الفصل الثالث
أمان الحاسوب وتراخيص البرامج

CHAPTER THREE
Computer Safety and Software Licenses

الفصل الثالث

أمان الحاسوب وتراخيص البرامج

Computer Safety and Software Licenses

3-1 مقدمة:

يتم استخدم الحواسيب في جميع المجالات، للتعامل مع البنوك والتسوق والاتصال مع الآخرين عبر الرسائل الإلكترونية أو برامج المحادثة. ومن المهم المحافظة على الرسائل الخاصة والبيانات الشخصية ومحتويات الحاسوب. لذا يجب الاهتمام بأمن وحماية الحاسوب.

ان التطورات الحديثة في أنظمة شبكات الحاسوب وتقنية المعلومات أحدثت تغيرات مستمرة في أساليب العمل والميادين كافة، إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسوب من الأمور الروتينية في يومنا هذا، وإحدى علامات العصر المميزة التي لا يمكن الإستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب خزن وتوفير المعلومات، إذ أن انتشار أنظمة المعلومات المحوسبة أدى إلى أن تكون عرضة للإختراق، لذلك أصبحت هذه التقنية سلاحاً ذو حدين تحرص المنظمات على إقتناءه وتوفير سبل الحماية له. والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من الإختراقات والسرقة والفساد، أو الكوارث الطبيعية، وفي نفس الوقت يسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها.

الإختراقات هي محاولة الدخول على جهاز أو شبكة حاسوب آلي من قبل شخص غير مصرح له بالدخول إلى الجهاز أو الشبكة وذلك بغرض الإطلاع أو السرقة أو التخريب أو التعطيل.

3-2 أخلاق العالم الإلكتروني:

أصبح استخدام الحواسيب ضرورياً في مجالات الحياة، بسبب ما يحدث من تطور كبير وسريع في تكنولوجيا المعلومات، إذ يلعب الحاسوب دور هام وفعال في مجالات مختلفة (التعليم والصناعة والتجارة والعسكرية)، مما تتطلب تعلم استخدام الحاسوب من قبل المتخصصين وغير المتخصصين، وضرورة معرفة القواعد التي يجب من خلالها التعامل مع الحاسوب والإنترنت.

وللعالم الإلكتروني أخلاق تكاد تكون تشبه أخلاق العالم التقليدي، فضلاً عن بعض الآداب التي يتطلبها هذا العالم الجديد. وينبغي الالتزام بمجموعة من الأخلاق والآداب العامة عند استخدام الإنترنت، ومن أهمها:

- احترام الطرف الآخر.

- الالتزام بعدم الإضرار بالآخرين.
- الإيجاز في طرح الأفكار ومحاورة الآخرين.
- الالتزام بالقانون.
- احترام الخصوصية الشخصية للآخرين.

3-3 أشكال التجاوزات في العالم الرقمي Abuse Forms in Digital World:

تشمل عدد من المخالفات القانونيه في عالم الأنترنت والحاسوب، والتي تصدر من بعض المستخدمين لغرض الوصول إلى أهداف تخالف القانون والخلق العام والتجاوزات على خصوصية الأخرين، وتشمل على:

1 جرائم الملكية الفكرية Intellectual Property Crimes. وتشمل نسخ البرامج بطريقة غير قانونية، وسرقة البرامج Software Piracy التطبيقية، سواء كانت تجارية أو علمية أو عسكرية، إذ تمثل هذه البرامجيات جهودا تراكمية من البحث.

2- الاحتيال Fraud احتيال التسويق، سرقة الهوية، الاحتيال على البنوك والاحتيال عن طريق الاتصالات، وسرقة الأرصدة Account Information Theft وسرقة المال من خلال التحويل الإلكتروني من البنوك أو الأسهم.

3- سرقة البيانات الخاصة والتشهير بالأخرين وابتزازهم.

3-4 أمن الحاسوب Computer Security:

يعد أمن الحاسوب جزء من أمن المنظومة المعلوماتية والتي هي بدورها جزء من الأمن العام Cyber Security والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية.

وبعبارة أخرى، هي عملية منع واكتشاف استعمال الحاسوب لأي شخص غير مسموح له (مخترق Attacker أو Intruder). وهي إجراءات تساعد على منع المستخدمين غير المسموح لهم بالدخول للحاسوب واستعمال ملفاته. وان الكشف عن هذه العمليات تساعد في تحديد الشخص الذي حاول اقتحام النظم ونجح في ذلك وعن تصرفاته في الحاسوب. ففي يومنا هذا، أصبحت المعلومات الشخصية أكثر عرضة للسرقة من دون أخذ الاحتياطات وتأمين الحماية الحاسوب في المنزل وأماكن العمل.

