مقدمة إلى المعلومات

شهادة كامبردج الدولية في مهارات المعلومات CIT

مدرب الدورة : د. زياد الحلايبه

الفصل الأول لعام ٣٤-١٤٣٥ هـ

القسم الخامس: أمن المعلومات

الدرس ١ : أن تكون استباقيا

الدرس ٢ : التعريف بنفسك

الدرس ٣ : حماية البيانات

الدرس ٤ : التعرف على البرامج الضارة

الدرس ٥ : الوقاية من البرامج الضارة

أن تكون استباقيا

أفضل سياسات أمن الحاسب الآلي هي التي يترتب عليها كلاً من التدابير الأمنية الإستباقية والتفاعلية ، في هذا الفصل ستتم مناقشة مايلي :

- ✓ أن تكون استباقيا فيما يتعلق بأمن الحاسب .
- ✓ شبكة الاتصال .
- ✓ سياسات الأمن الأساسي لنظام الحاسب .
- ✓ كيفية إعداد إجراءات حالة وجود خرق للحماية .
- ✓ بعض الأمور التي يمكن للموظفين والإداريين القيام بها لتحسين الوضع الأمني .

أن تكون استباقيا(مزايا أن تكون استباقيا)

الخطة الأمنية الجيدة تشمل التدابير الأمنية الإستباقية ، لذا الأمن ألاستباقي لديه بعض المزايا الواضحة والتي تجعل منه جزءا أساسيا في أية خطة أمنية ، ومنها مايلي :

- ✓ التدابير الأمنية الإستباقية تمنع الاختراقات .
- ✓ الحد من التعرض العام للتهديدات الأمنية .
- ✓ توفر استجابات ذكية معدة ومخطط لها في حال تم الاختراق .

أن تكون استباقيا(السياسات الأمنية)

السياسة الأمنية عبارة عن بيان التوجيهات التي تحدد كيفية الحفاظ على الأمن في مؤسسة معينة ، وتعتبر حماية البيانات الحساسة صميم أمن الحاسب . لذا ينبغي أن تشمل سياسة الأمن النقاط التالية :

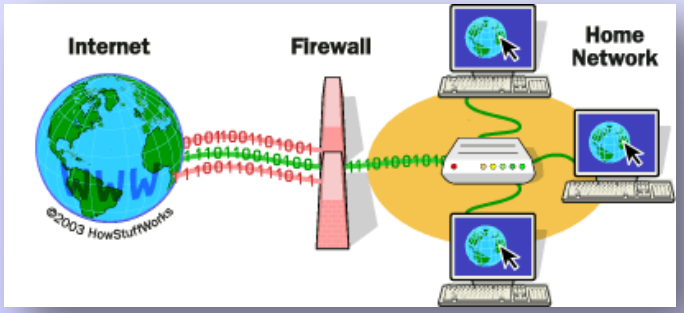
١. تنزيل وتثبيت البرامج المصرح بها بانتظام .

تنشأ العديد من الهجمات من خلال استغلال الثغرات في برمجيات الحاسب . لذا تأكد من أنك تستخدم التحديثات المقدمة من قبل مصنعي البرمجيات ، وبذلك ستقلل الفرص المتاحة لدى المخترقين .

تابع: أن تكون استباقيا(السياسات الأمنية)

٢. فحص الأمان والتشفير اللاسلكي .

في حالة تشغيل الشبكة اللاسلكية يجب التأكد من استخدام عناصر الأمن أو التشفير الأقوى المتوفر في معدات الاتصال اللاسلكي ، وذلك لأنها تعتبر أسهل أنواع الاختراقات لشبكات الحاسب .



٣. استخدام جدار الحماية **Firewall** .

استخدام جدار الحماية يوفر أقصى درجات التحكم بتدفق المعلومات من شبكة الانترنت العامة إلى الحاسب الشخصي أو شبكة حواسيب العمل الجماعي .

