

وزارة التعليم العالي والبحث العلمي
الجامعة المستنصرية
كلية الادارة والاقتصاد

المحاضرة الخامسة/الاختراق الالكتروني

حاسوب 1/ الكورس الاول/ المرحلة الاولى/ صباحي مسائي

البروفائل الاكاديمي للاستاذ

<https://uomustansiriyah.edu.iq/e-learn/profile.php?id=1740>

اسم التدريسي

أ.م. علياء هاشم محمد

امان الحاسوب

Computer Saftey

الاختراق الالكتروني Electronic Intrusion

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

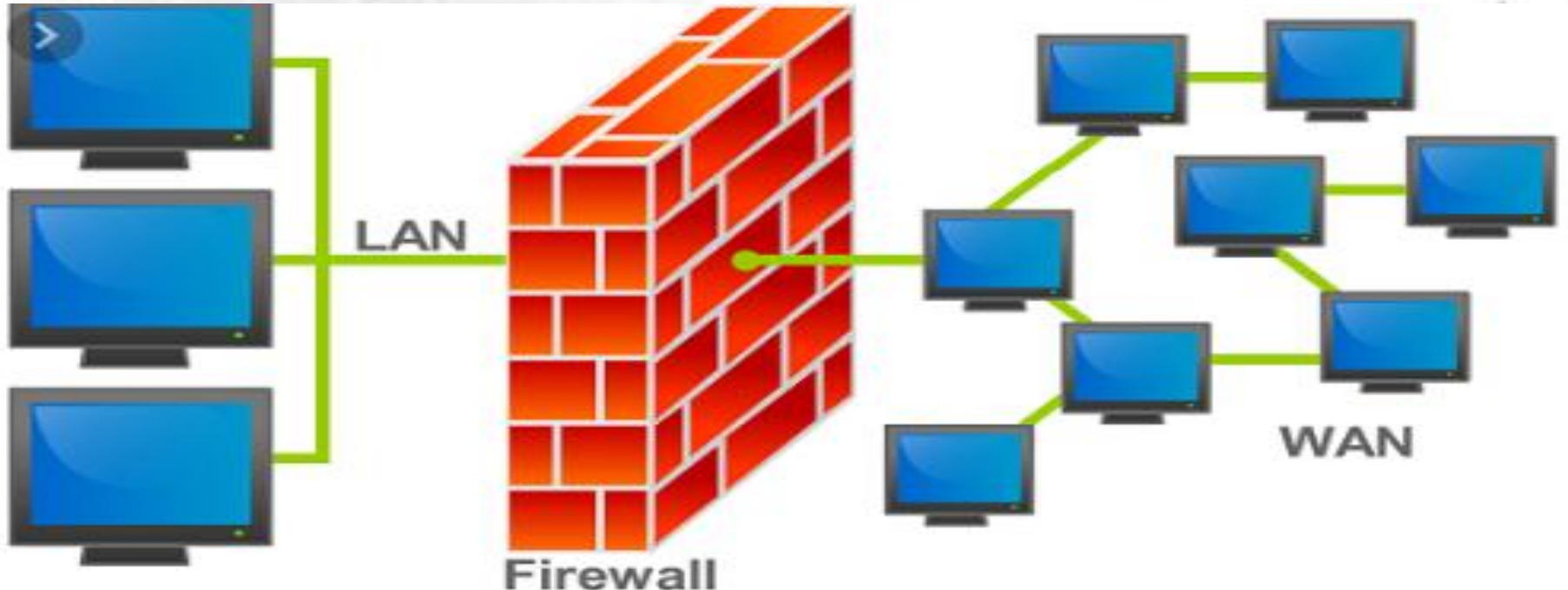




انواع الاختراق الالكتروني

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 (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.



Firewall

Officially invented in early 1990s



2. الأجهزة الشخصية والعبث بما فيها من معلومات وتعد من الطرق الشائعة لقلّة خبرة أغلب مستخدمي هذه الأجهزة من جانب ولسهولة تعلم برامجيات الاختراق وتعددتها 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



مصادر الاختراق الالكتروني

1. **مصادر متعملة**، ويكون مصدرها جهات خارجية تحاول الدخول إلى الجهاز بصورة غير

المشروعة بغرض قد يختلف حسب الجهاز المستهدف.