3-5 خصوصية الحاسوب Computer Privacy:

يُستخدم هذا المصطلح ليشير إلى الحق القانوني في الحفاظ على خصوصية البيانات المخزنة على الحاسوب أو الملفات المشتركة. وتظهر حساسية مسألة خصوصية الحاسوب أو

البيانات الخاصة عندما يتعلق الأمر ببيانات التعريف الشخصية المحفوظة في أي جهاز رقمي (سواءً كان حاسوب أو غيره). وان عدم القدرة على التحكم بإخفاء هذه البيانات هو ما يؤدي إلى تهديد خصوصية البيانات في الغالب.

ومن أكثر المشاكل التي تكون محور خصوصية البيانات فهي:

- المعلومات الصحية.
- السجل العدلي.
- المعلومات المالية.
- معلومات الموقع والسكن.
- الصور الشخصية.

6-3 تراخيص برامج الحاسوب:

قد يقرأ المستخدم الجمل الأتية على احد المنتجات البرمجية للحاسوب:

"الرجاء قراءة هذه الاتفاقية بكل اهتمام وعناية. عند قيامك بنسخ كافة أجزاء هذه البرامج أو جزء منها أو تثبيتها أو استخدامها، فإنك (والمشار إليك فيما بعد باصطلاح "العميل") بذلك تقبل جميع البنود والشروط الواردة بهذه الاتفاقية، بما يشمل على سبيل المثال لا الحصر، الأحكام المتعلقة بقيود الترخيص الواردة بالمادة (4)، والضمان المحدود بالمادة (6) و(7)، وتحديد المسؤولية بالمادة (8)، والأحكام والاستثناءات المحددة الواردة بالمادة (16). ويوافق العميل على أن تكون هذه الاتفاقية كأية اتفاقية خطية مكتوبة تم التفاوض بشأنها وموقعة من ....، مع العلم أن هذه الاتفاقية قابلة للتنفيذ بالقوة ضد العميل. إذا لم يوافق العميل على بنود هذه الاتفاقية، فلا يجوز له استخدام برنامج ...."

هذا ما يعرف بـ"رخصة أو تراخيص البرامجيات" **(Software license)** وهي وثيقة قانونية تحكم استعمال أو إعادة توزيع البرامجيات المحمية بحقوق النسخ. إذ يخضع استخدام برامج الحاسوب لاتفاقية التراخيص التي هي بمثابة عقد بين المستخدم وبين الجهة المنتجة للبرامج. وتسمح اتفاقية التراخيص باستخدام البرنامج، كما أنها تمنح حقوق أخرى وتفرض بعض القيود أيضاً. وغالباً ما توجد اتفاقية الترخيص على المنتج بشكل:

- مطبوعة على ورقة مستقلة مرفقة مع المنتج.
- مطبوعة في دليل الاستخدام، وغالبا ما يكون ذلك على ورقة الغلاف من الداخل.
- مدرجة كصفحة من صفحات البرنامج نفسه تظهر على الشاشة لدى تشغيله .

وتنص اتفاقية التراخيص في ضرورة الحصول على ترخيص مستقل لكل نسخة من كل برنامج يتم استخدامه على الحاسوب، فكل اتفاقية ترخيص تمنح الحق في استخدام نسخة واحدة من البرنامج على الحاسوب.

وتختلف اتفاقية التراخيص من برنامج إلى أخر ومن شركة إلى أخرى ومن طريقة استعمال إلى أخرى. فمنهم ما يوجب استخدام المنتج:

- مرة واحدة.
- عدة مرات وحسب تاريخ معين.
- على نوع معين من الأجهزة أو وفق موارد محددة.
- استخدام المنتج على أجهزة وحدات إدارية كاملة كان تكون شركة أو جامعة أو مؤسسة حكومية.
- استخدام المنتج مدى الحياة.
- استخدام البرنامج حسب البيانات أو حسب قيود الإدخال بغض النظر عن عدد الحواسيب أو المستخدمين.
- استخدام الفعالية المكانية أو الزمانية.

7-3 أنواع التراخيص:

1- اتفاقية الترخيص للمستخدم التطبيقات وأنظمة التشغيل، وتتمثل في منح ترخيص استخدام المنتج على جهاز حاسوب واحد باستخدام مفتاح للتفعيل لكل حاسوب.

2- التراخيص الجماعية: تختلف من منتج إلى آخر، وهي تسمح باستخدام البرنامج على عدد معين من أجهزة الحاسوب، وهي غالباً ما توفر مزايا سعرية كما يسهل الاحتفاظ بها، وتختلف عن النوع الأول باستخدام مفتاح تفعيل واحد لكل الحواسيب أو لمجموعة بين الحواسيب.

وسنقوم بعرض عدد من التعاريف المتعلقة بهذا الموضوع:-

- الاستخدام المتزامن: ينطبق على بعض برامج التطبيقات ولا ينطبق على نظم التشغيل أو لغات البرمجة أو برامج الترفيه والألعاب، ويحدث الاستخدام المتزامن عندما يتم استخدام نسخة واحدة من برنامج الحاسوب بواسطة أكثر من مستخدم عبر جهاز الخادم (سيرفر) على الشبكة، ونظراً لعدم قيام بعض الشركات المصنعة باستخدام تدابير لـ"الاستخدام المتزامن" فإن المستخدم يحتاج إلى تراخيص منفصلة لكل حاسوب سواء كان هذا الجهاز قيد الاستعمال أو لا.