تابع: أن تكون استباقيا(السياسات الأمنية)

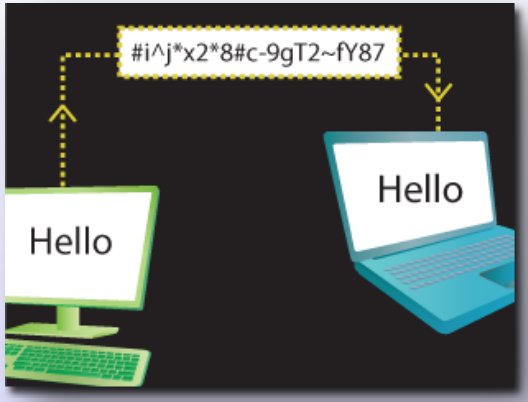
٤. استخدام نظام كشف الاختراق **IDS** .

في برمجيات نظام الاختراق **IDS** يمكن الكشف عن محاولات اختراق أمن شبكة الحواسيب وتنبيه المسؤولين عنها .

٥. تحديد سياسة البريد الالكتروني **E-mail**.

يجب على سياسة الاستخدام المقبول للبريد الالكتروني تحديد منهج المؤسسة أو الفرد في التعامل مع مرفقات البريد الالكتروني (**إرسال واستقبال**) .

تابع: أن تكون استباقيا(السياسات الأمنية)



٦. استخدام التشفير عند نقل البيانات عبر الانترنت .

عند نقل المعلومات الحساسة عبر شبكة الانترنت العامة يمكن استخدام التشفير لجعل البيانات غير قابلة للقراءة .

٧. تشفير البيانات الحساسة عند التخزين .

عند تخزين بيانات هامة وحساسة على جهاز الحاسب يجب حفظها على هيئة ملفات مشفرة لمنع قراءتها ومعرفتها في حالة سرقة الجهاز .

تابع: أن تكون استباقيا(السياسات الأمنية)

٨. عمل نسخ احتياطية من البيانات الهامة باستمرار .

أن تكون لديك إجراءات لعمل نسخ احتياطية **Backup** للبيانات الهامة وأرشفتها بعيدا عن جهاز الحاسب تكون مهمة للغاية في حالة سرقة الجهاز أو فقدانها نتيجة الحوادث الغير متوقعة كالحريق أو الزلازل ... الخ .

٩. استخدام برامج مكافحة الفيروسات .

تثبيت برامج مكافحة الفيروسات وإعداد جدول بأوقات منتظمة لاكتشاف الفيروسات والتخلص منها .

تابع: أن تكون استباقيا(السياسات الأمنية)

١٠. تحديد سياسة للتحكم بالأجهزة المحمولة .

يجب تحديد إجراءات نقل الأجهزة المحمولة من وإلى شبكة الاتصال الآمنة ، وذلك لأنها قد تصيب أجهزة الحاسب على الشبكة (إذا كان الجهاز المحمول يحتوي على فيروس) .

١١. تثقيف المستخدمين .

يجب تثقيف المستخدمين حول الاحتيال الذي يهدف للحصول على البيانات الحساسة وبشأن اختيار كلمة المرور القوية والبرامج التي يمكن تثبيتها من مصادر موثوقة .

أن تكون استباقيا(الإجراءات المتعلقة بالاختراقات الأمنية)

الاختراق الأمني هو الدخول الغير مصرح به أو اقتناء معلومات الكترونية تمت سرقتها وتغيير أو تبديل البيانات المهمة أو الشخصية للأغراض الضارة .

وبشكل عام يوجد العديد من الأسباب التي تحدث الاختراق الأمني وهي كالتالي :

- ✓ حاسب محمول يحتوي على معلومات شخصية تمت سرقته .
- ✓ اختيار كلمة مرور ضعيفة يسهل تخمينها .
- ✓ استخدام شبكة **الواي فاي** التشفير الضعيف أو المعدوم نهائي .
- ✓ سرقة المعلومات داخليا من قبل شخص ما مع الوصول إلى النظام .

تابع : أن تكون استباقيا(الإجراءات المتعلقة بالاختراقات الأمنية)

أياً كان سبب الاختراق الأمني ، يجب أن تكون السياسات والإجراءات متوفرة بالفعل للتعامل مع الاختراق الأمني بطريقة ذكية ويمكن أن تشمل على ما يلي :

- ✓ اكتشاف الاختراق الأمني .
- ✓ منع دخول غير المصرح له على نظام المعلومات .
- ✓ إيجاد الثغرة الأمنية التي تم اختراقها والقيام بإصلاحها .
- ✓ تقييم دقيق جدا إلى نوع المعلومات المخترقة .
- ✓ تنبيه المسؤولين والمنظمات اللازمة مثل الشرطة .
- ✓ إشعار الأفراد بالمعلومات المتعلقة بهم لاتخاذ التدابير اللازمة .
- ✓ إعادة تثقيف الموظفين لتجنب أحداث مماثلة في المستقبل .