ومن الأمثلة عن المصادر المتعملة للاختراق الإلكتروني:

- محترفون والهواة، لغرض التجسس دون الإضرار بالحاسوب.

- اختراق شبكات الاتصال والأجهزة الخاصة بالاتصال للمتنتصت أو للاتصال المجاني.

- اختراق لنشر برنامج معين أو لكسر برنامج أو لفك شفرتها المصنعية (Crackers).

- أعداء خارجيون وجهات منافسة.

- مجرمون محترفون في مجال الحاسوب والإنترنت.

2. **مصادر غير متعملة**، وهي تنشأ بسبب ثغرات موجودة في برامج الحاسوب والتي قد تؤدي

إلى تعريض الجهاز إلى نفس المشاكل التي تنتج عن الأخطار المتعملة.



المخاطر الامنية الاكثر انتشاراً

٥. الفيروسات (Viruses) : هي برامج مصممة للانتقال إلى أجهزة الحاسوب بطرق علة وبدون أذن المستخدم، وتؤدي إلى تخريب أو تعطيل عمل الحاسوب أو إتلاف الملفات والبيانات.



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 الإنترنت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامجيات، قد يفتح ثغرة في جهاز الحاسوب تمكن الآخرين من اختراق الجهاز.

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

وزارة التعليم العالي والبحث العلمي
الجامعة المستنصرية
كلية الادارة والاقتصاد

المحاضرة السادسة

البرامجيات الخبيثة

حاسوب 1 / الكورس الاول / المرحلة الاولى / صباحي مساني

البروفائل الاكاديمي للاستاذ

<https://uomustansiriyah.edu.iq/e-learn/profile.php?id=1740>

اسم التدريسي

أ.م. علياء هاشم محمد

2022-2021

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 النواقد الإعلانية غير المرغوب بها خلال عمل المستخدم على الحاسوب متصلاً أم غير متصلاً بالشبكة) إلى أذى غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرامجيات الخبيثة هي **الفيروسات** و**أحصنة طروادة**

3-10-1 فايروسات الحاسوب:

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

الاضرار الناتجة عن فايروسات الحاسوب

1. تقليل مستوى أداء 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 التخزين) وظهور رسالة تعذر الحفظ لوحدات التخزين.
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** تسمح 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.

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

1. الفيروس (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. فمثلاً البسيطة ومنها الخطيرة، وينتقل بواسطة نسخ الملفات من حاسوب بحوي ملفات مصابة إلى حاسوب آخر عن طريق الأقراص المدججة (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 بسرعة عبر الشبكة.

3. حصان طروادة (Trojan Horse): فيروس تكون آلية عمله مرفقاً (ملحقاً) مع أحد البرامج، أي يكون جزءاً من برنامج دون أن 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 (2-3) أشكال مختلفة من الفيروسات

3-11 أهر 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 الآتية:

1. استخدام نظم تشغيل محمية من الفيروسات كنظم يوتكس ولينكس ومشتقاتها وتم بنه هذه النظم بحيث لا يمكن ان يدخل اليها أي برنامج خارجي إلا بموافقة وعلم المستخدم بشكل واضح وصريح، كما ان ملفات النظم الأساسية تكون محمية من أي تغير أو تلاعب حتى عن طريق الخطأ غير المتعمد

2. تثبيت البرامج المضادة أو المكافحة للفيروسات (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 نظم التشغيل ويندوز وحزمة أوفيس ونسخة من ملفات المستخدم.

4. عدم فتح أي رسالة أو ملف ملحق بريد 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. علم الاحتفاظ بأية معلومات شخصية في داخل الحاسوب كـ(الرسائل الخاصة، الصور

الفوتوغرافية، الملفات المهمة، والمعلومات المهمة مثل أرقام الحسابات أو البطاقات

الائتمانية)، وخزنها في وسائط تخزين خارجية.