- المنتج "قيد الاستخدام": يعتبر برنامج الحاسوب "قيد الاستخدام" عندما يكون مثبتاً في الذاكرة الدائمة (على القرص الثابت أو على قرص مضغوط) أو عندما يكون محملاً في الذاكرة المؤقتة. أما على الشبكة فقد يكون المنتج قيد الاستخدام بأحد الأسلوبين

1- التثبيت على القرص الثابت لمحطة عمل على شبكة "محلية".

2- التثبيت على خادم (سيرفر) الشبكة فقط وتشغيله عن طريق الخادم (سيرفر) – وفقاً للأسلوب الأخير– بتحميل نسخة من البرنامج في الذاكرة المؤقتة لمحطة العمل، إنما ينبغي أن لا يكون مخزنا في الذاكرة الدائمة لمحطة العمل، زمن المهم أن يتم التمييز بين هذين الأمرين عند إحصاء عدد التراخيص التي تحتاجها الشبكة.

ملاحظة:

ننصح جميع أبنائنا الطلبة بعدم اقتناء وتنصيب نسخ البرامجيات غير الأصلية والتي تباع بالأسواق، وذلك للأسباب الأتية:

- ان هذا العمل يتنافى مع الشريعة السماوية التي حرمت سرقة جهد الأخرين وتسويق منتجاتهم بدون علمهم، كما أن هذا العمل يتنافى أيضاً مع الخلق الرفيع والأعراف الأصلية، وكذلك مع المقاييس العالمية لضمان الجودة الاعتمادية.
- أغلب هذه البرامج عادة ما تحمل فايروسات أو برامج التجسس والقرصنة.

وهنا، قد يتسأل الطالب عن البديل، واننا نضع له الحلول الأتية:

- البحث عن مراكز التسويق لهذه البرامجيات داخل العراق، إذ قامت اغلب الشركات المصنعة للبرامجيات بفتح مراكز لها للتسويق، وبنسبة خصم عالية وخصوصا للطلبة، وبالإمكان الدخول لمواقع محركات البحث وكتابة **Iraq** ثم **Software reseller**.
- البديل الثاني هو التحول للبرامجيات ونظم التشغيل المفتوحة والأمينة، وهي تكافئ في عملها نظم التشغيل مدفوعة الأجر (إذا لم تكن اعلى)، ويجب التعلم عندها على كيفية مع العلم أنها متشابهة.

8-3 الملكية الفكرية Intellectual Property:

هي اتفاقية قانونية تكون موثقة في دوائر عدلية مثل المكتبات العامة أو دوائر الملكية الفكرية (حالها حال الملكية للأرضي أو السيارات أو الأموال). وهي مجموعة الحقوق التي تحمي الفكر والإبداع الإنساني وتشمل براءات الاختراع والعلامات التجارية والرسوم والنماذج الصناعية وحق المؤلف وغيرها.

ويعد حق المؤلف من حقوق الملكية الفكرية التي يتمتع بها مبدعون للمصنفات الأصلية بما في ذلك برامج الحاسوب والجداول وقواعد البيانات الخاصة بالحواسيب، والتي من الممكن أن تتخذ شكل كلمات أو أرقام مشفرة "كود" أو مخططات أو أي شكل آخر.

- حقوق النسخ والتأليف (Copyright):

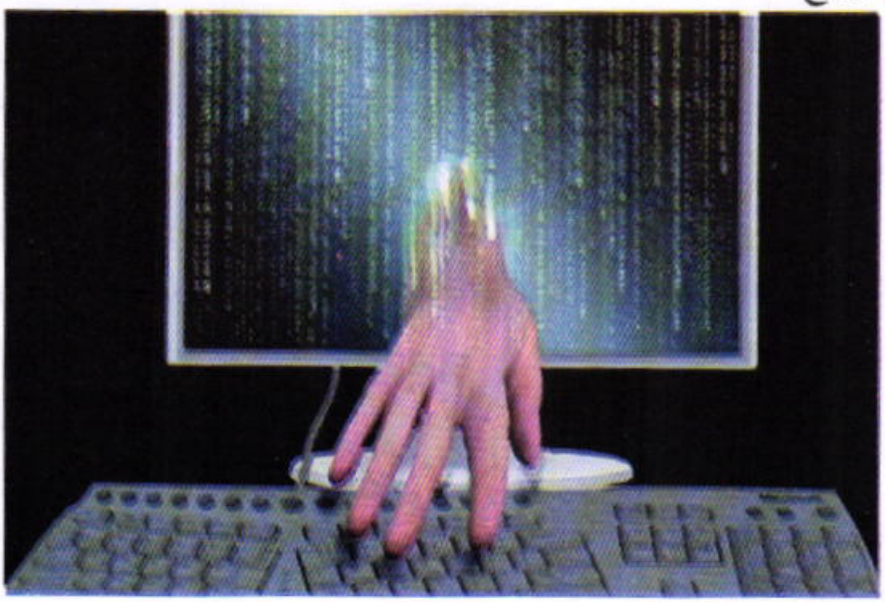
مجموعة من الحقوق الحصرية (Exclusive Rights) التي تنظم استعمال النصوص أو أي تعبير عملي (فني، أدبي، أكاديمي) عن فكرة أو معلومة ما، بمعنى أخر؛ أن "حقوق نسخ

