الفصل السابع
المشاكل والأمان والأخطار

مشاكل الإنترنت والحلول:

مهما تكن مستخدماً لجهازك فى المنزل، أو كنت جزءاً من شبكة أعمال كبيرة فسوف تجد بعض مشاكل الاتصال، أو بعض مشاكل استخدام الإنترنت .

لا أتمكن من الاتصال بصفة عامة:

عندما لا تتمكن من الاتصال لأول مرة فهذا راجع إلى أسباب متعددة منها : عدم توصيل خط الهاتف مع المودم، أو عدم توصيف المودم بدقة ، أو عدم تثبيت برمجيات تشغيل المودم، وعلى الرغم من أن نظم التشغيل والأجهزة الحالية تعمل بخاصية التوصيل والتشغيل Plug and Play (PNP) إلا أنها قد لا تتمكن من تثبيت برنامج التشغيل بدقة لذلك فعليك أن تراجع : التوصيلات وتوصيف المودم ورقم هاتف مزود الخدمة، وبرمجيات تشغيل المودم .

عندما يكون هناك اتصال سابق فبرامجك وأجهزتك تعمل بطريقة طبيعية، لكن هناك صعوبة فى الاتصال ، أحياناً يجد المودم الخاص بك صعوبة فى الاتصال بالإنترنت ، وهذا غالباً يحدث عندما يكون هناك كثير من الناس يحاولون أن يكونوا على الإنترنت مباشرة فى ذات الوقت ومزود الخدمة مشغول ، وربما تقول نافذة طلب الاتصال إنك غير قادر على إنشاء اتصال ، وإذا حدث ذلك فإن برامج اتصال الإنترنت سوف يحاول الاتصال مرة أخرى ويمكنك أن تنقر على زر اتصال Connect لتحاول مرة أخرى.

بعد ذلك اسأل مزود الخدمة متى تكون الفترة الأكثر انشغالاً وحاول تجنبها، وغالباً إذا كانت لديك مشكلة اتصال فربما بها من الأفضل أن تغير مزود الخدمة .

كلمة السر غير صحيحة:

إذا كنت تتصل بمزود خدمة، وكنت مضطرا لكتابة كلمة السر تأكد من أنك تكتبها صحيحة تماما ففى بعض الأحيان يكون لدى النظام الذى يقبل كلمة السر حساسية الحالة "Case Sensitive" التى تعنى أنك تكون مضطرا إلى استخدام نفس الحروف الكبيرة والصغيرة التى استخدمتها فى نفس أماكنها كل مرة .

فشل التوثيق:

ربما تجد رسالة تقول بفشل التوثيق "Authentication Failed" وهذا يحدث عندما تحاول الاتصال، ويرسل المودم الخاص بك إشارات إلى خادم مزودك بالخدمة ، فيرد خادم مزودك بالخدمة هذه الإشارات فيما يعرف بالتصافح ، وهى عملية تخبر الخادم عمن تكون أنت وتتأكد من أن لديك السماح لاستخدام الاتصال بالإنترنت ، وإذا افتقد التوثيق فهذا يعنى أن التصافح لم يتم الاعتراف به ، وهذا قد يكون بسبب مشكلة فى اسم المستخدم، أو كلمة السر، أو مع مزود الخدمة، أو نتيجة انشغال خادم مزود الخدمة، أو ربما يكون بسبب تجهيز برامج الاتصال ، وعليك أن تتحدث مع مزودك للخدمة واطلب النصح ، أما إذا كنت تستخدم خدمة أرقام عامة فقم بتغيير الرقم ، وإذا لم تحصل على نتيجة فتأكد من خصائص الاتصال الهاتفى .

لا أستطيع الحصول على البريد الإلكترونى:

إذا كنت تتوقع بريداً إلكترونياً ولم يصل فقد لا يكون المرسل قد قام بإرساله فإذا تأكد لك أنه قام بإرساله فهناك عدة مشاكل ممكنة :

يمكن أن تكون المشكلة مع خادم مزودك بالبريد الإلكترونى ، وإذا كنت متصلاً مع ويب فربما تكون قادراً على أن تختبر الصفحة الرئيسة لمزودك، وابحث عن رابطة "خدمة الأعضاء" أو "الخدمات الإعلانية" وإذا كان مزودك ليس لديه تقرير

عن أى أخطاء فإن المشكلة ربما تكون مع مرسل مزود الخدمة، وعادة يقوم العديد من مزودى الخدمة بتصحيح الأخطاء خلال يوم أو أكثر .

هناك سبب آخر فالشخص الذى يحاول أن يتصل بك ربما يكتب العنوان بطريقة خطأ ، فتأكد من كتابة عنوان البريد الإلكترونى صحيحاً تماماً وإلا لن تـ.ستلم أى رسائل ، وتستطيع أن تحاول إرسال بريد إلكترونى له لتختبر صحة العنوان .

فيروس من خلال البريد الإلكترونى:

إذا كنت تشك وترتاب فى أن البريد الإلكترونى يحتوى على فيروس ، قم بحذفه فوراً بدون أن تفتحه، وتأكد من أنك حذفته من مجلد العناصر المحذوفـ.ة Deleted Items أيضا.

إذا حصلت على تحذير بفيروس من خلال البريد الإلكترونى، وأنت لست متأكداً تستطيع أن تبحث على موقع ويب عن معلومات الفيروسات مثل موقـ.ع www.F-secure.com/virus-info، وإذا حصلت على فيروس حقيقى عبر البريد الإلكترونى فقم بتشغيل برنامج حذف الفيروسات، واتصل بمزود الخدمة بمجرد معرفتك.

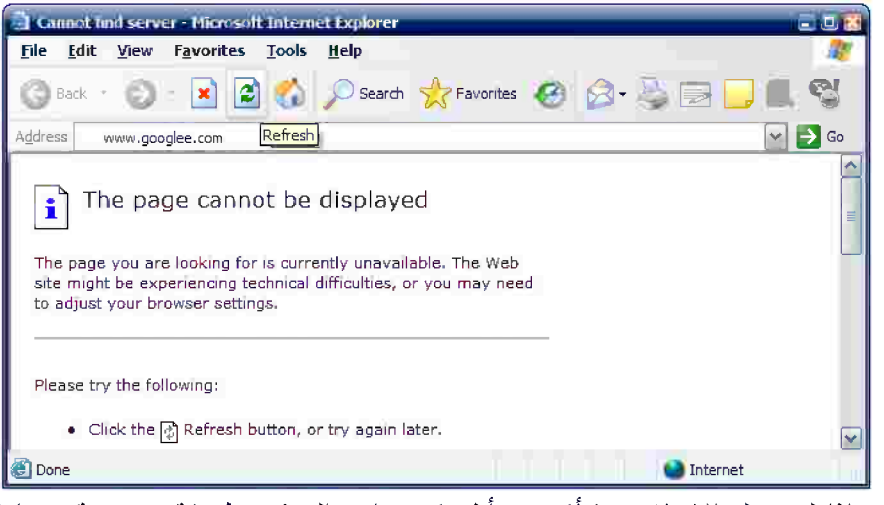
مشاكل شبكة ويب :

أصبحت اتصالات ويب أحسن وأكثر إتاحة طوال الوقت لكن المشاكل مازالت تحدث ، ومع احتقان الإنترنت (عندما يستخدم كثير من الناس الإنترنت فى وق.ت واحد) تظهر هذه المشاكل .