7. علم تشغيل **برامجيات الألعاب** على نفس الحاسوب الذي يحتوي البيانات والبرامجيات

المهمة، لأنها تعد من أكثر البرامجيات تداولاً بين الأشخاص والتي تصاب بالفيروسات.

8. إيقاف خاصية مشاركة الملفات إلا للضرورة. وعمل نسخ احتياطية من الملفات المهمة

والضرورية.

9. **ثقافة المستخدم** وذلك من خلال التعرف على الفيروسات، وطرق انتشارها، وكيفية الحماية

منها، والآثار المترتبة حال الإصابة بها. ويتم هذا عن طريق التواصل المستمر من خلال

زيارة المواقع التي تهتم بالحماية من الفيروسات.

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 قلم المستخلم 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

3-12 أضرار الحاسوب على الصحة :Damage Computer Health

الجلوس لفترات طويلة أمام الحاسوب الجلوس الخاطئ أمام شاشة الحاسوب، والتعرض للأشعة الصادرة من هذه الشاشة التي 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 يحنقه كثيراً.

- آثار 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

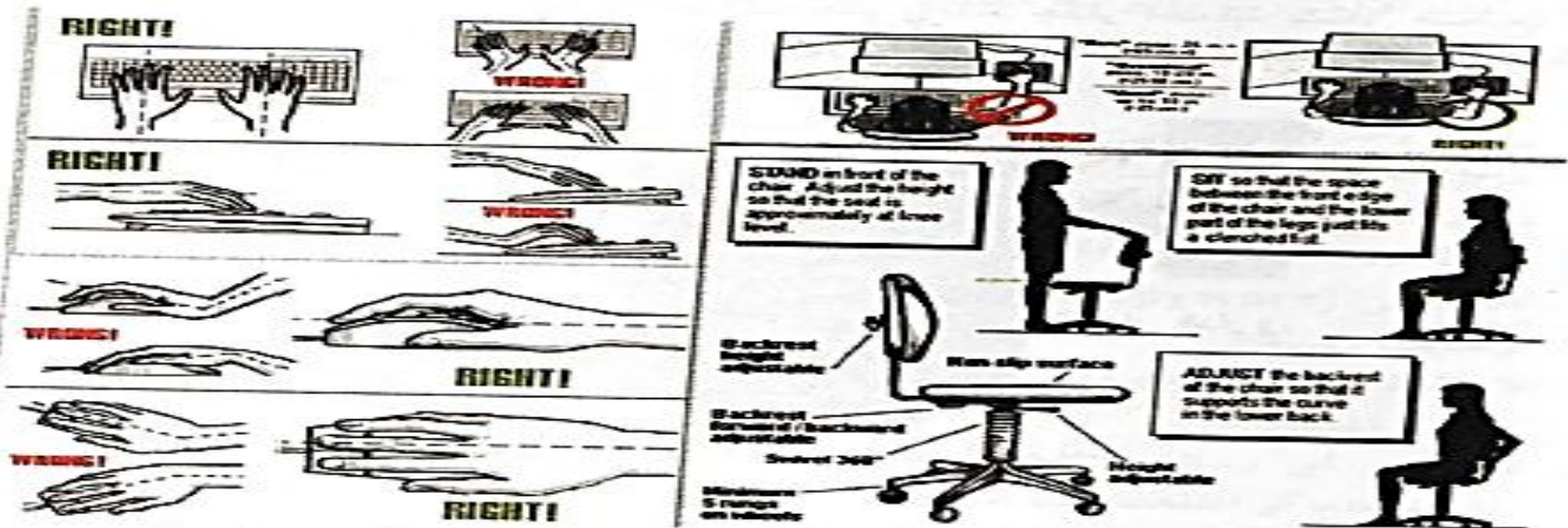
وسط افتراضي والعلاقات الخيالية لمن يدمنون على الإنترنت. وأفضل وقاية لذلك هو التوقف