واستخدام" عمل إبداعي جديد. تشكل هذه الحقوق نوع من الحماية للمبدع ليتقاضى أجرا عن إبداعه لفترة محددة تختلف حسب البلد والاتفاقية. الأعمال التي تنتهي مدة حمايتها الفكرية تدخل ضمن ما يسمى ملكية عامة (Public Domain)، الشكل (3-1)، فتصبح في متناول استخدام الجميع. وتشكل الحماية الفكرية أهميّة كبيرة في عصرنا الحالي، إذ يضمن القانون حق خاص بالمفكّر والمبتكر يحفظ له حقوقه الفكرية ونسبها له والحفاظ أيضاً على حقوقه بالأرباح المالية، تدخل من ضمنها حقوق الملكية الفكرية الرقمية والتي تشمل المصنفات الرقمية.

الشكل (3-1) عدد من الأيقونات تستخدم للملكية العامة وحق المليكة

3-9 الاختراق الإلكتروني Electronic Intrusion:

هو فيام شخص غير مخول أو أكثر بمحاولة الدخول (الوصول) الكترونياً إلى الحاسوب أو الشبكة عن طريق شبكة الإنترنت وذلك بغرض الإطلاع، والسرقة، التخريب، والتعطيل باستخدام برامج متخصصة.



3-9-1 أنواع الاختراق الإلكتروني:

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلى ثلاثة أقسام:

1. المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدار الناري **Firewall** والتي توضع لحمايتها يتم ذلك باستخدام المحاكاة لغرض الخداع **Spoofing** (هو مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام)، إذ أن حزم البيانات تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة.
2. الأجهزة الشخصية والعبث بما فيها من معلومات. وتعد من الطرق الشائعة لقلة خبرة أغلب مستخدمي هذه الأجهزة من جانب ولسهولة تعلم برامجيات الاختراق وتعددها من جانب آخر.
3. البيانات من خلال التعرض والتعرف على البيانات أثناء انتقالها ومحاولة فتح التشفير اذا كانت البيانات مشفرة وتستخدم هذه الطريقة في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية لبطاقات البنوك.

3-9-2 مصادر الاختراق الإلكتروني

1. مصادر متعمدة: ويكون مصدرها جهات خارجية تحاول الدخول إلى الجهاز بصورة غير المشروعة بغرض قد يختلف حسب الجهاز المستهدف.

ومن الأمثلة عن المصادر المتعمدة للاختراق الإلكتروني:

- المحترفون والهواة، لغرض التجسس دون الإضرار بالحاسوب.
- اختراق شبكات الاتصال والأجهزة الخاصة بالإتصال للتنصت أو للإتصال المجاني.
- اختراق لنشر برنامج معين أو لكسر برنامج أو لفك شفرتها المصدرية (**Crackers**).
- أعداء خارجيون وجهات منافسة.
- مجرمون محترفون في مجال الحاسوب والإنترنت.

2. مصادر غير متعمدة: وهي تنشأ بسبب ثغرات موجودة في برامجيات الحاسوب والتي قد تؤدي إلى تعريض الجهاز إلى نفس المشاكل التي تنتج عن الأخطار المتعمدة.

3-9-3 المخاطر الأمنية الأكثر انتشارا

a. الفيروسات (**Viruses**) : هي برامج مصممة للانتقال إلى أجهزة الحاسوب بطرق عدة وبدون أذن المستخدم، وتؤدي إلى تخريب أو تعطيل عمل الحاسوب أو أتلاف الملفات والبيانات. وسيتم التحدث عن الفايروسات وأنواعها بشكل موسع.

b. ملفات التجسس (Spywares): هي برامج مصممة لجمع المعلومات الشخصية مثل المواقع الإلكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الإلكترونية، وكذلك تستطيع الحصول على أمور مهمة للمستخدم مثل رقم بطاقة الائتمان دون علمه.

c. ملفات دعائية (Adware) هي برامج مصممة للدعاية والإعلان وتغيير الإعدادات العامة في أجهزة الحاسوب، مثل تغيير الصفحة الرئيسية للمتصفح وإظهار بعض النوافذ الدعائية أثناء اتصالك بالإنترنت وتصفحك للمواقع الإلكترونية.

d. قلة الخبرة في التعامل مع بعض البرامج: مع ازدياد استخدام الإنترنت من عامة الناس غير المتخصصين، واستخدامهم وتعاملهم مع برامجيات متطورة الخاصة بخدمة تطبيقات الإنترنيت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامجيات، قد يفتح ثغرة في جهاز الحاسوب تمكن الأخرين من اختراق الجهاز.

e. أخطاء عامة: مثل سوء اختيار كلمة السر أو كتابتها على ورقة مما يمكن الأخرين من قراءتها، أو ترك الحاسوب مفتوح مما يسمح للأخرين (خاصة غير المخولين أو الغرباء) بالدخول لملفات الحاسوب أو تغير بعض الإعدادات.