أن تكون استباقيا(ماذا يمكن للموظفين القيام به)

بصفتك موظفاً ومستخدم للكمبيوتر ، هناك العديد من الأمور التي يمكنك القيام بها ، للحفاظ على أمن المؤسسة وهي كما يلي :

- ✓ تأكد من أن تكون على دراية جيدة بسياسات أمن المعلومات .
- ✓ عليك أن تكون حذراً عند امتلاك الأجهزة المتنقلة معك من وإلى العمل .
- ✓ لا تقم بالكشف لأي شخص عن كلمات المرور مهما كانت الأسباب .
- ✓ اختيار كلمة مرور قوية بحيث يصعب تخمينها .

أن تكون استباقيا(ماذا يمكن للمسؤولين القيام به)

يجب على مسؤولي الشبكة إدراك أهمية الأمن ألاستباقي وبذل كل ما في وسعهم لمنع الاختراقات والهجمات الأمنية وذلك من خلال ما يلي :

- ✓ إنشاء سياسات أمنية وتثقيف المستخدمين حول هذه السياسات .
- ✓ ضمان تمكن المستخدمين إتباع السياسات بأفضل المهارات .
- ✓ المحافظة على جدران الحماية ، والتشفير ، والبرامج المضادة للفيروسات ، وأنظمة كشف التسلل .
- ✓ افتراض انه سيتم اختراق الشبكة وتطوير سياسة الأمن .
- ✓ تصحيح كافة الثغرات المعروفة في برنامج شبكة الاتصال .
- ✓ تثقيف الموظفين حول أهمية اختيار كلمات مرور قوية .
- ✓ تثقيف أنفسهم حول أحدث التهديدات الأمنية المتطورة وطرق الوقاية .

القسم الخامس: أمن المعلومات

الدرس ١ : أن تكون استباقيا

الدرس ٢ : التعريف بنفسك

الدرس ٣ : حماية البيانات

الدرس ٤ : التعرف على البرامج الضارة

الدرس ٥ : الوقاية من البرامج الضارة

التعريف بنفسك

ما هي هوية تعريف المستخدم ؟

هي سلسلة من الأحرف التي تستخدم لتمييز مستخدم واحد عن غيره على نظام الكمبيوتر وهذا هو ما يعرف باسم المستخدم **User Name** .

تستخدم غالبا أسماء المستخدمين بالاشتراك مع كلمات المرور لتسجيل الدخول إلى نظام محدد .

أسماء المستخدمين غالبا تتكون من الأحرف (مثل اسم شخص) ويسهل معرفتها أو تخمينها ولهذه الأسباب اسم المستخدم لا بديل عنه لأنه من خلاله يتم تحديد هوية الشخص على أنظمة الحاسب ويكون مرئي علناً على النظام .

التعريف بنفسك(ما المقصود بكلمة المرور)

تعتبر كلمة المرور عنصرا رئيسا في أمن معلومات نظام الحاسب ، وللوصول إلى نظام محمي يجب على المستخدم إدخال كلمة المرور صحيحة وصالحة للوصول إلى النظام . وفي العادة إذا كانت كلمة المرور صحيحة وتتوافق مع اسم المستخدم يحصل المستخدم على تصريح الوصول إلى النظام .