العنوان الخطأ :

ربما تكتب اسم الموقع، وعندما تضغط على مفتاح الإدخال تحصل على رسالة تقول: إن الصفحة لن تعرض، أو أن المتصفح غير قادر على عرضها ، أو أن.ه غير قادر على الاتصال مع الخادم ، أو أن الملف غير موج.ود "HTTP 404-file not found" .

هذا يعنى أن لديك مشكلة اتصال مؤقتة ، حاول النقر على زر إنعاش Refresh أولاً .



إذا لم يعمل الإنعاش ، فتأكد من أنك كتبت اسم الموقع بطريقة صحيحة ، حاول أن تكتبه مرة أخرى واهتم بالنهايات مثل .com , .org وغيرها ، وإذا كتبت عنواناً طويلاً جداً يمكن أن تجعله أقل طولا بالتوقف عند الصفحة الرئيسة للموقع وع.دم كتابة جزء العنوان بعد علامة / لتحاول أن تحصل على صفحة أخرى من نف.س الموقع ، ومن هناك يمكن أن تكون قادراً على الإبحار إلى الصفحة الت.ى تبح.ث عنها.

الصفحة غير متاحة:

عدم إتاحة الصفحة يعنى أنها قد اختفت من شبكة ويب، أو أن العنوان قد تغير،

أو أن هناك الأخطاء التى تمنع ظهور الصفحة، أو نتيجة تدمير الموقع من القراصنة، أو نتيجة حجب الموقع فى بعض البلاد .

تضع بعض المواقع الرسائل الإعلامية، أو برمجيات الانتقال الآلى عندما تفقد الصفحات ، لكن لا تقوم كل المواقع بفعل ذلك ، لكن عادة ما سوف تجد ما تبحث عنه فى موقع آخر، أما تغيير بعض هذه المواقع فعادة عندما يحدث هذا سوف تجد رسالة على الموقع الأصلى تعطيك العنوان الجديد أو يتم تشغيل بعض البرمجيات التى تنقلك إلى الموقع الجديد ، وإذا كان الموقع على مفضلتك فيجب أن تغير الاسم مستخدماً تنظيم المفضلات Organize Favorites ، وأحياناً قد تعيد المواقع إدارة وتشغيل الموقع آليا، أو قد تتيح لك النقر على اسم الموقع الجديد لتذهب إليه من الموقع القديم .

عندما تكون هناك أخطاء على الصفحة فقد تحمل الصفحة جزئياً ، وربما ترى رسالة تقول: إن هناك أخطاء فى تحميل الصفحة ، حاول أن تنقر على زر إنعاش Refresh .

بطء الاستعراض:

إذا كانت صفحات ويب تأخذ وقتاً طويلاً للتحميل فإن ذلك سوف يكون محبطاً جداً ومكلفاً إذا كنت تدفع من أصل الوقت على الخط المباشر .

ربما تكون هناك مشاكل مؤقتة مع موقع الخادم المستضيف ، حاول أن تنقر زر إنعاش Refresh أولا ، وقد تحدث هذه المشكلة أيضاً عند احتقان الإنترنت ، حاول الاتصال بالموقع فيما بعد فى وقت يكون فيه الاتصال مناسباً ويكون الاتصال أقل انشغالاً .

إذا وجدت أن صفحات ويب تأخذ وقتاً طويلاً للتحميل فقد يكون السبب أيضا بصفة عامة أن لديك إصدارا قديما من المستعرض ، وإذا كان هناك إصدار أكثر تحديثاً متاحاً على موقع ويب فانقله واستخدمه ، قد يكون السبب أيضا أن جهازك قد عمل لفترة طويلة وشغلت الذاكرة التخيلية ، أو لا توجد عليه مساحة ذاكرة كبيرة ، أو لا تتوافر فيه مساحة خالية على القرص الصلب ، أو قد لا يكون سريعا بما يكفى للتحميل السريع ، أو أنك ربما لا تملك المودم عالى السرعة .

الأمان والحماية من أخطار الإنترنت:

ملايين الناس يستخدمون الإنترنت وربما تجد هناك الذين يسيئون استخدامه، ومهما يكن فهناك الكثير من المحاذير التى تستطيع أن تتصدى لها، والتى تؤمن الإنترنت ليكون مكاناً آمناً قدر الاستطاعة.

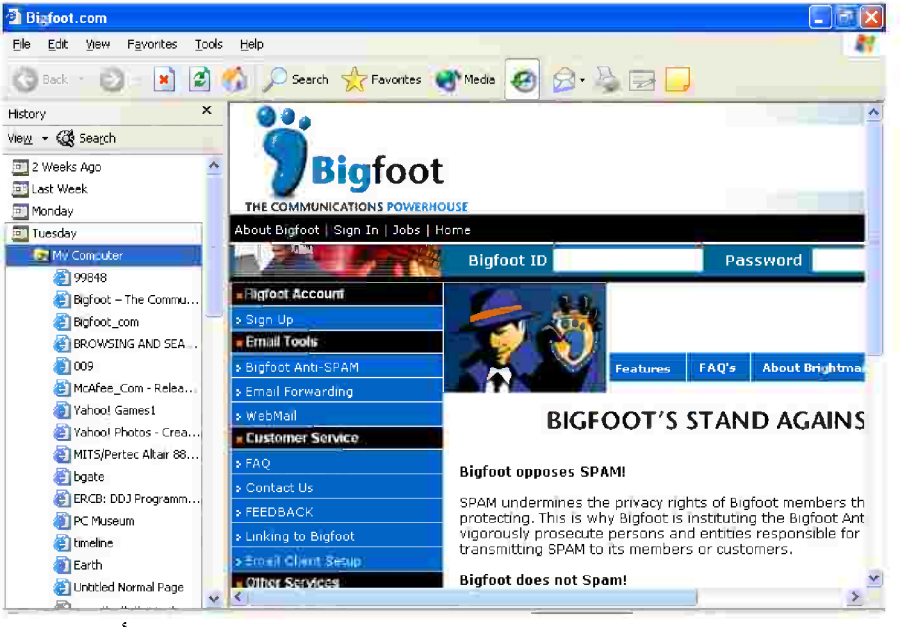
هناك أخطار كامنة على الإنترنت تتربص بمعلومات الأجهزة، والملفات، وبأولادنا وبطاقات الاعتماد المالى تجسسا وانتهاك خصوصية أو تلصصا أو اختراقا، وهى أخطار حقيقية يجب أن نعرف مدى خطورتها للمحافظة على سلامة الأولاد، وحماية البريد الإلكترونى، والتغلب على إدمان الإنترنت، وحماية بطاقات الاعتماد، والأجهزة، والبيانات، والخصوصية، ففى الإنترنت برامج الهجوم على الأجهزة وشبكات الحاسب، والتجسس، والفيروسات، وديدان الإنترنت، وأحصنة طروادة، والملوثات.