10-3 برامجيات خبيثة Malware:

Malware هي اختصار لكلمتين **Malicious Software** وهي برامج مخصصة للتسلل لنظم الحاسوب أو تدميره بدون علم المستخدم. وما إن يتم تثبيت البرمجية الخبيثة فإنه من الصعب إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح ضررها من إزعاج بسيط (بعض النوافذ الإعلانية غير المرغوب بها خلال عمل المستخدم على الحاسوب متصلاً أم غير متصلا بالشبكة) إلى أذىً غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرامجيات الخبيثة هي الفيروسات وأحصنة طروادة

1-10-3 فايروسات الحاسوب:

هي برامج صغيرة خارجية صممت عمداً لتغيير خصائص الملفات التي تصيبها وتقوم بتنفيذ بعض الأوامر إما بالحذف أو التعديل أو التخريب وفقاً للأهداف المصممة لأجلها. ولها القدرة على التخفي، ويتم خزنها داخل الحاسوب بإحدى طرق الانتقال لإلحاق الضرر به والسيطرة عليه.

3-10-2 الأضرار الناتجة عن فايروسات الحاسوب

1. تقليل مستوى إداء الحاسوب
2. إيقاف تشغيل الحاسوب وإعادة تشغيل نفسه تلقائياً كل بضع دقائق أو إخفاقه في العمل بعد إعادة التشغيل.
3. تعذر الوصول إلى مشغلات الأقراص الصلبة والمدمجة (وحدات الخزن) وظهور رسالة تعذر الحفظ لوحدات الخزن.
4. حذف الملفات أو تغيير محتوياتها.
5. ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات والقوائم والبيانات.
6. تكرار ظهور رسائل الخطأ في أكثر من تطبيق.
7. إفشاء معلومات وأسرار شخصية هامة.

3-10-3 صفات فايروسات الحاسوب

1. القدرة على التناسخ والانتشار Replication
2. ربط نفسها ببرنامج آخر يسمى الحاضن (المضيف Host)
3. يمكن أن تنتقل من حاسوب مصاب لآخر سليم.

3-10-4 مكونات الفايروسات

يتكون برنامج الفايروس بشكل علم من أربعة أجزاء رئيسة تقوم بالآتي:

1. آلية التناسخ The Replication Mechanism نسمح للفايروس أن ينسخ نفسه.
2. آلية التخفي The Hidden Mechanism تخفي الفايروس عن الاكتشاف.
3. آلية التنشيط The Trigger Mechanism تسمح للفايروس بالانتشار.
4. آلية التنفيذ The Payload Mechanism تنفيذ الفايروس عند تنشيطه.

3-10-5 أنواع الفايروسات

تقسم الفايروسات إلى ثلاثة أنواع، كما في الشكل (3-2):

1. الفايروس (Virus): برنامج تنفيذي (ذات الامتداد com, exe, bat, pif, scr)، يعمل بشكل منفصل ويهدف إلى إحداث خلل في الحاسوب، وتتراوح خطورته حسب المهمة المصمم لأجلها، فمنها البسيطة ومنها الخطيرة، وينتقل بواسطة نسخ الملفات من حاسوب يحوي ملفات مصابة إلى حاسوب آخر عن طريق الأقراص المدمجة (CD) والذاكرة المتحركة (Flash Memory).
2. الدودة (Worm): تنتشر فقط عبر الشبكات والإنترنت مستفيدة من قائمة عناوين البريد الإلكتروني (مثل تطبيق برنامج التحدث الماسنجر Messenger)، فعند إصابة الحاسوب

يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في قائمة العناوين ويرسل نفسه إلى كل الأشخاص في القائمة، مما يؤدي إلى انتشاره بسرعه عبر الشبكة.

3. حصان طروادة (Trojan Horse): فايروس تكون آلية عمله مرفقاً (ملحقاً) مع أحد البرامج، أي يكون جزءاً من برنامج دون ان يعلم المستخدم. سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، إذ اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.