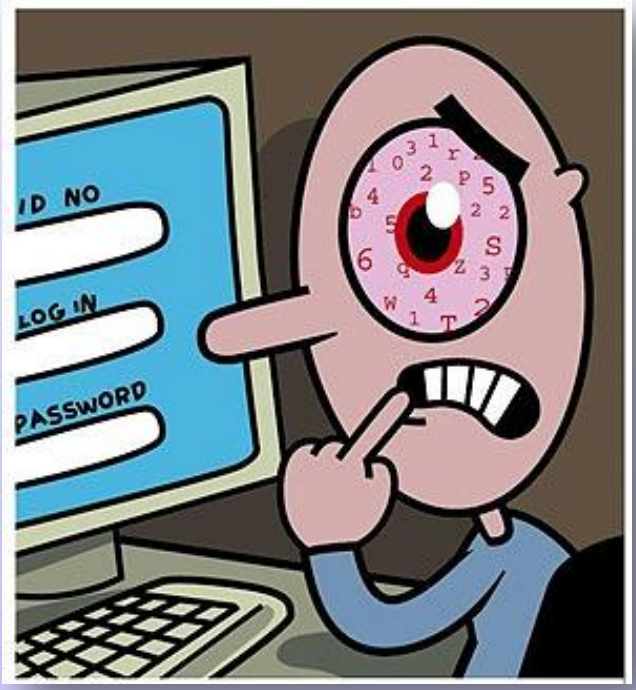
باعتبار كلمة المرور غاية في الأهمية بالنسبة لأمن نظام الحاسب يجب اختيارها بتفكير جيد بحيث يصعب تخمينها .

التعريف بنفسك(اختيار كلمة المرور)

تعتبر كلمة المرور هي خطك الدفاعي الأول ضد مجرمي الإنترنت لذا يجب تحسين اختيار كلمات المرور الخاصة بنا، ومن المُشَجِّع أننا إذا قمنا باختيار كلمات مرور مثل **Pa$$word1** ذات المستوى العالي من الصعوبة، لكن ما قد يسبب فشل الحماية هو تكرار استخدام كلمات السر على نطاق واسع، حتى وإن كانت صعبة مثل ما تم ذكره ، وكلمة المرور القوية تستغرق وقتاً طويلاً – جداً – للتعرف عليها أو فهمها .

تابع : التعريف بنفسك(اختيار كلمة المرور)

اتبع النصائح التالية لإنشاء كلمة مرور قوية :



- أن تحتوي على الأقل على ستة أحرف (الأكثر يكون أفضل) .
- استخدام الأرقام والرموز والأحرف الصغيرة والكبيرة باللغة الانجليزية .
- تجنب استخدام أسماء الأشخاص .
- استخدام كلمة مرور فريدة لكل حساب من الحسابات المهمة .
- تغيير كلمة المرور باستمرار .
- الاحتفاظ بكلمات المرور في مكان سري لا تسهل رؤيته .

التعريف بنفسك(الوصول Access)

الوصول إلى البيانات المخزنة في أجهزة الحاسوب من قبل أشخاص غير شرعيين ليس بالأمر السهل ، وذلك لان الوصول لا يتم بشكل مباشر وإنما عن طريق عدد من الخطوات للتحكم بعمليات الوصول Access Control ومنها ما يلي :

١. إدخال كلمات العبور User Password : كلمات العبور عبارة عن تشكيلة من الأرقام والأحرف يختارها المستخدم ويحتفظ بها ولا يطلع احد عليها.

٢. إدخال دليل تأكيدي User Authentication : هذا الدليل يمكن ان يكون بطاقة ذكية أو توقيعاً أو صوت المستخدم، وذلك للتأكد من هوية المستخدم المسموح له بالدخول للجهاز.

٣. استخدام الصلاحيات User Authorization: يتمتع المستخدمون بصلاحيات محددة للتعامل مع البيانات المخزنة. فمثلاً يتمتع البعض بصلاحية قراءة البيانات فقط، بينما يمكن لشخص آخر القراءة والتعديل على هذه البيانات.إلا أن تنفيذ هذه الخطوات لا يعني منع الوصول للبيانات أو حماية هذه البيانات من مرتكبي جرائم الحاسوب.

القسم الخامس: أمن المعلومات

الدرس ١ : أن تكون استباقيا

الدرس ٢ : التعريف بنفسك

الدرس ٣ : حماية البيانات

الدرس ٤ : التعرف على البرامج الضارة

الدرس ٥ : الوقاية من البرامج الضارة

حماية البيانات

لماذا النسخ الاحتياطي للبيانات ؟

١. فشل وسيلة التخزين : (بسبب تلف الأقراص الصلبة أو خدش الأقراص المضغوطة) .