تختلف مصادر التهديد تبعا للقائمين بها وطرقهم فى الوصول إلى تنفيذ هذه التهديدات ومنها : التطفل والتجسس على البريد، والمزعجون والمحاولون، الاختراق، وجواسيس البريد الإلكترونى، ورصد لوحة المفاتيح، وتهديد الأولاد بالإباحية والجنس والعنف والأفكار المتطرفة، والعقائد الفاسدة ودس الأفكار والتقليد الأعمى، وإفقاد الهوية والانتماء، والنصب وتدليس الحقائق ونشر الأكاذيب وتزوير النصوص الدينية.

توجد بالفعل كافة أشكال وأنواع الأخطار على كافة خدمات الإنترنت دون استثناء لكن أكثرها فى المجموعات الإخبارية، ومواقع ويب والقوائم البريدية.

إذا أردت حقا حماية أولادك فيجب أن تقضى معهم وقتا أطول على الحاسب،

حتى لو لم تكن تعرف استخدامه ، أما إذا كنت تعرف استخدامه فقم بتتبع تـ.اريخ History المواقع لمتابعة المواقع التى تم الدخول إليها .



كما يمكنك معاينة الملفات View Files التى استعرضوها من مخبأ القرص .

هناك أيضا برامج تساعدك فى منع الوصول إلى مواقـ.ع غيـ.ر مرغوبـ.ة، أو موضوعات غير مرغوبة مثل برنامج Blocker أو برنامج Net Nanny فبرنامج مثل Net Nanny يتضمن قائمة مواقع يمكنك جعلها محجوبة ، وتجد برنامج Net Nanny فى العنوان http://www.netnanny.com .

باستخدام ذلك النوع من البرامج يمكن حجب المواد الخليعـ.ة، ومذ.ع معظـ.م الأشياء التى لا ترغب فى ظهورها على جهازك .

للعثور على برامج أخرى من هذا القبيل ابحث عن كلمة "blocking" بواسطة بحث ياهو Yahoo أو أى من مواقع البحث الأخرى على ويب، وستجد الكثير من البرامج مثل: SurfWatch, CyberPatrol, CYBERSitter, NetShepherd, TattleTale , Bess the Internet Retriever .

أصبحت أدوات الحماية والحجب من البنية الضمنية لبـ.رامج تـ.صفح ويـ.ب، وبرنامج التصفح إنترنت إكسبلورر يملك مثل تلك الأدوات.

لاستخدام تلك الأدوات اختر أمر خيارات الإنترنت Internet Options مـ.ن قائمة الأدوات Tools وستجد منطقة تشغيل، وتعطيل ميزة التـ.صفية، والحمايـ.ة

باستخدام كلمة مرور، ويمكنك ضبط هذه الميزة لحجب بعض المواقع حجبا كلي.ا، وإتاحة المرور إليها عبر كلمة مرور فقط .

مواقع الحماية على الإنترنت:

يمكنك البحث فى الإنترنت عن روابط المواقع التى تمنـ.ع التطفـ.ل، وتحجـ.ب المواقع غير المرغوب فيها ، وإذا استقبلت بريدا إلكترونيا غيـ.ر مرغـ.وب فيـ.ه تستطيع هذه البرامج ترشيح ومنع وصول البريد المتطفل إليك ، ومن المرشـ.حات المتاحة: البرنامج التجريبى على موقع Spam killer ، وإذا أردت معلومات عن الفيروسات راجع صفحة F- secure virus descriptions بموقعها ، وإذا أردت البرامج المضادة للفيروسات اتجه إلى موقـ.ع Symantec أو برنـ.امج نورتـ.ون Norton المضاد للفيروسات، أو على موقع ويـ.ب McAfee ، أو موقـ.ع Dr. Solomon لأجهزة الماكنتوش ، ولبرامج الترشيح يمكن زيارة مواقع ويب Net Manny أو موقع Cyber Patrol ، أو غيرها من المواقع .

البريد الإلكترونى :

لا تعط عنوان بريدك الإلكترونى للغرباء بمثل ما أنت لا تريد أن تعطى عنوان منزلك للغرباء أبداً ، وبالإضافة إلـ.ى ذلك فلماذ لا يكون لك أكثر من عنوان بريد مختلف؟

عادة ما تقوم الشركات بطلب ملء نموذج فيه عنوان بريـ.دك الإلكترونـ.ى، أو عندما تشترى المنتجات، أو تحمل البرامج من مواقع ويب لكن تأكـ.د مـ.ن أنـ.ك تستطيع بسهولة أن تجد تفاصيل اتصالاتهم على الموقع، وابحـ.ث عـ.ن صـ.ندوق استقبال أى إعلانات من الشركة حتى تتأكد من أنك لن تـ.ستقبل بريـ.دا مـ.نهم ، وبخلاف ذلك تستطيع حجبه .

التفاصيل الشخصية :

العديد من مواقع ويب خاصة مواقع التسوق تـ.سألك أن تمـ.لأ نموذجا فيه معلومات تشمل اسمك وعنوانـ.ك وعنـ.وان البريـ.د الإلكترونى، ورقم الهاتف حتـ.ى يمكـ.نهم الاتصال بك ليخبروك عـ.ن عـ.روض خاصة ، لكـ.ن لا تقـ.م بإعطـ.اء هـ.ذه التفاصيل إلا إلى شركات ومؤسـ.سات معروفـ.ة وشـ.هيرة وحسنة السمعة ، وسوف تجد أن معظم شركات الإنترنـ.ت

المعتمدة الصادقة تحافظ جيداً على سياسة الخصوصية، التى تخبرك أنها لن تقوم بتمريرها إلى شركة أو شخص آخر .

