وهو يحتوي على قائمة أنظمة التشغيل و أسمائها التي تريد أن تظهر في القائمة ، و موقع ملفات النظام على القرص الصلب، و مع خيار نظام التشغيل ويندوز XPتستطيع استخدام مجموعة من المفاتيح أهمها:

/basevideoلتشغيل الويندوز XPباستخدام مشغلات VGAالقياسية و هذا مفيد في حالة أن أردت لفترة مؤقتة تغيير بطاقة العرض و لم تشأ إتعاب نفسك بتغيير الإعدادات كل مرة .

/fastdetectهذا المفتاح يضعه برنامج التنصيب تلقائيا لكي لا يقوم الويندوز بالتعرف على كل أجهزة Plug and Playالتسريع تشغيل الويندوز .XP

/noguibootيمنع ظهور لوحة بدء التشغيل لويندوز .XP

/bootlogيسجل كل خطوات بدء التشغيل في الملف Windows\Nbtlog.txt.

/safebootيشغل الويندوز XPفي نمط الأمان.

/sosيظهر على الشاشة جميع أسماء المشغلات التي يشغلها ويندوز XPعند الإقلاع و هذا مفيد عند الرغبة في استكشاف المشاكل و معرفة الملفات المسئولة عنها..كما يمكن التحكم بخيارات هذا الملف بالذهاب إلى ابدأ ثم تشغيل و كتابة msconfigثم تبويب boot.iniفي النظام . XP

## تعليق سواقة القرص المضغوط

● **محمد منصور**
**mo-mansour@hotmail.com**

*لدي جهاز كمبيوتر عندما أقوم بتشغيل قرص مضغوط فيلمي أو غيره لا يتم الفتح وإن تم الفتح يقف أو يعلق أو يختفي اسم القرص ؟

هناك عدة احتمالات لهذه المشكلة فالاحتمال الأول وجود مشكلة في نفس المحرك أي سواقة الأقراص المضغوطة وعندما يبدأ عمل قراءة في القرص المضغوط يتوقف عن العمل لصعوبة إنجاز المهمة الملقاة على هذا المحرك أما الاحتمال الثاني هو وجود تعارض بين أجزء الكمبيوتر وهذا التعارض قد يكون سبب لتوقف الكمبيوتر عن العمل أما في حالة اختفاء محرك الأقراص المضغوطة ولم يظهر مرة أخرى فتستطيع استعادة بالطريقة التالية : وذلك بالذهاب إلى قائمة ابدأ ثم تشغيل و اكتب الأمر regeditثم قم باختيار حسب المسار و هناك اذهب إلى

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}ثم اذهب إلى مفتاح cdrom و احذف القيم UpperFiltersو/أو LowerFilters اضغط على Winkey+Breakثم اذهب إلى تبويب الجهاز ثم إدارة الأجهزة ثم احذف إدخالات CD Deviceثم قم بإعادة التشغيل .

## وظيفة F8

● **خالد علي الضبيبي - الأمانة**
**kh_007_21@hotmail.com**

● **ماهي وظيفة F8عند إعادة التشغيل ؟**

– عندما تقوم بالضغط على F8عند سماعك لصفارة الكمبيوتر عند النهوض أو بدء الإقلاع فحينها يمكن الضغط على مفتاح F8وسوف تظهر قائمة خيارات تخص النظام الموجود على الكمبيوتر .

