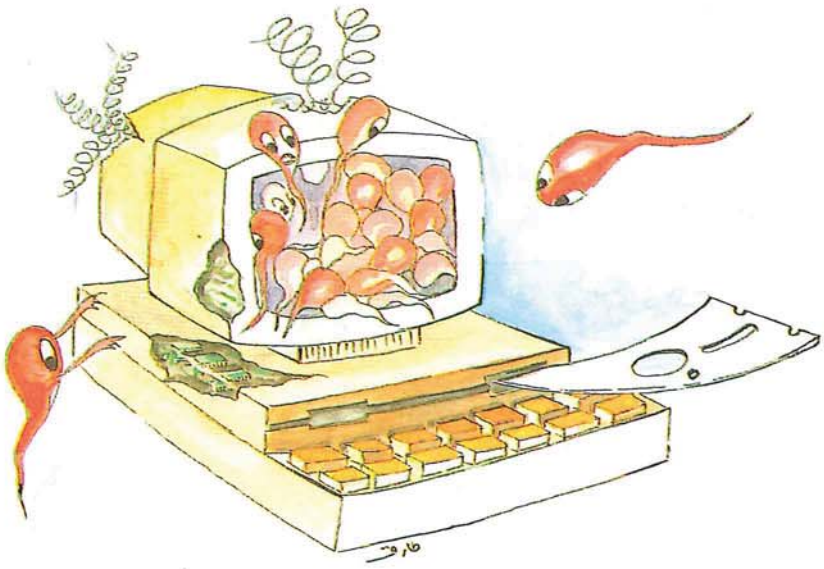
فيروسات الحاسب في المملكة العربية السعودية

د.محمد صالح بنتن

يتسع نطاق مستخدمي الحاسب الآلي في المملكة العربيةالسعودية ليشمل الأفراد واستخداماتهم الخاصة للحاسب سواء في المنزل أو المكتب إما لتحرير النصوص أو لإجراء الحسابات الشخصية أو قد يكون أحيانا للترفيه.كما ينتشر إستخدام الحاسب في الشركات والمؤسسات الخاصة وفي القطاع الحكومي أيضا إما كأداة ثانوية أو كجزء مهم لايمكن الإستغناء عنه. ويبدو جليا أن استخدام الحاسب في المملكة العربية السعودية في زيادة مضطردة وذلك للحاجة لميكنة الأعمال التي يمكن ميكنتها لتوفير الأيدي العاملة التي تقل في هذا المجتمع.



يتم استغلال الحاسب في المملكة كوسيلة لإجراء العمليات الحسابية بسرعة فائقة، كما يتم استخدامه كخِزانات آمنة لتخزين الكثير من المعلومات المهمة والحساسة، كذلك يستخدم الحاسب الألي في حالات كثيرة في المساعدة على إتخاذ القرارات التي قد تؤثر على كثير من الأحداث اليومية، ولهذا يجب علينا أن نحمي الحاسب الآلي من الأيدي العابثة. ومع إنتشار البرامج التي يطلق عليها برامج الفيروسات والتي بدأت تنتشر بسرعة فائقة بهدف التدمير والتخريب، يجب علينا أن نتعرف على هذه البرامج وطريقة عملها وطرق إبطال مفعولها حتى نتمكن من تجنب عواقبها الضارة.

يطلق إسم فيروس الحاسب على بعض برامج الحاسب التي لها بعض الخصائص التي تشبه خصائص الفيروسات الأحيائية مثل إصابتها لخلايا الكائنات الحية وإتلافها وانتقالها إلى الخلايا المجاورة. ففيروس الحاسب عبارة عن برنامج يقوم بمهاجمة وإتلاف برامج معينة في الحاسب والإنتقال إلى برامج أخرى عند تشغيل البرنامج المصاب والتلاعب بالمعلومات المخزنة في الحاسب آنذاك، وقد تصبح في بعض الأحيان إستمرارية إستخدام الحاسب مستحيلة حيث أنه كلما تم إسترجاع المعلومات التالفة من الذاكرة إلى الحاسب، يقوم الفيروس بالعبث بها من حين إلى أخر. هناك أيضا حالات أخرى غير العبث بالمعلومات قد يصاب بها الحاسب نتيجة للإصابة بفيروس الحاسب ومنها الشلل، ففي هذه الحالة يتوقف الحاسب عن العمل كلما تم تشغيل أحد البرامج المصابة، كما أن هناك بعض أنواع الفيروسات تقوم بإشعار المستخدم بأن هناك مشاكل وأعطال فنية بالحاسب ويجب إصلاحه.