الفيروسات :

يمكن لجهازك أن يلتقط الفيروسات إذا نسخت ملفات من حاسب غير معروف أصابته العدوى Infected ، أو أن نفتح اتصال بريد إلكترونى غير معروف ، وتنتشر الفيروسات سريعاً على الإنترنت نتيجة اتصالات الحاسبات بعضها ببعض على الرغم من جدران النار وبرمجيات الحماية فغالبا ما يتم توزيعها عبر البريد الإلكترونى وقد انتشر فيروس رسالة بريد جملة "أنا أحبك" I love you وأصاب ملايين الأجهزة حول العالم فى خلال 24 ساعة، تأكد دائما من أن لديك برامج مضادة للفيروسات مثبتة على جهازك واحفظها، وقم بتحديثها.

عمليات تحميل ونقل ملفات قد تؤدى إلى نقل فيروسات تختبئ فى ملفات البرامج ثم تقوم بنسخ نفسها إلى البرامج الأخرى فى الحاسب عند تشغيلها ، وهى تتسبب فى أضرار حقيقية .

تقوم شبكات الخدمة المباشرة الكبرى دوريا بفحص أجهزتها وبرامجها والملفات المنقولة من خلالها فالمشتركون فى تلك الشبكات لا يمكنهم إرسال ملفات إلى منطقة عامة، بل ينبغى لهم إرسال الملفات إلى منطقة خاصة للتحقق من نظافة الملفات قبل إرسالها لكن الأمر على الإنترنت يعود إلى تقدير كل مسئول عن أنظمة الخدمة.

يستخدم مصطلح الفيروسات للإشارة إلى برامج صغيرة تلحق نفسها بملف ما وتقوم بإعادة إنتاج نفسها (تكاثر) وتتميز بسرعتها فى إعادة إنتاج نفسها وتظل كامنة فى بعض البرامج قابعة بانتظار تاريخ أو حدث معين لتقوم بحركتها، وتنسخ نفسها من ملف إلى أخر ومن حاسب إلى آخر، وتعمل بشكل مستقل عن ملفات التشغيل الأخرى وتقوم بالسيطرة على الذاكرة ومساحة القرص.

لا يستطيع الفيروس أن يوجد كملف مستقل بحد ذاته بل عليه أن يلتصق مذ البداية ببرنامج آخر.

أعراض الإصابة بالفيروس تظهر على شكل واحد أو أكثر. ومن الأعراض :

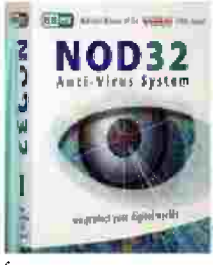
نقص الذاكرة، عرض رسائل خطأ ، تغير عدد ومكان الملفات وحجمها ، ظهور حروف غريبة عند استخدام لوحة المفاتيح ، توقف النظام ، عمل القرص الصلب بطريقة عشوائية.

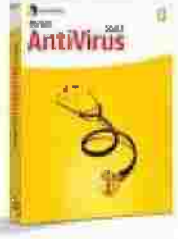
والفيروسات بهذا هى برامج تنتج تلحق نفسها ببرامج أو ملفات عن طريق تزييف أو تعديل توقيع البرنامج الاصلى (مجموعة أرقام ثنائية) ، وتتمكن هذه البرامج من تدمير البرامج والمعلومات، أو إصابة الأجهزة بالخلل بعدة طرق .

من هذه البرامج ما يعمل مباشرة عند الإصابة، وبعضها يعمل عند تنفيذ أمر ، وبعضها الاخر يعمل فى توقيت أو تاريخ مبرمج ، وتتميز برامج الفيروسات بقدرتها على التكاثر والاختباء والانتقال عن طريق نقل الملفات بين المستخدمين .

بعد نشاط الفيروس يقوم بنشاطه التخريبى بناء على تصميمه؛ فهناك ما يقوم بعرض رسالة، وهناك ما يقوم بحذف أو تعديل ملفات، وهناك من يقوم بنسخ نفسه لشلل الجهاز، وهناك ما تقوم بمسح معلومات القرص .

إذا كان فى نيتك تحميل وجلب ملفات من الإنترنت؛ فيجب استخدام برنامج جيد مضاد للفيروسات، وهذا النوع من البرامج متوافر، وفى كل مرة تقوم فيها بجلب ملف يتضمن برنامجا قم بفحص ذلك الملف بواسطة برنامج مكافحة الفيروسات .



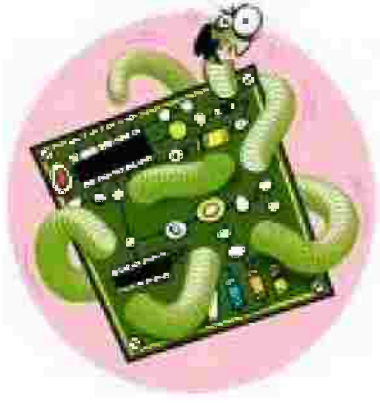


تأكد من الاحتفاظ بنسخة احتياطية للمعلومات المهمة، وبالرغم من أن النسخة الاحتياطية قد تصاب بالفيروسات أيضا لكن عند حدوث إصابة يمكن جلب النسخة الاحتياطية وتنظيفها كما أن بعض برامج النسخ الاحتياطى تقوم بالتحرى عن الفيروسات أثناء عملية النسخ .

تتم الوقاية بالحصول على برنامج متخصص ضد الفيروسات مع متابعة تحديثه.

القرصنة والاختراق:

يعنى الاختراق دخول شخص على جهاز آخر، أو ربط جهازين بعضها ببعض عن طريق المودم وباستخدام بروتوكول TCP/IP وبذلك يمكن الـ.سيطرة عل.ى الجهاز الآخر بطريقة أو أكثر، إما بالتخفى أو بطرق ظ.اهرة ، ويمك.ن إرس.ال ملفات أو تحميل ملفات وإجراء محادثة أو كتابة أو مسح معلومات .