الشكل (3-2) أشكال مختلفة من الفايروسات

3-11 أهم الخطوات اللازمة للحماية من عمليات الاختراق:

الحفاظ على جهاز الحاسوب ضد هذه الملفات بشكل كامل صعب جداً مادام الجهاز مربوط بشبكة الإنترنت، لكن يمكن حماية الحاسوب بنسبة كبيرة وتقليل خطر الإصابة بالاختراقات الالكترونية والبرامج الضارة باتباع الخطوات الأتية:

1. استخدام نظم تشغيل محمية من الفايروسات كنظم يونكس ولينكس ومشتقاتها. وتم بناء هذه النظم بحيث لا يمكن ان يدخل اليها أي برنامج خارجي إلا بموافقة وعلم المستخدم بشكل واضح وصريح، كما ان ملفات النظام الأساسية تكون محمية من أي تغير أو تلاعب حتى عن طريق الخطأ غير المتعمد.
2. تثبيت البرامج المضادة أو المكافحة للفايروسات (Antivirus) مثل (Norton, Kaspersky, McAfee, Avira) وبرنامج مكافحة ملفات التجسس (Antispyware) مثل AVG Anti-Spyware ذات الإصدارات الحديثة وتحديث النسخة.
3. الاحتفاظ بنسخ للبرامجيات المهمة مثل نظام التشغيل ويندوز وحزمة أوفيس ونسخة من ملفات المستخدم.
4. عدم فتح أي رسالة أو ملف ملحق ببريد إلكتروني وارد من شخص غير معروف للمستخدم، أو الملفات ذات امتدادات غير المعروفة.

5. تثبيت كلمة سر Password على الحاسوب والشبكة اللاسلكية الخاصة بالمستخدم مع تغييرها كل فترة، وعدم السماح إلا للمستخدمين الموثوقين بالاتصال واستخدام الحاسوب.
6. عدم الاحتفاظ بأية معلومات شخصية في داخل الحاسوب كـ(الرسائل الخاصة، الصور الفوتوغرافية، الملفات المهمة، والمعلومات المهمة مثل أرقام الحسابات أو البطاقات الائتمانية)، وخزمها في وسائط تخزين خارجية.
7. عدم تشغيل برامجيات الألعاب على نفس الحاسوب الذي يحتوي البيانات والبرامجيات المهمة، لأنها تعد من اكثر البرامجيات تداولاً بين الأشخاص والتي تصاب بالفايروسات.
8. إيقاف خاصية مشاركة الملفات إلا للضرورة. وعمل نسخ احتياطية من الملفات المهمة والضرورية.
9. ثقافة المستخدم وذلك من خلال التعرف على الفايروسات، وطرق انتشارها، وكيفية الحماية منها، والآثار المترتبة حال الإصابة بها. ويتم هذا عن طريق التواصل المستمر من خلال زيارة المواقع التي تهتم بالحماية من الفايروسات.
10. فك الارتباط بين الحاسوب والموديم (Modem) أو الخط الهاتفي عند الانتهاء من العمل، فذلك يمنع البرامج الخبيثة التي تحاول الاتصال من الدخول إلى الحاسوب.
11. تفعيل عمل الجدار الناري Firewall: يقوم الجدار الناري بتفحص المعلومات الواردة من الإنترنت والصادرة إليه. ويتعرف على المعلومات الواردة من المواقع الخطرة أو تلك التي تثير الشك فيعمل على إيقافها. إذا قام المستخدم بإعداد جدار الحماية بشكل صحيح، فلن يتمكن المتطفلون (الذين يبحثون عن أجهزة الحاسوب التي لا تتمتع بالحصانة) من الدخول والاطلاع على هذه الأجهزة. الشكل (3-3).

الشكل (3-3) تفعيل عمل الجدار الناري لحجب المعلومات الخطيرة عن الحاسوب

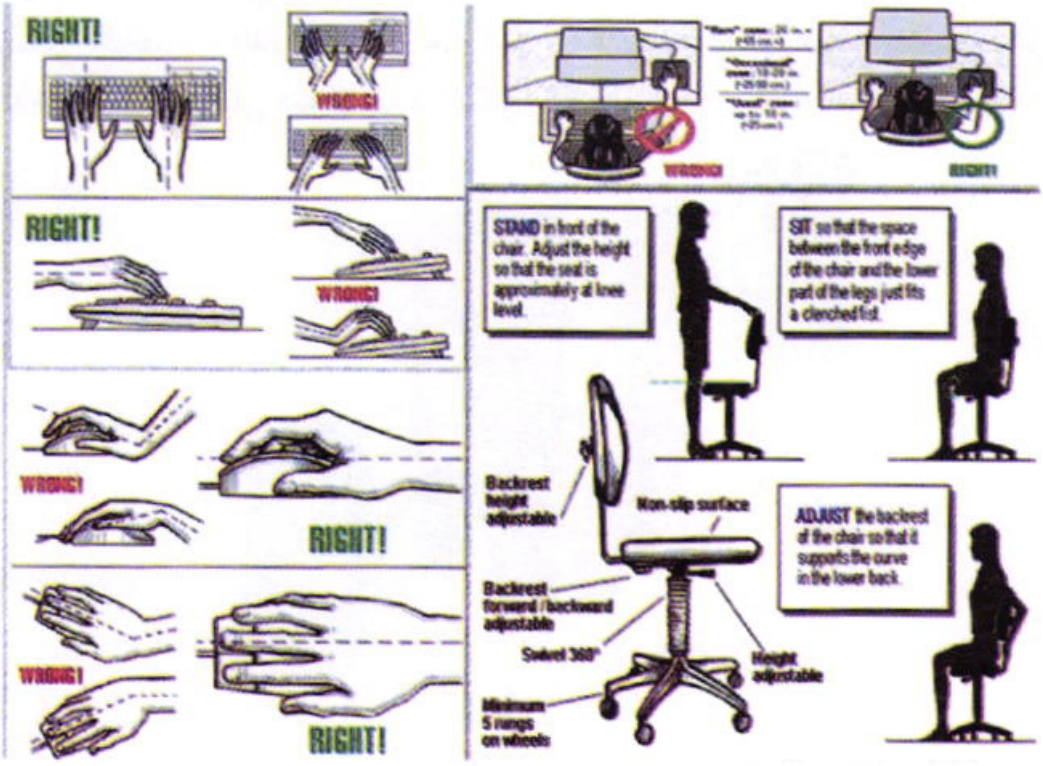
12-3 أضرار الحاسوب على الصحة Damage Computer Health:

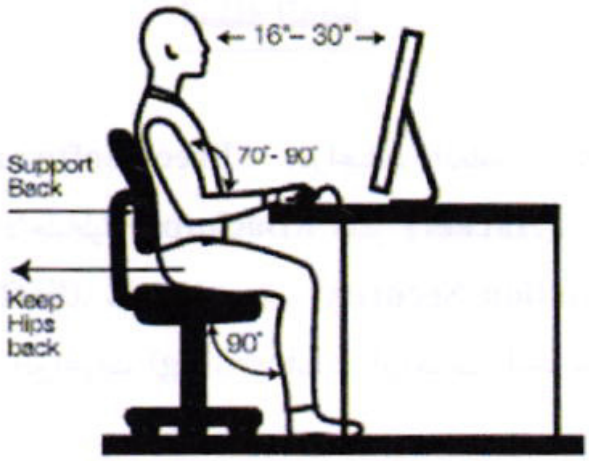
الجلوس لفترات طويلة أمام الحاسوب. الجلوس الخاطئ أمام شاشة الحاسوب، والتعرض للأشعة الصادرة من هذه الشاشة الذي يؤثر في العين والإبصار والبشرة والجلد. وأفضل وقاية هنا هي التأكد من صحة وضعية الجلوس أمام الحاسوب مع الحفاظ على وضع الشاشة بشكل مناسب حتى لا يرفع المستخدم للحاسوب رأسه أو يخفضه كثيراً.

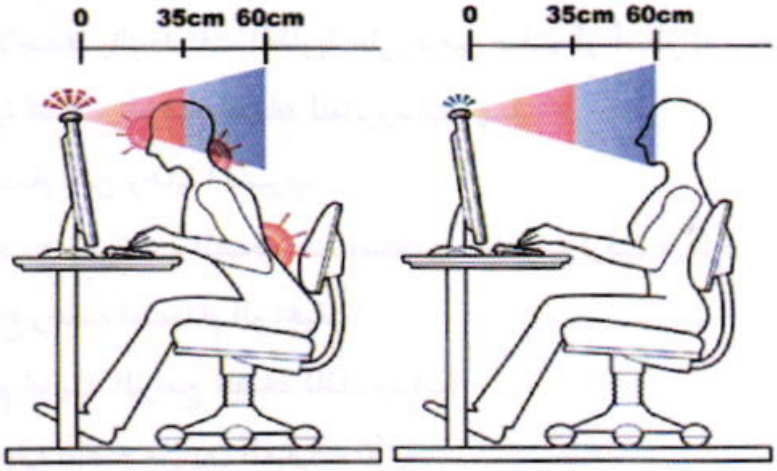
- أثار بدنية ونفسية قصيرة المدى **Physical and Psychological Effects Include Short-Range** وتشمل توتر وإجهاد عضلات العين والقلق النفسي.

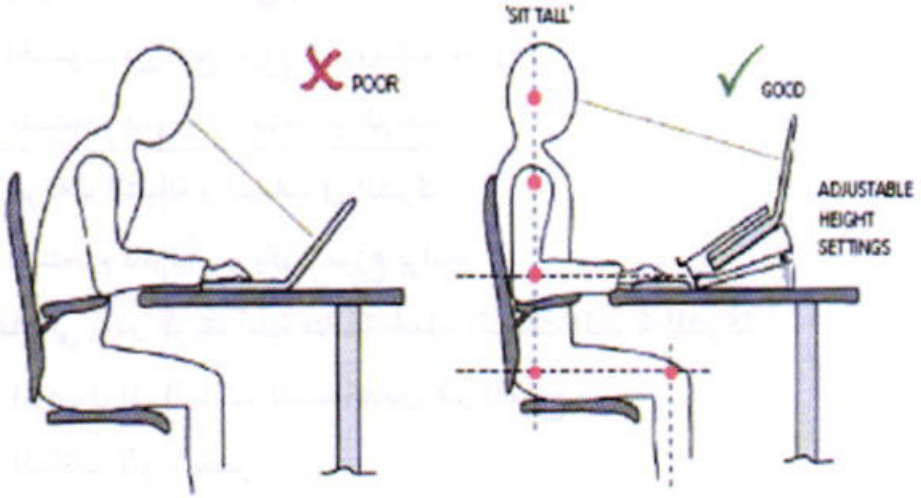
الآثار البدنية والنفسية بعيدة المدى-**Physical and Psychological Effects Far Reaching** التي تأخذ فترة أطول لظهورها ومنها آلام العضلات والمفاصل والعمود الفقري وحالة من الأرق والقلق النفسي والانفصال النفسي والاجتماعي عن عالم الواقع والعيش في وسط افتراضي والعلاقات الخيالية لمن يدمنون على الإنترنت. وأفضل وقاية لذلك هو التوقف من حين لآخر عن العمل بالحاسوب، وبسط الساقين والكاحلين والقيام ببعض التمارين الرياضية الخفيفة لتسريع جريان الدم وتحديد ساعات العمل بالحاسوب في الليل.