أنواع الفيروسات وتأثيرها

يمكن تصنيف الفيروسات إلى أنواع مختلفة حسب تأثيرها على الحاسبات كما يلي:-

١ ـ الفيروسات البسيطة

يقتصر عمل هذا النوع من الفيروسات على إزعاج مستخدم الحاسب دون المساس بأمن المعلومات أو البرامج، وفي كثير من الأحيان يمكن التخلص من هذه الفيروسات بصورة سهلة ونهائية من الحاسب.

٢ ـ الفيروسات المزعجة

هذا النوع من الفيروسات أكثر إزعاجا للمستخدم ولايمكن التخلص منها بسهولة، وكلما ظن المستخدم بأنه قد تخلص منها ظهرت أعراض الإصابة بها مرة أخرى.

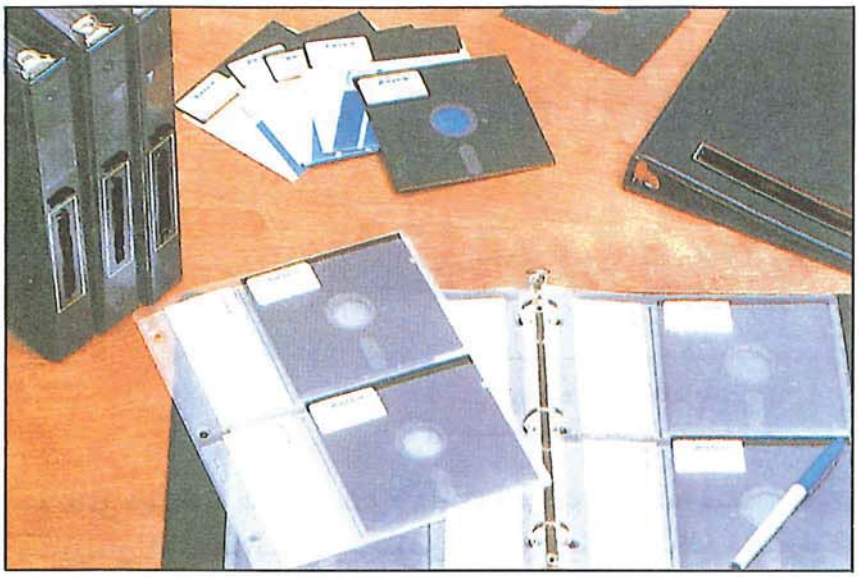
٣ ـ الفيروسات القاتلة

هذا النوع من الفيروسات يتخصص في التخريب والعبث بالمعلومات، وتنقسم هذه الفيروسات إلى قسمين، قسم يمكن التخلص منه واسترجاع جزء من المعلومات، وقسم آخر لايمكن التخلص منه أبداً إلا بعد الدمار الشامل لكل المعلومات التي كانت في الحاسب وقت الإصابة .

يمكن أن تكون جميع أنواع الفيروسات آنفة الذكر موقوته بحيث أنها تعمل بعد وقت معين أو في يوم معين. لذا يجب الحيطة والحذر عند التعامل مع برامج الحاسبات لحمايتها ووقايتها من الإصابة بتلك الفيروسات تجنبا للمشاكل التي قد تنجم عن تلف المعلومات والسجلات .

مصادر فيروسات الحاسب

هناك عدة نظريات عن مصادر فيروسات الحاسب، ويرى البعض أن أحد تلك المصادر يتمثل في الأشخاص الذين يجيدون فن البرمجة حيث يضعون من باب «الدعابة» بعض البرامج المؤذية في الحاسبات، وقد نمت هذه المهارات لدى المبرمجين والمستخدمين فطوروها إلى برامج تنقل العدوى إلى برامج أخرى. ويرى آخرون أن الفيروسات قد بدأت من بعض المبرمجين المتمكنين الذين كانوا يقومون بحماية برامجهم من النَسخ غير المشروع



● برامج الحاسبات مصدر الفيروسات .

عن طريق كتابة برامج تخريبية. هذا ويمكن إرجاع مصادر فيروسات الحاسب عموما إلى أربعة مصادر رئيسة هي:ـ

١ ـ البرامج غير المملوكة والتي يمكن تبادلها بدون مقابل.

٢ ـ البرامج غير الشرعية (غير الأصلية) وغير معروفة المصدر.

٣ ـ الإرتباط مع شبكات الربط العالمية .