يتمكن بعض المتصلين بشبكة الإنترنت من استغلال الثغرات فى نظم التـ.شغيل وبرمجيات الاتصالات ليتمكنوا مـ.ن الاتـ.صال بـ.أجهزة الحاسـ.ب بـ.دون إذن ، ويستطيعون ربط أجهزتهم الخاصة بالشبكات ويفتحون ملفات خاصة على الأجهزة الأخرى ، ويقومون بقراءة أو تغيير المعلومات فى هذه الملفـ.ات ، وقـ.د يـ.تمكن بعضهم من العبث بكلمات السر، أو الوصول إلى بيانات بطاقات الائتمان لـ.سرقة المال والبضائع ، وإذا كان جهازك يعمل على شبكة، أو كان دائماً علـ.ى اتـ.صال بشبكة الإنترنت فتذكر أن هناك آخرين ربما يكونون قادرين على الوصـ.ول إلـ.ى ملفاتك ، وتأكد من أن لديك بعضاً من الحماية والمعروفة ببرمجيات جـ.دار النـ.ار Firewall .

حصان طروادة Trojan هو برنامج تجسس يعمل على فتح منفذ فى الجهاز ، وتصل هذه البرامج عن طريق البريد الإلكترونى أو جلسات الدردشة .

لمعرفة حدوث الاختراق يمكن تنفيذ الآتى :

الـ. ..دخول إلـ. ..ى موقـ. ..ع http://www.privacy.net ، أو موقـ. ..ع http://www.consumer.net .

ثم اطلب فحص الحاسب أثناء الاتصال بشبكة الإنترنت ليعرض محتويات الجهاز، كما تستطيع من المواقع التالية الحصول على معلومات عن جهاز، والاختراقات التى تمت .

لحماية النظام من الاختراق

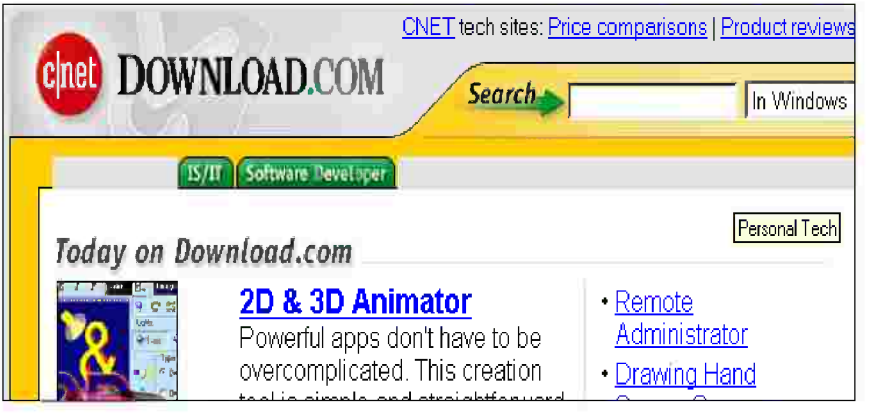
- تحديث البرامج المضادة للفيروسات .
- منع استقبال الملفات أو البرامج أو الصور من أشخاص موثوق بهم .
- عدم فتح ملفات منقولة إلا بعد قطع الاتصال، وبعد فتحها يتم البحث عن الفيروسات .
- الحرص فى نقل ملفات مرفقات البريد الإلكترونى .
- استخدام كلمات سر قوية طويلة متغيرة .
- عدم تحميل برامج من موقع غير معروف أو موثوق به .
- عدم جعل الحاسب المتصل بالشبكة على وضع مشاركة ، وللتأكد افتح لوحة التحكم وانقر أيقونة شبكة الاتصال ثم مشاركة الملفات والطباعة وتأكد من عدم إتاحة الخيارات .
- عند استخدام ويندوز Windows يمكن تحميل ملف حماية القرص الصلب من المتسللين عبر الشبكة بنقله من موقع شركة مايكروسوفت Microsoft .
- استخدام برامج مكافحة القرصنة التى تستطيع الإعلام عن محاولات الاختراق والتأكد من سلامة النظام، ومعرفة وقت التعرض لمحاولات الاختراق ، وبوابة الدخول ومعلومات أخرى ، ومن هذه البرامج AntiBo , Lookdown , Zoonalaram .

فى برنامج المتصفح ومن قائمة أدوات اختر خيارات الإنترنت ثم خيارات

متقدمة ثم قم بإلغاء اختيارات تمكين تسجيل دخول جافا، وتمكين جهاز تحكم جافا ، ثم اختر التأمين ثم تخصيص المستوى ، واختر تعطيل، أو مطالبة ملفات تعريف الارتباط cookies .

لإزالة الإعلانات التى تقفز على الشاشة يمكن استخدام البرنامج المجانى OptOut المتاح من الموقع http://grc.com .

أو ابحث فى موقع التحميل www.download.com .



أحصنة طروادة:

برامج تبدو آمنة ومفيدة لكنها تقوم بأعمال غير مشروعة فى الخفاء نتيجة زرع برامج ذاتية التشغيل بها دون علم المستخدم.

المادة العدوانية:

الناس يكونون أحرارا فى نشر أى شىء على الإنترنت مهما كان ، وبالإضافة إلى المتعة والأشياء القيمة توجد أيضا المعلومات غير الـ.سارة وغيـ.ر المناسـ.بة والخطيرة ، وتستطيع برامج الاستعراض تعديل عرض الصفحات لوقف وحجـ.ز الاتصال مع مواقع معينة، أو رفض أنواع معينة من المواد والموضوعات .

إذا كنت فى حجرة دردشة وبعض الأشخاص يقولون أشـ.ياء لا تعجبـ.ك فـ.لا تستجب لهم، وإذا أصروا فاخرج من الغرفة .

المواقع المريبة:

قد تصل إلى موقع مريب وغير لائق رغما عنك تدفعه شبكة الإنترنت أو آلات البحث ، وقد تدخل أنت بنفسك إلى موقع مريب رغبة فى الاستكشاف ، ويمكنـ.ك تجنب الوقوع فى هذا النوع من المشاكل من خلال تفادى تلك المواقـ.ع بالدرجـ.ة الأولى .

المقابلات والمواعيد:

بعض الذين تدردش معهم على الخط المباشر ربما يقترحون موعدا ولقاء فـ.ى الحياة الحقيقية، ومن الطبيعى أنها فكرة سيئة ، تذكر أنه من السهل علـ.ى الذ.اس

على الخط المباشر أن يتظاهروا بعرض أنفسهم كشخصيات غير حقيقية ، وإذا لم تستطع أن ترى شخصا ما أو تسمع صوته، فليست لديك أية فكرة عنه إذا كان ذكرا أو أنثى فى العشرين أو فى الستين ، ولتجنب خيبات الأمل أو الخطر من الأفضل أن تحتفظ بصداقات الخط المباشر فقط على الخط المباشر .