٢. انقطاع التيار الكهربائي : (يمكن أن يتلف أية ملفات مفتوحة) .

٣. الفيروسات : (تتسبب بإتلاف البيانات وفقدانها) .

٤. الحذف بطريق الخطأ : (الظن بأن ملف هام غير هام) .

٥. الحذف المتعمد : (عن طريق الاختراقات والوصول الغير شرعي للبيانات) .

٦. تلف البناء : (حوادث بيئية مثل زلزال أو حريق أو فيضان)

تابع :حماية البيانات (أساليب النسخ الاحتياطي)

النسخ الاحتياطي يتم من خلال نسخ البيانات إلى وسائل تخزين إضافية مستخدمة لغايات الأرشفة

ويمكن إتباع أي من الوسائل التالية في عمليات النسخ الاحتياطية :

١. الأقراص المضغوطة **DVD** & **CD** .

٢. الأقراص الصلبة الخارجية .

٣. محركات أقراص الشريط (كاتردج البيانات).

٤. خوادم شبكة الاتصال (يتم تخزين البيانات على قرص صلب موجود في خادم بعيد)

٥. مصفوفة التعدد للأقراص المستقلة **RAID** : (يرمز Redundant Array Of Independent Disks) وهي مجموعة أقراص اثنين أو أكثر تتصرف بشكل منطقي كأنها واحد . تفيد في حالة وجود إخفاق للقرص الصلب الرئيسي إمكانية استعادة البيانات من الأقراص المتبقية .

حماية البيانات (الآثار المترتبة على سرقة البيانات)

إذا تمت سرقة البيانات الشخصية الحساسة فإن الخصوصية الشخصية تكون قد اخترقت .

وبذلك يمكن استخدام المعلومات التي سرقت للأغراض التالي :

- ✓ فتح الحسابات المصرفية .
- ✓ الحصول على بطاقات الائتمان .
- ✓ تنفيذ الأنشطة الجنائية .
- ✓ استخدام أرقام بطاقات الائتمان للاحتيال .
- ✓ الابتزاز والتهديد .
- ✓ نقل ملكية الأسهم .
- ✓ زيادة الفواتير بتحويل فواتير المجرم للضحية .

القسم الخامس: أمن المعلومات

الدرس ١ : أن تكون استباقيا

الدرس ٢ : التعريف بنفسك

الدرس ٣ : حماية البيانات

الدرس ٤ : التعرف على البرامج الضارة

الدرس ٥ : الوقاية من البرامج الضارة

التعرف على البرامج الضارة (ما هي الفيروسات)

ما المقصود بفيروس الحاسب ؟

فيروس الحاسوب : عبارة عن برنامج يدخل للحاسوب ليدمر أو يشوه البيانات والبرامج المخزنة داخل الحاسوب . يتنقل فيروس الحاسوب إلى حواسب آخرى عن طريق شبكات الحاسوب Computer Network واستخدام الأقراص النقالة الملوثة.

أنواع الفيروسات الحاسوبية:

١. الفيروسات الدودية Worms :

الفيروس الدودي لا يسبب أضراراً لأي نوع من الملفات ولكنه يتسبب بتوقيف النظام عن العمل من خلال أعادة نسخ نفسه . يحتل هذا النوع من الفيروسات الذاكرة الرئيسية وينتشر بسرعة فائقة جداً في الشبكات.

تابع : الفيروسات Viruses

٢. القنابل الموقوتة Time Bombs:

فيروس القنبلة الموقوتة : عبارة عن برنامج يقوم بتفجير نفسه في وقت محدد او بعد تنفيذه عدة مرات . يستخدم هذا النوع من قبل شركات الحاسوب التي تعطي نسخاً مجانية على أمل شراء النسخة الأصلية لاحقاً. إذا لم يقم المستخدم بشراء النسخة الأصلية ، يقوم البرنامج بتفجير نفسه .

٣. فيروسات قطاع الإقلاع (الاستنهاض) Boot Sector Viruses :

قطاع الإقلاع (الاستنهاض) : هو مكان تواجد الملفات لتحميل نظام التشغيل عند بدء تشغيل الحاسوب. ويحتل فيروس قطاع الإقلاع في الأماكن التي يقرأها الحاسوب وينفذ التعليمات المخزنة ضمنها على القرص الصلب ضمن جهازك ، وعند الإقلاع يصيب الفيروس منطقة قطاع الإقلاع الخاصة بنظام دوس (Dos Boot Record) مما يمنع الحاسب من التشغيل كلياً .