الشكل (3-4) يوضح الطريقة الصحيحة لاستخدام الماوس ولوحة المفاتيح، وكيفية الجلوس الصحيح أمام الحاسوب (نوع المكتبي والمحمول).









الشكل (3-4) الوضع الصحيح لاستعمال لوحة المفاتيح والماوس
والوضعية الصحيحة لكرسي الجلوس أمام الحاسوب

أسئلة الفصل

س1/ عرف ما يأتي:

البرامجيات المجانية (Free Software)، البرامجيات العامة (Public Domain Software)، النسخ الاحتياطية (Backups)، هاكر (Hacker)، حق ملكية البرامجيات (Software Copyright)، سرية المعلومات (Information Security)، الخصوصية (Privacy)، تراخيص البرامجيات (Licensing)، البرامجيات التجارية (Commercial Software).

س2/ علل ما يأتي:

- ينصح بالاحتفاظ بالتحديثات المطلوبة على قرص صلب أو أسطوانة مدمجة.
- تعد عملية تحديث البرامج المضادة للفايروسات مهمة.
- يجب الاهتمام بأمن وحماية الحاسوب.

س3/ اذكر عدد من المشكلات الصحية عند استخدام الحاسوب لوقت طويل؟

س4/ عدد أنواع رخصة استخدام البرامجيات؟

س5/ كيف يتم تحديث البرامج المضادة للفايروسات؟

س6/ اختر العبارة الأصح من بين العبارات الأتية:

➢ اتفاقية رخصة المستخدم هي رخصة ملحقة بالبرنامج لـ:

- حماية الحاسوب من جميع أنواع الفيروسات المعروفة.
- تقييد المستخدم قانونياً في استخدام البرامج.
- حماية محركات الشبكة والبيانات في الشركة.
- إلزام المستخدم قانونياً بأن يكون موزّع برامج.

➢ أي مما يأتي يعتبر طريقة أمنية مناسبة لحماية البيانات السرية للشركة:

- توفير الوصول إلى البيانات للمستخدمين غير المصرح لهم.
- توفير البيانات لأي شخص.
- توفير الوصول للبيانات فقط للأشخاص المصرح لهم.
- عدم توفير البيانات لأي شخص.

➢ تستخدم كلمة المرور:

- لتسهيل الوصول لمعلومات الحاسوب.
- لحماية الحاسوب من المستخدمين غير المصرح لهم.
- لتسهيل اتصال الحاسوب بالشبكة.
- لمنح المستخدمين غير المصرح لهم حق صلاحية الدخول لحواسيب الشبكة.

➢ أي مما يأتي يعتبر من أنواع فيروسات الحاسوب؟

- المعالج.
- الملف.
- حصان طروادة.
- ماكرو.

➢ أي مما يأتي يمكن استخدامه بحيث لا يستطيع أحد غير المستخدمين المسجلين من الوصول إلى الحاسوب؟

- برنامج مضاد الفيروسات.
- كلمة المرور (الرقم السري).
- الجدار الناري.
- قاعدة بيانات.

➢ من الطرق الجيدة لتأمين معلومات الشركة:

- لا توجد طريقة للتبليغ عن الاختراقات الأمنية.
- أخذ نسخ احتياطية للملفات الحاسوب على نحو منتظم.
- عدم تغيير كلمات المرور للموظفين بانتظام.
- توفير البيانات السرية لأي شخص.

➢ كيف تتجنب وصول الفيروسات إلى الحاسوب؟

- إعادة تشغيل الحاسوب
- مسح برنامج البريد الإلكتروني
- تثبيت برنامج مضاد للفيروسات
- إخراج بطاقة الشبكة من الحاسوب

➢ الطريقة القانونية لاستخدام البرامج هي:

- الاتفاقية الشفهية
- التفاهم
- التراخيص

➢ نوع من أنواع تراخيص استخدام البرامج لفترة مقابل مبالغ زهيدة

- البرامج التطبيقية
- البرامج التجريبية
- البرامج التنفيذية
- الأنظمة والبرامج