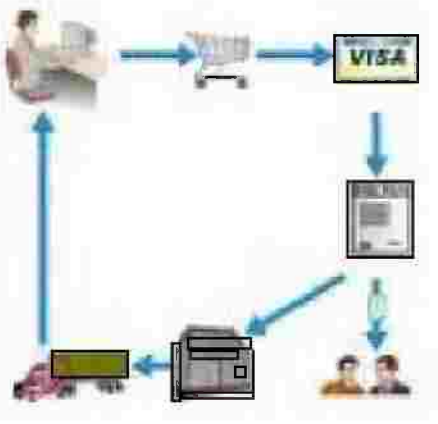

الشراء على الخط المباشر:

إذا قررت أن تشترى شيئا على الإنترنت تأكد من أن الموقع الذى تشترى منه مؤمن قبل إعطائه أى تفاصيل مالية ، فالموقع المؤمن سوف يؤمن تفاصيلك داخل كود خاص بك لذلك لن يستطيع أى شخص أخر أن يستخدمها ، وسوف تجد أن كلا من برنامج مايكروسوفت إنترنت اكسبلورر Explorer وبرنامج نتسكيب نافيجاتور Netscape سيظهران قفلا معلقا على نافذة المستعرض عندما يكون موقعك مؤمنا.


العديد من الناس مختصون بالاحتيال على الإنترنت، لكن على الرغم من ذلك فمن الممكن ارتكاب الجريمة على الخط المباشر، وليس على الخط غير المباشر .

سرقة بطاقة الاعتماد:

التسوق على الإنترنت قد يؤدى إلى سرقة رقم بطاقة اعتمادك المالى، فاستخدام بطاقة الاعتماد المالى على الإنترنت ينطوى على الخطورة مع مراعاة أن عمليات السطو على أرقام بطاقات الاعتماد على الإنترنت عمليات نادرة، ويمكن لتلك العمليات أن تحدث لكن من قبل شخص ماهر فى مجال الحاسب ويعرف ما يقوم به .



إضافة إلى ذلك فإن برنامج نتسكيب، وبرنامج إنترنت إكسبلورر هما الأكثر استخداما بين برامج التصفح ويتضمنان آلية ضمنية لترميز المعلومات، كما أن العديد من مواقع ويب تستعمل خدمة تتضمن آلية ترميز ضمنى وعندما يتم إرسال رقم البطاقة من خلال أحد هذين البرنامجين إلى خادم يعمل بنظام ترميز للحماية فإنه يتم ترميز المعلومات مما يجعلها غير مجدية بالنسبة للغير .

لمعرفة المواقع التى تتمتع بالحماية لاحظ رمز القفل الصغير الموجود فى الزاوية السفلية للنافذة، فهذا القفل هو الرمز الذى يستخدمه المتصفح إنترنت إكسبلورر للإشارة إلى أن الموقع يتمتع بالحماية ، أما برنامج نتسكيب فيستخدم صورة مفتاح فى الزاوية السفلية اليسرى للإشارة إلى الغرض نفسه فإذا كانت صورة المفتاح مكسورة فذلك يشير إلى أن الموقع لا يتمتع بالحماية.

ليس المهم إذن الطريقة التى تستخدمها لتمرير رقم بطاقتك إلى البائع، بل المهم ما يحدث بعد أن يتم تسلُّم الرقم وكيف سيتصرف فيها البائع .

جمع المعلومات:

تقوم المواقع المختلفة فى شبكة الإنترنت بجمع معلومات عن المستخدمين للشبكة ، ويتم جمع المعلومات عن مستخدمى الشبكة بعدة طرق منها: كعكة الإنترنت ، وبقة الإنترنت ، وبريمجات جافا، وبرامج نصوص جافا سكريبت وغيرها .

بقة الإنترنت : عبارة عن صور صغيرة جدا تبلغ 1 بكسل، أو رسالة إلكترونية ضمن لغة ترميز صفحة الإنترنت وتستقر فى الشاشة الخلفية ولا يستطيع المستخدم ملاحظتها .

يمكن متابعة مستخدم الإنترنت عن طريق برامج النصوص مثل: جافا سكريبت

أو بريمجات جافا الصغيرة التى تنزل إلى الجهاز، وتبدأ العمل تلقائيا فى خفاء دون علم المستخدم خاصة لدى مواقع الدردشة .

يمكن التحكم فى استقبال كعكة الإنترنت، وجافا سكريبت، وبرمجيات جافا فـ.ى المتصفح لمنعها أو السماح بها أو اختيار مستوى أمان لها ، أمـ.ا بقـ.ة الإنترنـ.ت فتزرع فى الصفحة أو الرسالة الإلكترونية وتبدأ عملها حال فتح صفحة أو رسـ.الة ولا يمكن التحكم بها.

تقوم المواقع بالحصول على رقم بروتوكول الإنترنت الخاص بالمتصل، ثم يتم إصدار رقم خاص لتعريفه ومتابعته داخل المواقع عند الانتقال من صـ.فحة إلـ.ى أخرى، أو من موقع إلى آخر وبعد ذلك يتم التعرف على الجهاز، وسرعة المعالج ونظام التشغيل المستخدم ، ونوعيـ.ة المتـ.صفح المـ.ستعمل ، وتـ.سجيل المواقـ.ع والصفحات التى يتردد عليها المتصل ، ورصد توجهاته ورغباته من الخـ.دمات أو السلع والصفحات المفضلة لديه ، وعند تعبئة استمارة أو طلب يتم تخزين وحفـ.ظ معلومات المستخدم من: اسم وتاريخ ميلاد والعنوان وعنوان بريد وغيرهـ.ا مـ.ن البيانات .

تستفيد المواقع من جمع المعلومات بتحليلها وتصنيفها وعمل إحصاءات مفيـ.دة فى إدارة وتخطيط السياسات والإعلانات كما تبيع أو تبادل هذه المعلومـ.ات مـ.ع غيرها من المواقع التى تعمل فى أنشطة البيع والتسويق والترويج والإعلان بحيث يتم إرسال إعلانات وتسويق خدمات للمهتمين بها .

كما يتم رصد السلع والخدمات التي قمت بشرائها مؤخرا بحيث يتم توجيه السلع أو الخدمات المتعلقة بما اشتريت فمثلا: لو قمت بشراء جهاز حاسب من الإنترنت فهذا يعني أن عليهم توجيه الإعلانات الخاصـ.ة بملحقـ.ات الحاسـ.ب كالطابعـ.ات والأحبار لعميل جديد .