تابع : الفيروسات Viruses

٤. فيروس ملوث الملفات File Viruses:

تربط نفسها بالملفات التنفيذية التي تنتهي بالامتدادات exe. و com. وعندما يعمل احد البرامج الملوثة ، فإن هذا الفيروس ينتظر في الذاكرة إلى أن يشغّل المستخدم برنامجاً أخر ، فيلوثه وهكذا يعيد الفيروس نسخ نفسه .

٥. فيروس متعدد الأجزاء (Multipartite):

وهو خليط من فيروس قطاع الإقلاع وفيروس تلويث الملفات . تلوث الملفات ، وعندما يتم تشغيلها تلوث قطاع الإقلاع . وعندما يتم استنهاض(تشغيل) الحاسوب يبدأ الفيروس بعمله .

تابع : الفيروسات Viruses

٦. فيروسات الماكرو (**Macro Viruses**) :

الماكرو : هو عملية تنفيذ مجموعة من الأوامر ضمن برنامج . وقد أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج **MS-Word** عند فتح مستند ينشط الفيروس ويؤدي مهمته التخريبية بإجرائه تغييرات على كل المستندات الأخرى المنشأة . وقد بُرمج هذا الفيروس لينسخ نفسه الى ملفات المستندات الاخرى، مما يؤدي الى انتشاره مع استمرار استخدام البرنامج .

٧. أحصنة طروادة **Trojan Horses**:

فيروس حصان طروادة : عبارة عن برنامج يدخل إلى الحاسوب بشكل شرعي ، وهذا النوع من الفيروسات لا ينسخ نفسه. بل يقوم بسرقة الملفات أو أرقام سرية من جهازك. كثير منها تنتقل عبر البريد الالكتروني **E-mail** ضمن أي ملف أو صورة ولا يعلم المستخدم عن وجودها غالباً.

التعرف على البرامج الضارة (ما المقصود ببرامج التجسس)

ملفات التجسس Spyware

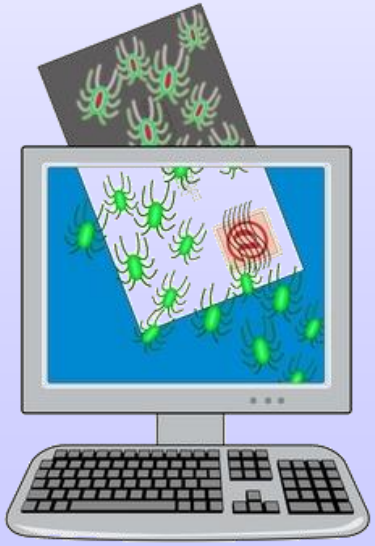
هي عبارة عن برامج غير مرغوب فيها ،مهمتها جمع وتسجيل نشاطات الشخص بحيث يتم تحميلها على الأجهزة بدون علم الشخص عن طريق برامج يتم تحميلها من الإنترنت أو عن طريق تصفح المواقع .

التعرف على البرامج الضارة (ما المقصود ببرامج التجسس)

كيف تصاب بملفات التجسس ؟

١. المواقع المشبوهة تستخدم ملفات الانترنت المؤقتة لجمع معلومات الشخص لأغراض سيئة.

٢. التحميلات الموجودة على بعض المواقع: تقوم بعض المواقع بعملية إخفاء ملفات التجسس على شكل أداة مساعدة يتم تحميلها لتصفح الموقع .



٣. المرفقات والروابط على البريد الإلكتروني : بطريقة تشبه الفيروسات.

٤. التطبيقات المضافة (**add-ons**) وتأتي غالبا مع حزمة البرامج الشائعة كالألعاب المجانية وأدوات حذف ملفات التجسس المزيفة .

التعرف على البرامج الضارة (ما المقصود ببرامج التجسس)

كيف تعلم أنك أصبت بملفات تجسس ؟

١. بطء أداء الجهاز .