## تشغيل اللعبة

● **القارئ/ bestguy5@hotmail.com**

● **كلما أردت لعبة كرة القدم على جهاز الكمبيوتر يقوم الجهاز بالتعليق بعد خمس**

# في أحدث إحصائية لموقع متخصص

# أخطر الفيروسات وشائعاتها خلال شهر فبراير ٢٠٠٥م

في إحصائية أعلنها موقع صوفوس sophos.comالمتخصص في أمن المعلومات ومكافحة الفيروسات لمنشآت الأعمال أظهرت وبالأرقام مدى الانتشار الواسع الذي حققته بعض الفيروسات والديدان، وكذلك نجاح بعض الشائعات في إشاعة الرعب لدى مستخدمي الإنترنت في العالم من فيروسات لا وجود لها، أو بث شائعات مغرضة يقصد منها النيل من شخصيات حقيقية أو اعتبارية، وشائعات أخرى يبتغي وراءها بعض ضعاف النفوس استغلال عواطف الناس أحياناً ومطامعهم أحياناً أخرى في القيام بعمليات نصب واحتيال ومحاولة ابتزازهم. وسنعرض ما ورد في هذه الإحصائية بشكل تفصيلي لا يخلو من الإيضاح لبعض الجوانب الهامة إما لدواعي التحذير أو لغرض التثقيف لتحصين القارئ الكريم ضد أي أخطار محتملة، فالإنسان عدو ما يجهل، ونقص المعلومة يعد أم المشاكل.

## العرض والتحليل:

على مستوى الفيروسات لا تزال دودة W23/Zafi-Dتتربع على قمة قائمة الفيروسات الأكثر انتشاراً ولشهرين متتاليين، حيث بلغت نسبة الإصابة بها ٣٠.٨٪ من إجمالي الإصابة بالفيروسات الأخرى، تلتها W23/Netsky-Pوالتي حققت ما نسبته ٢٢.٣٪ متقدمة على W23/Zafi-Bالتي كانت تتقدمها خلال شهر يناير ٢٠٠٥ فاصبحت بالمركز الثالث بنسبة ٩.٧٪، أما المرتبة الرابعة فقد جاءت من نصيب W23/Bagle-BKوحققت نسبة عالية تقدر بـ ٥.٢٪ مقارنة بتاريخ ظهورها حيث اكتشفت في أواخر يناير ٢٠٠٥م، وهذا مؤشر خطر داهم لهذه الدودة في سرعة انتشارها.

W23/Netsky-Dأما الدودة السابقة فبلغتْ بنسبة الإصابة بها حوالي٤.٢٪ من إجمالي الإصابات، تلتها في المرتبة الخامسة W23/Netsky-Zوالتي بلغت نسبتها ٣.٨٪، وجاءت W23/Sober-Kسابعاً دودة W23/Sober-Kالتي تعد الأسرع انتشاراً من بين فيروسات العام ٢٠٠٥م حيث حققت ما نسبته ٣.٤٪ منذ أول اكتشاف لها في أواخر شهر فبراير ٢٠٠٥م (الشهر الذي شملته هذه الدراسة الإحصائية) وهي نسبة مذهلة تنذر بالمزيد من الخطر القادم، أما المرتبة الثامنة فكانت من نصيب W23/Sobig-Fوالتي لم تحقق سوى ٢.٥٪ وهي نسبة ضئيلة إذا ما قورنت بالفترة التي سبقت بها خلفها W23/Sober-K.

المرتبة التاسعة كانت من نصيب W23/Netsky-Bالتي تأخرت عن المركز الثامن وبنسبة بلغت ٢.٤٪ أما المؤخرة فتحتلها دودة W23/MyDoom-Oبنسبة بسيطة لم تتجاوز ١.٥٪ أما بقية الفيروسات فلم تتجاوز (مجتمعة) ما نسبته ١٤.٢٪

*أما على نطاق شائعات الفيروسات فقد جاءت شائعة Hotmail hoaxفي المرتبة الأولى بنسبة مرتفعة جداً بلغت ٣٦.٨٪، هذه الشائعة تأتي على هيئة رسالة (مستعجلة) لمستخدمي بريد الهوتميل تطلب من المرسل إليه إرسالها إلى عشرة أشخاص لمعرفة الأشخاص الذين يستخدمون بريدهم بشكل نشيط وحذف الحسابات الخاملة، وتتضمن تهديداً بأنه إذا لم توزع هذه الرسالة خلال ٤٨ ساعة للعدد المطلوب سيتم إلغاء بريد المرسل إليه. وهي من الشائعات القديمة نسبياً ولكن صيغتها قد ساهمت في زيادة انتشارها خصوصاً بين أوساط المستخدمين قليلي الخبرة.