كانت المواقع تجمع المعلومات اعتمادا على عنوان بروتوكول الإنترنت IP ثم أصبحت تقوم بتحديد رقم الهاتف وتسجيل كل ما تقوم بكتابته أو تستقبله فى غرف الدردشة أو الرسائل الإلكترونية .

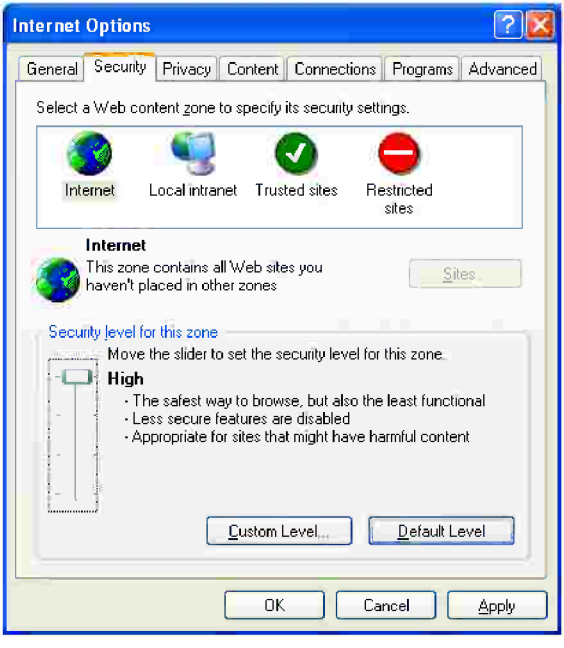
نتيجة لتتبع المواقع للأفراد على شبكة الإنترنت قامت صناعة تهتم بتقديم حلول التتبع ومنع التتبع ببرامج شركات متخصصة تحمى الأمن والخصوصية .

تحاول شركات المتصفحات سد الثغرات الأمنية، وإحكام طرق التجسس وزيادة تحكم المستخدم ، وتتوفر شركات خدمة التصفح الحر بحيث تدخل إلى الشبكة تحت مظلتهم وتستطيع استخدام عنوان بروتوكول الإنترنت الخاص بهم ولا يظهر عنوان المستخدم ، كما يتم تخزين كل البرامج والكعك فى أجهزة هذه الـ.شركات لتجنـ.ب التتبع .

كعك الإنترنت :

كعك cookies الإنترنت هى ملفات نص صغير ، وما إن تزر موقـ.ع ويـ.ب وتدخل صفحة حتى يقوم الموقع بإصدار نسختين من الكعكة: واحدة تبقى فى خادم الموقع ، والأخرى يتم إرسالها لزائر الموقع (قد تكون هناك أكثر من كعكة) حـ.ال تعبئة استمارة أو بيان .

يقوم الموقع بتخزين الكعكة على القرص الصلب للزائر فى ملـ.ف مـ.ع كعـ.ك المواقع الأخرى التى يتم تخزينها دون أن تشعر أنت ، وتبدأ الكعكة مهمتها بجمـ.ع المعلومات وإرسالها إلى مصدرها أو إلى شركة تحليل المعلومات .



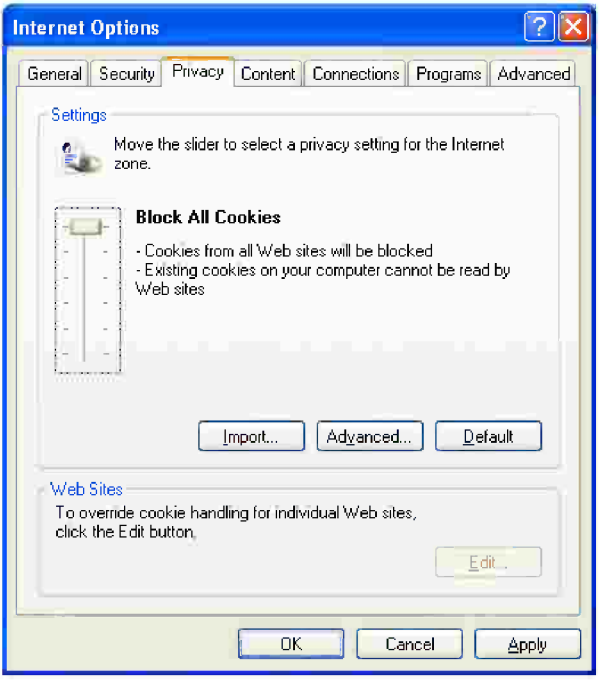
ليست كل أنـ.واع الكعـ.ك مخصصة لجمـ.ع معلومـ.ات فهناك كعك يساعد على إتمام مهام مثل الشراء أو سـ.رعة تحميل صفحة عنـ.د تكـ.رار الزيارة.

يمكن التحكم بالمتـ.صفح لعدم السماح له بتخزين الكعك على القرص الـ.صلب بنقـ.ر أيقونة المتصفح بالزر الأيمن للفأرة واختيار أمر خصائص Properties ثـ..م اختيـ..ار تبويـ.ب الـ.سرية Security وفيه تختار مستوى الـ.سرية مثل المخصص Costom Level .

أو تختار الكعك تحت بند الخصوصية Privacy ورفع مستوى تأمين الخصوصية لإغلاق كافة أنواع الكعك Block All cookies .

لتخلص من الكعك Cookies يمكن استخدام برامج منها:

برنامج Zeroclick الذى يمكن تحميله مجانا ليمنع الكعك من الالتصاق بالجهاز، أو من الموقع:



http://www.osdn.com/redirect.shtml/86321.html.

هناك برامج تخير بين قبول الكعك Cookies أو رفضه مثل: برنامج Cookie Pal فى موقع www.kburra.com ، وبرنامج Cookie Cop بموقع www.pacificnet.net .

البرامج ذاتية التحميل:

تم تطوير وتصميم تقنيات فى الإنترنت تيسر وتسرع نقل المعلومات عبر

الشبكة وتحميل هذه التقنيات على أجهزة المستخدمين لتوفر سهولة وسرعة التصفح والإبحار، وجعل الصفحات أكثر جاذبية وحركة ، لكن انتشار هذه التقنيات ساعد على وجود سوء استخدام من بعض المبرمجين والمستخدمين مما تسبب فى مشاكل أمنية على شبكة الإنترنت ، ومن هذه التقنيات البرامج ذاتية التحميل مثل: تحكمات أكتف اكس ActiveX وبريمجات جافا Java Applets وبرامج النصوص مثل جافا سكريبت Java Script وغيرها .