٢. ظهور شريط أدوات على المتصفح لا يمكن حذفه بشكل نهائي .

٣. ظهور الإعلانات المتطايرة (**pop-up ads**) عند كل تشغيل للجهاز حتى ولو لم تكن متصلا بالإنترنت .

٤. تغير صفحة البداية للمتصفح ومحرك البحث الافتراضي.

التعرف على البرامج الضارة (ما المقصود ببرامج التجسس)

كيف تحذف ملفات التجسس:

١. إنهاء العمليات المشبوهة من خلال إدارة المهام.

٢. تعطيل الخدمات المشبوهة من خلال كونسول الإدارة **Management Console** .

٣. تعطيل الخدمات المشبوهة وعناصر بدء التشغيل التي تعمل مع بداية تشغيل الجهاز من خلال أداة تكون النظام **System Configuration Utility** وذلك بالضغط على ابدأ ثم تشغيل ثم كتابة **Msconfig**.

٤. حذف مدخلات الريجستري المرفقة مع الخدمات وعناصر بدء التشغيل المشبوهة .

٥. حذف الملفات المشبوهة في الجهاز.

٦. تحميل عدة برامج تقوم بحذف واكتشاف ملفات التجسس مثل **AntiSpyware Microsoft** وغيرها.

التعرف على البرامج الضارة (ما المقصود ببرامج التجسس)

كيف تحمي نفسك من ملفات التجسس ؟

١. قم بتحميل التحديثات بشكل دوري لنظام التشغيل ولبرامج مكافحة التجسس ولأي برنامج تستخدمه.

٢. عند ما تريد أن تحمل برنامجا انتبه للآتي :

- حمل البرامج فقط من المواقع الموثوقة.
- قم بقراءة تحذيرات الأمان واتفاقيات الترخيص وسياسة الخصوصية.
- لاتقم بالضغط على موافق أو **OK**أو **I Accept**لقفل أي نافذة تحميل تظهر لك واستبدل ذلك بالضغط على علامة (**X**) .

٣. قم بإجراء مسح دوري لجهازك بواسطة برامج مكافحة ملفات التجسس والفيروسات.

٤. استخدم الجدار الناري .

٥. اضبط إعدادت المتصفح **Internet Explorer** ليصبح أكثر أمانا من خلال الآتي :

- حمل أدوات حظر الدعايات المتطايرة **Pop_up Blocker .**
- اجعل إعدادات الأمان لمتصفحك عالية : فإذا كنت تستخدم **Internet Explorer** للتصفح ، فابق إعدادات الأمان لمنطقة الإنترنت **Internet Zone** إلى مستوى متوسط .

التعرف على البرامج الضارة (ما المقصود ببرامج Adware)

تعتبر **Adware** نوعا من البرامج التي يتم تصميمها لهدف محدد ومشروع ، وكذلك تقوم بعرض الإعلانات آليا للمستخدم خلال تصفح الانترنت ، وتقوم بتغيير صفحة البدء للمتصفح ، أو تغيير صفحة البحث، أو إذا كتبنا عنوان موقع الغوغل على سبيل المثال.. فإن المستكشف سيذهب إلى موقع آخر دون إرادتنا .....!! وهي في الحقيقة ليست مصممة بالضرورة للنوايا الخبيثة وممكن أن تكون مزعجة جداً

التعرف على البرامج الضارة (التخلص من الفيروسات)

الحماية من الفيروسات Protecting from Viruses

تستخدم برامج مضادة للفيروسات مثل McAfee, PC-Cillin, Norton تقوم باكتشاف الفيروسات وتقوم بتنظيفها ، تقيم هذه البرامج في الذاكرة وتكون في حالة نشطة.تسمى عملية تنظيف الفيروسات التطهير Disinfecting.

في حال عدم توفر مضاد فيروسات حديث قم بما يلي:

١. لا تستخدم أقراصاً مرنة من مصادر غير موثوقة.

٢. استخدم البرمجيات المسجلة فقط. .

٣. لا تفتح البريد الالكتروني إلا إذا كانت الرسالة من مصدر موثوق .

٤. قم بعمل نسخة احتياطية بانتظام لتجنب الضرر الواقع في حالة دخول الفيروس.