أما المرتبة الثانية فجاءت بها شائعة Bonsai kittenالتي بثت على هيئة احتجاج ضد أحد المواقع بدعوى إساءة معاملة القطط.. وبلغت نسبة انتشار هذه الشائعة ١٠.٦٪، أما الشائعة الثالثة Meninas da Playboyفقد انتشرت بالبرتغال تضمنت رسالة باللغة البرتغالية تشير إلى فيروس أعلنت عن اكتشافه شركة مايكروسوفت وأن الشركات المتخصصة مثل مكافي ونورتن لم تتوصل حتى تاريخ الرسالة لاكتشاف علاج أو وقاية منه. وتطلب الرسالة إعادة إرسال هذا التحذير إلى الأصدقاء.

المرتبة الرابعة جاءت بها الشائعة التي انطلقت قبيل البدء باحتفالات الميلاد ورأس السنة والتي تسمى شائعة Virtual Card for Youوالتي انطلقت بعدة إصدارات مختلفة، أبرزها الرسالة التي تدعي اكتشاف فيروس جديد انتشر في نيويورك ياتي على شكل رسالة بعنوان: Virtual Card for Youبمجرد أن يفتح المستخدم البطاقة يتصلب الجهاز ولا يستجيب إلى أية أوامر تصدر له بعدها، وبعد أن يقوم المستخدم بإعادة التشغيل باستخدام الأزرار Alt + Ctrl + Deleteيقوم الفيروس بإتلاف القرص الصلب بشكل نهائي. وأن هذا الخبر قد بث نقلاً عن محطة السي إن إن الأمريكية، وفي النهاية تطلب من المستقبل تمرير التحذير لكل الأصدقاء. هذه الشائعة انتشرت بشكل سريع قدرت نسبته بـ ٢.٨٪

المركز الخامس احتلته شائعة Letter from tsunami victimوهي من نوع شائعات (الغش والنصب) يدعي كاتبها أنه أصيب بمرض عضال في المريء وأن لديه ثروة طائلة يريد أن يتبرع بها لحساب مستقبل الرسالة ليقوم هو بدوره بالعمل على توزيعها على الفقراء والمحتاجين لتكون آخر الأعمال الصالحة التي يقصد بها وجه الله تعالى خاصة وأنه لم يعد في العمر متسع ولا يمكنه أن يقوم بهذه الأعمال بنفسه. بلغت نسبة انتشار هذه الشائعة ٢.٨٪

الخامس مكرر شائعة Unidentified tsunami boy والتي تتكون من رسالة مرفق بها صورة بحجم ١ ميجابايت تفيد الرسالة أن صاحب الصورة طفل مجهول يعتقد أنه من ضحايا كارثة تسونامي ويطلب من المستقبل أن يقوم ببثها إلى جميع من يعرف ويقصد من هذه الشائعة – والتي بلغت نسبة أنتشارها ٢.٨ - ؟إحداث انهيارات لمواقع خدمة البريد الإلكتروني المشهورة عندما يتم تبادل هذه الشائعة التي تتضمن هذا الملف الكبير.

● الشائعة السابعة في الترتيب شائعة Budweiser frogs screensaverوهي من شائعات الفيروسات بلغت نسبتها ٢.٥٪، وهي من الشائعات المضادة، فشركة Budweiserهي إحدى الشركات المشهورة في إنتاج البيرة كانت قد صنعت شاشة توقف دعائية للترويج لمنتجاتها وجعلت هذا الملف متاحاً للتحميل من موقعها على الإنترنت، فجاءت هذه الشائعة لتنذر الآخرين من الضرر الكبير الذي سيترتب على تحميلها والذي قد يصل إلى فقدان جميع البيانات وتلف القرص الصلب.

المرتبة الثامنة احتلتها شائعة Applebees Gift Certificateبمعدل انتشار بلغ ٢.٣٪، هذه الشائعة من فئة (الغش) ويدعي كاتب الرسالة أن اسمه بيل بالمر مؤسس Applebees، وأنه قرر منح خمسين دولاراً كجائزة تشجيعية لأي شخص يقوم بإعادة إرسال هذه الرسالة لتسعة أشخاص آخرين.