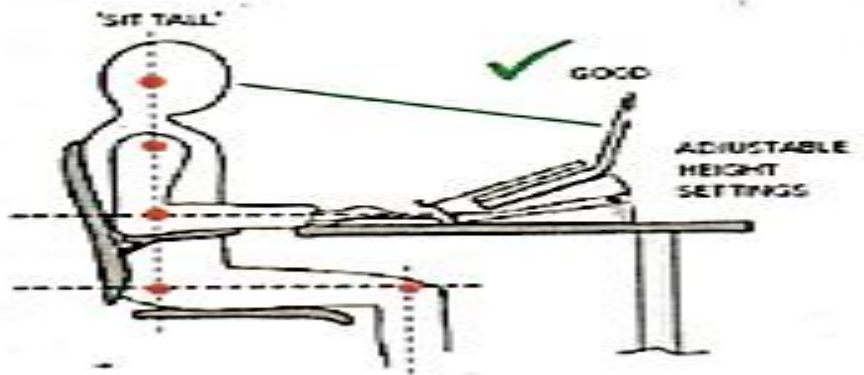
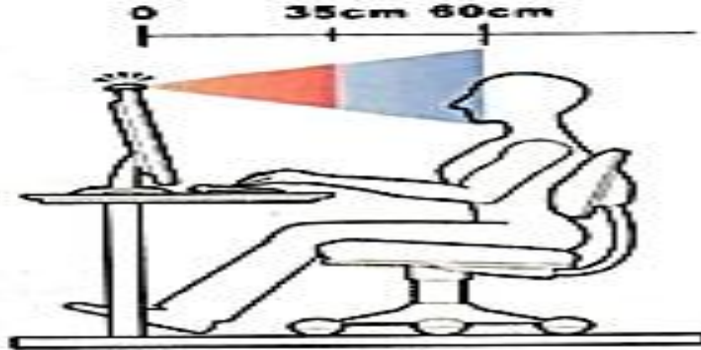
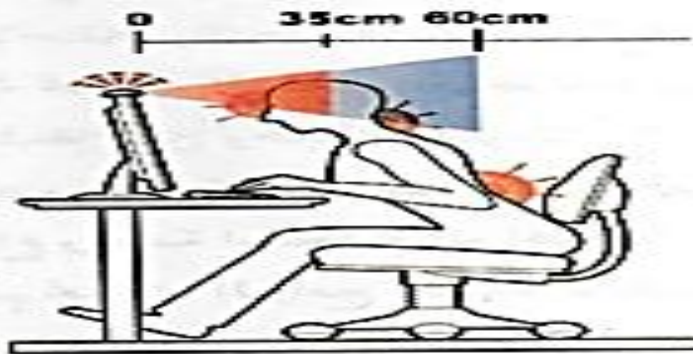
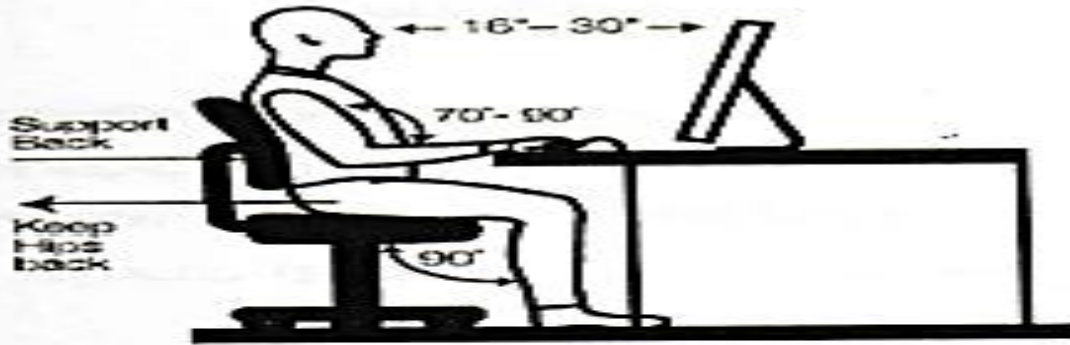
من حين لآخر عن العمل بالحاسوب، وبسط الساقين والكاحلين والقيام ببعض التمارين

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