٤ ـ المتعاونون والمتواطئون والدخلاء.

فيروسات الحاسب في المملكة

تشير الإحصائيات التي تم الحصول عليها من معامل الحاسبات الشخصية في بعض الجامعات السعودية وأماكن بيع برامج الحاسبات الشخصية بأن هناك ما يزيد عن المائة نوع من الفيروسات التي تصيب الأجهزة المكافئة لأجهزة IBM والتي تعمل بنظام (MS-DOS)، وتختلف هذه الفيروسات في طريقة عملها من فيروسات بسيطة إلى فيروسات قاتلة. وهناك نوع آخر من الفيروسات يصيب حاسبات الماكنتوش تم حصر ما بين خمسة إلى عشرة منها في معامل الجامعات وفي وكالة شركة ابل لبيع حاسبات الماكنتوش.

وتجدر الاشارة إلى أن هناك حاسبات كبيرة في المملكة العربية السعودية تعمل بنظام (IBM VM) ونظام (IBM MVS) تفيد المعلومات بأن مثيلاتها في الدول الغربية قد أصيبت بأنواع من الفيروسات. الا إننا لانستطيع أن نثبت أو ننفي إصابة الأنواع الموجودة في المملكة بتلك الفيروسات كما أن حاسبات المملكة التي تعمل بنظام (UNIX) ونظام (VMS) قد تكون عرضة للفيروسات التي تعرضت لها مثيلاتها في الدول الغربية.

مصادر الفيروسات في المملكة

يمكن إرجاع مصادر فيروسات الحاسب في المملكة العربية السعودية إلى ثلاثة مصادر هي:ـ

١ ـ البرامج غير المشروعة وغير معروفة المصدر، وهي ما يتم تبادلها عادة بين الأصدقاء والغرباء أو شراؤها بأسعار زهيدة من أماكن بيع البرامج والحاسبات الشخصية المنتشرة في أنحاء المملكة. وتشكّل هذه البرامج خطرا على أمن المعلومات خصوصا وأن الحاسبات المقصودة هنا هي الأجهزة التي تعمل بنظام (MS-DOS) والتي تمثل الجزء الأكبر من الحاسبات العاملة في المملكة. ونظراً لرخص أسعار هذه الحاسبات وتوفر الكم الهائل من البرامج المتقدمة والمفيدة التي تعمل عليها،

فإن كثيرا من الأشخاص يستخدمون هذه الأجهزة في أماكن عملهم للأعمال الرسمية وفي منازلهم للإستخدام الشخصي. وحتى لو إقتصر استخدام البرامج الأصلية والشرعية في قطاع العمل، فإن الأشخاص عادة مايقومون بنقل أو تجربة برامجهم الشخصية في أماكن عملهم وبهذا فإن أي إصابة للحاسب الشخصي يمكن أن تنتقل إلى الحاسبات في الشركات والقطاعات الحكومية المختلفة. ولهذا يجب منع استخدام البرامج الخاصة وتبادل المعلومات بين الحاسبات في قطاع العمل منعا باتاً وشرح الأسباب للعاملين على هذه الأجهزة حتى يتم تفهمهم للمشكلة وتعاونهم في هذا الصدد.

٢ ـ شبكات الربط العالمية، مثل (BITNET) وشبكات الإتصال التليفونية العامة (BBS)، ففي التعامل مع هذه الشبكات يتم تبادل بعض البرامج التي قد تكون حاملة وملوثة بفيروسات الحاسب، ويجب أخذ الحذر من التعامل مع مثل تلك الشبكات وعدم تبادل البرامج عن طريقها.

٣ ـ المتعاونون والدخلاء، وقد يقوم هؤلاء بغرس فيروسات في البرامج التي يطورونها كجزء من عملهم وذلك لحماية أنفسهم في حالة تهديد مستقبل عملهم أو طردهم من أعمالهم. لهذا يجب مراقبة العاملين في مجال البرمجة وإدارة مراكز الحاسبات الآلية والتعاون معهم بثقة حذرة وعدم الإعتماد كلية على شخص واحد فقط، بل التأكد من أن مجموعة من الأشخاص تقوم بالأعمال الخاصة بإدارة مراكز المعلومات. وهذا سبب كاف للتنبيه على ضرورة الإهتمام بموضوع أمن المعلومات في المملكة العربية السعودية وأخذه مأخذ الجد في كل الأحيان وتثقيف المستخدمين بمخاطر عصر الحاسب الآلي.