٥. اجعل الأقراص المرنة في حالة قراءة فقط..

القسم الخامس: أمن المعلومات

الدرس ١ : أن تكون استباقيا

الدرس ٢ : التعريف بنفسك

الدرس ٣ : حماية البيانات

الدرس ٤ : التعرف على البرامج الضارة

الدرس ٥ : الوقاية من البرامج الضارة

الوقاية من البرامج الضارة

ماذا يمكن ولا يمكن لبرامج مكافحة البرامج الضارة أن تفعل ؟

قد لا يتمكن البرنامج المضاد للفيروسات من منع فيروس أن يصيب الحاسب .

ويكون ذلك في إحدى الحالات التالية :

- تنزيل ملفات من الانترنت باستمرار قد تحتوي على فيروسات .
- الفيروسات الجديدة قد لا يمكن التعرف عليها من قبل البرنامج المضاد للفيروسات .

يمكن لبرامج مكافحة الفيروسات أن تفعل ما يلي :

- الكشف عن السلوك المشبوه في برامج أخرى .
- إذا حاول البرنامج نسخ نفسه .
- إذا حاول إتلاف الملفات أو البرامج الأخرى .
- في حالة الكشف يقوم باتخاذ الخطوات اللازمة لعزله وتنبيه المستخدم .

تابع : الوقاية من البرامج الضارة

ما الواجب عمله عند الإصابة بفيروس ؟

- أول أمر تشغيل المسح بواسطة برنامج مكافحة الفيروسات .
- قطع اتصال الانترنت أو شبكة الاتصال مع الحواسيب الأخرى .
- إذا لم يتم العزل للفيروسات فذلك يعني أنه لم يتم تحديث تعريفات الفيروسات .
- في حالة عدم التعرف على الفيروس يجب تحديث البرنامج المضاد للفيروسات .
- إذا تم إيجاد فيروس سيقوم البرنامج بإعطائك خيارات التصحيح كالحذف أو التطهير أو الحجر .
- عند الخطوة السابقة قم بكتابة اسم الفيروس للتعرف عليه أكثر من خلال معلومات الانترنت .
- أخيرا تشغيل مضاد الفيروسات مرة تلو المرة ، إلى أن تشير النتائج أنه لم يتم العثور على فيروس .

الوقاية من البرامج الضارة (تحديث البرامج باستمرار)

من المهم الحفاظ على تحديث كافة برامج الحاسب ومن المهم التحديث والتحميل يكون من المواقع الالكترونية الخاصة بتصنيع هذه البرمجيات بهدف تفادي أية نقاط ضعف أو ثغرات أمنية .

ومن المهم أيضا تحديث برامج مكافحة التجسس والبرامج المضادة للفيروسات وغالبا تقوم هذه البرامج بتنزيل وتثبيت أحدث التعريفات تلقائياً .

الهدف من تحديث البرامج : منع الفيروسات من استغلال الثغرات الأمنية في البرامج الحديثة والتي يتم تطويرها باستمرار .

الوقاية من البرامج الضارة (القيام بالفحص المنتظم)

تحدد برامج مكافحة الفيروسات الملفات أو البرامج التي يجب إصلاحها أو تطهيرها أو عزلها عن طريق مقارنة الملف الموجود على القرص الصلب إلى تعريفات الفيروسات في قاموس برنامج مكافحة الفيروس . تعرف هذه العملية باسم المسح .

يمكن لبرامج مكافحة الفيروسات أن تستهلك موارد الحاسب عند عملية المسح ، لذا يمكن :

- تحديد وقت لعملية المسح ليلاً .
- مسح الملفات منفردة بعد تحميلها من الانترنت .

الوقاية من البرامج الضارة (تعليمات السلامة)

- ✓ قم بالتفكير في ماهية البرامج التي تقوم بتحميلها من الانترنت .
- ✓ تأكد من أن تقوم بتحميل وتثبيت التحديثات المنتظمة .
- ✓ حافظ على برنامج مكافحة الفيروسات محدثاً .
- ✓ مسح الملفات بشكل دوري .
- ✓ كن حذراً على ما تنقر عليه أثناء تصفح الانترنت .
- ✓ كن حذراً في استخدام البريد الالكتروني .