● الشائعة التاسعة في الترتيب هي شائعة Yahoo instant messageبلغت نسبتها في الانتشار ما يعادل ٢.٢٪، وهي من نوع شائعات الفيروسات، وهي عبارة عن رسالة تحذيرية من شخص يحاول طلب الانتماء لمجموعة (مستقبل الرسالة) بمسمى dvorak@yahoo.com والرسالة تحذر من قبول استضافته لأنه بمجرد أن يتم قبوله يقوم بتدمير القرص الصلب، ويطلب من المستقبل أن يبث هذا التحذير إلى كل معارفه سواء في قائمة الماسنجر أو عناوين البريد الإلكتروني.

الشائعة الأخيرة هي Jamie Bulger، وهي من شائعات (الغش والنصب)، إذ قدر معدل انتشارها بما يوازي ١.٥٪، وهي عبارة عن رسالة تحكي ماساة (لا وجود لها) تعرض لها أحد الأطفال ويدعى Jamie Bulgerالذي خطف من أمه واوذي جسدياً وموورست معه بعض الأفعال الأخلاقية ثم ربط على وضع على سكة قطار ليسحقه وتصبح القضية كأنها حادث مروري عابر. الرسالة تطالب المستقبل بضرورة بثها والتوقيع لإيقاع العقوبة فيمن ارتكب هذه الجريمة ضد الطفل جيمي..أما بقية الشائعات الأخرى (مجتمعة) فقد استطاعت تحقيق انتشار بلغت نسبته ٢٤.٠٪

## التعليق:

إن النسب الواردة في ثنايا هذا التقرير بجزأيه وإن كانت بسيطة قد يرى البعض أنه ليس من المهم استعراضها خصوصاً التي جاءت نسبتها أقل من ٢٪، وهذا اعتقاد خاطئ لسببين: الأول هو أن هذه النسبة الضئيلة لا تعبر عن ١٠ أشخاص أو مئة أو ألف ولا حتى مليون، بل إنها تتجاوز إلى مئات الملايين.. ولكم أن تتخيلوا لو أن مستخدمي الإنترنت ١٠٠ مليون فكم سيكون الواحد بالمائة من هذا العدد؟! مليون مستخدم.. فهل هذه نسبة بسيطة؟ السبب الثاني، عامل الزمن.. فهذه الإحصائية تعبر عن شهر واحد وهذه الأعداد تعتبر كبيرة خلال هذه الفترة.. خاصة إذا علمنا أن بعض الفيروسات لم يمض على اكتشافه سوى أيام ويقفز للمرتبة الثالثة أو الرابعة.. أعتقد أن هذه النسبة تعد رقماً قياسياً.

تنبيه مهم:

كنت أهم بكتابة موضوع يعالج الرسائل البريدية التي تتضمن شائعات (النصب) التي تصل لبعض المستخدمين لمحاولة استمالة عواطفهم أو إثارة مطامعهم للحصول على مبالغ زهيدة منهم مقابل استلام وصاية على ثروات (لا وجود لها) وأن هذه المبالغ توجه لمقابلة بعض المصاريف الإدارية ككتابة الوكالة وخلافه. وقد يتساءل أحد الأذكياء.. لماذا يطالبني بهذا المبلغ وهو يمتلك كل هذه الثروة، فسيصل الرد على لسان (المحامي) بأن هذا المبلغ البسيط للتأكد من جدية المتقدم.

لذلك ينبغي على المستخدم الكريم أن يكون حذراً بحيث يقوم بإهمال أي رسائل ترد من هذا النوع، وبالنسبة للفيروسات يجب أن يستقي معلوماته حولها عن طريق مواقع الحماية الموثوقة كمثل مواقع Sophos.comو McAfee.comو Norton.comوغيرها من المواقع المعروفة حتى يتخلص من أي محاولات خداع قد تنتهي به إلى إلحاق الضرر بنفسه أو بمن حوله، خصوصاً وأن بعض هذه الشائعات تطلب من المستخدم البحث عن ملف وحذفه على أنه فيروس، وهو في الحقيقة أحد ملفات النظام.

**إعداد - خالد المسيهيج:**
almusaihij@alriyadh.com