فيروسات نظام (DOS - MS)

كما سبق أن ذكرنا بأن الفيروسات عبارة عن برامج كتبت لكي تصيب برامج تشغيل أخرى، لذلك فهي دائما تصيب الملفات التي تنتهي بالكلمات (EXE;COM;BAT). كما أنها تصيب البرامج التي يتم تحميلها وقت التشغيل مثل تلك التي تنتهي بالكلمة (OVL) حيث أن مثل هذه الملفات المصابة تسمى بالبرامج الحاملة للفيروس و يمكن أن تنقل فيروس الحاسب إلى غيرها من البرامج عند تشغيلها. كما أن الملفات الخاصة بنظام التشغيل والتي لا تظهر في دليل الملفات ولا يراها المستخدم يمكن أن تكون حاملة للفيروس. وتتميز البرامج الحاملة للفيروسات بكونها برامج عادية يعتقد المستخدم بأنها تؤدي وظيفة معينة، ولكنها في الحقيقة ملوثة ولا تؤدي وظيفتها الأصلية. ويمكن تصنيف التركيبة البنائية للبرامج المصابة والحاملة لفيروس الحاسب وتقسيمها إلى ثلاثة أقسام:ـ

١ ـ قسم نواة الفيروس (قسم العدوى).
٢ ـ قسم مهام الفيروس (قسم التخريب).
٣ ـ الجزء الأصلي للبرنامج.

كما أنه يمكن إحتساب قسم رابع في تركيبة البرامج المصابة، وهو قسم العلامة المميزة، وهو قسم يساعد نواة الفيروس للتعرف على البرامج الحاملة للفيروس لتجنب إعادة نقل الفيروس إليها مرة ثانية. وهو عادة ما يحتوي على كلمة خاصة يتم وضعها في مكان معين في البرامج المصابة.ويمكن الإستغناء عن هذا القسم بالتعرف على نواة الفيروس أو على قسم المهام أو على كليهما معا.

إنتشار الفيروسات

عندما يتم تشغيل برنامج ملوث بأحد الفيروسات، يقوم هذا البرنامج بالبحث عن برامج غير ملوثة بالفيروس وذلك بفحص البرامج التي تنتهي بـ COM أوEXE والمخزنة على الإسطوانات التابعة للحاسب. وفي حالة العثور على برنامج مناسب يتم تعديله بنقل نواة الفيروس وقسم المهام إلى ذلك البرنامج، بحيث يتم تشغيل نواة الفيروس عند تشغيل البرنامج المعدل. وتتم عملية نقل الفيروس وتعديل البرامج بإحدى طريقتين، هما:ـ

١ ـ عن طريق الطمس وإعادة الكتابة على الجزء الأول من البرنامج الفريسة.
٢ ـ عن طريق الإضافة ،وفي هذه الحالة يتم إضافة نواة الفيروس إلى البرنامج الفريسة كإضافة تسبق الجزء الأصلي للبرنامج. وبعد إتمام عملية التلويث ونقل الفيروس، تبدأ مهمة المعالجة والتي يقوم الفيروس من خلالها محاولا العبث بالمعلومات كما هو مخططا له.

الوقاية من الفيروسات

يمكن منع وصول الفيروسات والحماية منها بتثقيف العاملين في مجال الحاسب وحثهم على الحذر وأخذ الحيطة من مثل تلك البرامج. ويمكننا تلخيص طرق الحماية ومنع إنتشار الفيروسات في كثير من الأحيان باتباع النقاط التالية:ـ

- عدم إستخدام البرامج الحرة والتي يمكن الحصول عليها مجاناً عن طريق شبكات الربط والشبكات التليفونية.
- عدم إستخدام البرامج غير معروفة المصدر.
- عدم إستخدام البرامج غير الأصلية.
- إستخدام شريط الحماية ضد الكتابة على القريصات المغناطيسية المشبوهة.
- تحديد تبادل القريصات ودخول الغرباء إلى أماكن الحاسبات الآلية.
- عدم إستخدام القريصات المغناطيسية الشخصية في أماكن العمل أو العكس.
- فحص ملفات النظام غير المرئية بوساطة البرامج الخاصة بالكشف عن الفيروسات.
- إجراء عمليات تخزين المعلومات في الأرشيف بصورة دورية.
- تعليم وتثقيف الأفراد بمخاطر الفيروسات وما قد تسببه للمجتمع.
- عدم الإعتماد على شخص واحد لإدارة مراكز المعلومات.