ماذا أفعل للوقاية من البرمجيات الضارة ؟

- استخدام برامج مضادة للفيروسات حديثة، واقتناء واستخدام جدران النار .
- عدم تحميل البرامج المجانية مجهولة المصدر .
- عدم فتح الرسائل الإلكترونية غير المعروفة خاصة التى تحمل ملفات مرفقة .
- تعديل مستوى أمن المتصفح بحيث لا يتم قبول نزول برامج .
- قبول البرامج التى تحمل توقيعا إلكترونيا لمصدرها .
- شراء نسخة أصلية حديثة من نظام التشغيل .
- استخدام أحدث نسخ برامج التصفح .
- التحكم بملفات المشاركة فى الشبكة .
- حماية الجهاز بكلمة سر .
- تجنب تنزيل، أو تحميل ملفات برامج من مصادر غير موثوق بها .
- استخدام برنامج تشفير المعلومات والرسائل الإلكترونية .
- عدم القيام بالشراء من شبكة الإنترنت دون التأكد من استخدام خادم آمن بوجود علامة القفل المغلق في المتصفح .
- تجنب الموافقة على حفظ اسم المستخدم، وكلمات السر فى أى وقت لأنك لو وافقت فستسهل العملية على أى مستخدم آخر يستخدم الجهاز لأنه يجدها مخزنة وجاهزة .

من برامج الحماية :

- برامج الحماية من الفيروسات Antivirus Program .
- برامج جدران النار Firewall Programs .
- برامج تشفير المعلومات Encryption Software .
- برامج تشفير البريد الإلكترونى .

إدمان الإنترنت :

بعض تسهيلات الإنترنت مثل الألعاب والدردشة يمكن أن تصبح مزعجة ومرهقة جدا، وقد تسبب إدمان المراهقين للبقاء طويلا على الخط .

إذا كنت تدفع من أجل الوقت الذى تقضيه على الخط المباشر فهذا خطأ مكلف إلا أن استخدام الحاسب لأى غرض لفترة طويلة أيضا يمكن أن يسبب المخاطر الصحية ، ويجب أن تعطى لنفسك راحة لمدة عشر دقائق كل ساعة تستخدم فيها الحاسب لتريح عينيك وجسدك .

الصحة والإنترنت:

يمكن تقسيم المخاطر الصحية التى يتعرض لها مستخدم الإنترنت والحاسب إلى قسمين رئيسيين هما :

- مخاطر قصيرة المدى .
- مخاطر بعيدة المدى .

كما يمكن تقسيمها بصورة أخرى إلى مخاطر: نفسية وبدنية واجتماعية فهناك بالطبع مخاطر بدنية ونفسية قصيرة المدى مثل توتر وإجهاد عضلات العين، والشعور بحرقان العين، والقلق النفسى، وضعف التركيز إضافة إلى المواقع الإباحية التى تؤدى إلى الإثارة والشعور بالكبت، أو تفشى المشاكل الاجتماعية.

المخاطر بعيدة المدى تتضمن آلام العضلات والمفاصل والعمود الفقرى وآلام الرقبة وأسفل الظهر والرسغ كما يمكن أن تظهر أعراض الأرق ، والانفصام ، مع الأوهام ، وعلاقات خيالية فى منتديات الحوار ، كما يمكن أن يؤدى إلى زيادة الوزن نتيجة قلة الحركة وتناول وجبات ومشروبات عالية السعرات .

من أكثر المخاطر تأثيرا مخاطر الإشعاع الصادر من أجهزة العرض وتأثير المجالات الكهرومغناطيسية للدوائر الكهربائية .

لتجنب المشاكل قدر الإمكان يستحسن اتباع الإرشادات التالية :

- عدم الجلوس طويلا أمام الحاسب دون حركة ، ويجب تحريك أجزاء الجسم على فترات بالقيام، وعمل أى مهمة مثل تناول كوب ماء، أو إعداد الشاى أثناء تحميل البرامج ، وممارسة بعض الحركات الرياضية البسيطة مثل تحريك الأصابع وإغماض العينين والتنفس العميق والوقوف وشد العضلات ورفع الذراعين فى اتجاهات مختلفة وتحريك الساقين لتخفيف ضغط العضلات وتنشيط الدورة الدموية .
- تجنب إجهاد العين بجعل ارتفاع ومكان الشاشة مناسبين بأن يكون ارتفاع الشاشة مناسبا لمستوى النظر كخط مستقيم أعلى الحدود العليا للشاشة ، وأن تكون شاشة كبيرة بحجم 15 بوصة على الاقل ، ووضع الشاشة فى مكان مناسب لتقليل انعكاسات الإضاءة الخلفية أو النوافذ ، وتقليل التحديق فى الشاشة بأخذ فترة راحة كل 15 دقيقة بالنظر إلى منظر مختلف فى الغرفة بعيدا عن الشاشة لمدة نصف دقيقة أو إغماض العين ، وتكرار الرمش أو إغماض العين بين فترة وأخرى لتجنب الجفاف .
- تجنب آلام العمود الفقرى والمفاصل بالجلوس على مقعد مناسب الطول له مسند رأس وظهر ، واجلس بطريقة صحيحة بحيث يكون الرأس والرقبة والعمود الفقرى فى وضع مستقيم ، بطريقة جلوس سليمة بحيث تشكل المفاصل زاويا قائمة ، والمحافظة على استقامة اليدين قدر المستطاع أثناء الكتابة على

لوحة المفاتيح أو استخدام الفأرة مع جعل المرفق أقرب للجسم بزاوية قائمة بين العضد والساعد .

- تجنب تأثير إشعاعات الشاشة والدوائر الإلكترونية بتقليل آثارها عن طريق الابتعاد عن مصادرها بمسافة لا تقل عن نصف متر ، واستخدام شاشة جيدة تحجب الإشعاعات ، وإذا كانت الإشعاعات تصدر فى جميع الاتجاهات فيجب الابتعاد عنها من كل الاتجاهات خاصة فى المؤسسات ومقاهى الإنترنت عندما تكون شاشة الزميل خلف رأس الزميل الآخر مباشرة ، كما يمكن تقليل إجهاد العين وتأثير الإشعاعات باستخدام المرشح Filter وعمل زاوية ميل بين واجهة الشاشة، ومواجهة المستخدم .
- تجنب الآثار النفسية والاجتماعية بالتغلب على إدمان الألعاب، ومواقع الدردشة وفهم حقائق التضليل والكذب والخداع وإخفاء الحقائق عن الآخرين، وتجنب الدخول فى مهاترات ومغامرات تسبب الأرق وتشوش الأفكار.