

3.8. أمن الشبكة – Network Security

يمكن حماية شبكة الكمبيوتر من المخاطر التي يمكن أن تتعرض لها من خلال اتباع سلسلة من الإجراءات واستخدام مجموعة من الأدوات الوقائية، ونقع مسئولية حماية الشبكة على مدير النظام (System Administrator) والذي بدوره يقوم بالأمور التالية :

- إدارة حسابات المستخدمين بواسطة مدير الشبكة :

مدير الشبكة (Administrator) هو الشخص المسئول عن إدارة شبكة الكمبيوتر وتشمل العملية الإدارية : إدارة المستخدمين والمجموعات والمصادر و البرامج والأجهزة. وحتى يتمكن أي شخص من استخدام الشبكة وتسجيل دخوله عليها لابد أن يكون له حساب مستخدم

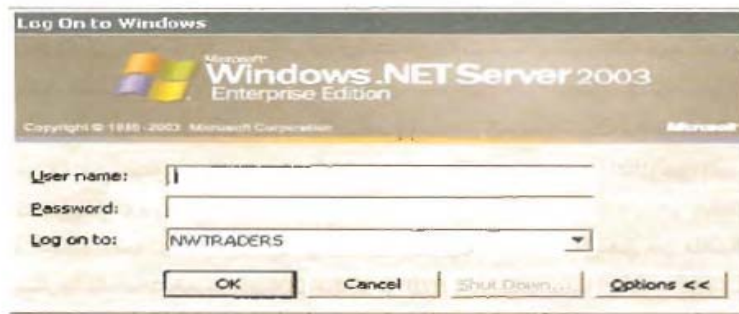


(Account User) وكلمة سر (Password) ويمكن تشبيه حساب المستخدم ببطاقة الانتماء وكلمة السر بالرقم السري للبطاقة، فإذا اجتمع الاثنان معا و بشكل صحيح عندها يستطيع المستخدم تسجيل دخوله على الشبكة والاستفادة من الخدمات المتوفرة عليها. ومن الجدير

بالذكر أن مدير النظام هو الذي يقوم بإنشاء حسابات للمستخدمين (User Accounts).

- توثيق حسابات المستخدمين :

حتى يستطيع المستخدم تسجيل دخوله على الشبكة والاستفادة من الخدمات والمصادر المتوفرة عليها لابد له من أن يقوم بكتابة اسم المستخدم (User Name) وكلمة السر (Password) الصحيحان بعدها يقوم نظام التشغيل من التحقق من هوية المستخدم فإذا وجد أن هناك تطابق ما بين ما كتبه المستخدم وبين ما هو متوفر لديه في قاعدة البيانات الخاصة بحسابات المستخدمين يسمح له بالدخول وغير ذلك سوف تفشل عملية تسجيل الدخول ولن يستطيع المستخدم تسجيل دخوله على الكمبيوتر ومن ثم على الشبكة.



- حماية الشبكة بواسطة الجدار الناري :

الجدار الناري (Fire Wall) يستخدم في البيانات للعزل بين الشبقتين أو المكاتب وذلك لمنع انتشار النار من مكان إلى آخر، وكذلك الأمر فإن الجدار الناري للشبكة هو عبارة عن برنامج أو جهاز كمبيوتر مزود بمعدات و برامج خاصة لحماية الشبكة الخاصة بالشركة من شبكة الإنترنت العامة وذلك لمنع تسلس الفيروسات أو الهاكرز من اختراق الشبكة الخاصة التي تكون متصلة بالإنترنت و يتم ذلك من خلال عمل تصفية للبيانات المتجهة من الإنترنت الى الشبكة الخاصة والتحقق منها فإذا كانت تحقق القواعد المطبقة على الجدار الناري يسمح لها بالدخول وغير ذلك يتم إسقاطها قبل دخولها إلى الشبكة الخاصة.

والشركات الكبرى !! كل ذلك بسبب عدم الأخذ ببديهييات الامن أو لضعف الإجراءات الأمنية المتخذة ونتج عن ذلك خسائر تقدر بمئات الملايين ولكن الأمور الآن أصبحت أكثر صرامة وصعوبة أمام المخترقين والمتطفلين خاصة بعد سن القوانين التي تجرم من يقوم بتلك الأفعال وتطور مستوى البحث والتحري لتتبع أثر المجرمين على الشبكة ، كما لا ننسى أنها أيضا نتيجة مباشرة لزيادة الوعي لدى الشركات والبنوك بأهمية الامن ولذلك فإن هؤلاء المتطفلين والمجرمين بدؤوا بالبحث عن مستخدمي عاديين لأنهم اهداف أبسط ولا يأخذ منهم وقت طويل للوصول إلى أجهزتهم ومعلوماتهم.

من مصادر التهديد الأمني لمستخدمي شبكة الإنترنت نجد :

♦ الفيروسات و احصنة طروادة وديدان الإنترنت.

♦ الاختراق (سواء كان اختراق لشبكة حاسب أو جهاز شخصي) وتعرف ب الهاكينج

Hacking.

♦ جواسيس البريد الإلكتروني .

الفيروسات : هي برامج صغيرة تصيب الأجهزة وتسبب في الكثير من المشاكل كمسح الذاكرة الصلبة أو مسح بعض الملفات الهامة في أنظمة التشغيل أو القيام بإصدار الأوامر لبعض البرامج دون علمك أو تدخل مباشر منك. أما أحصنة طروادة وديدان الإنترنت فهي شبيهة جدا بالفيروسات ولكنها تختلف في الهدف. أحصنة طروادة فهي لا تدمر ولا تفسح المعلومات ولكنها تتجسس وتقوم بجمع المعلومات والبيانات ومن ثم إرسالها لمصدرها (مرسل برنامج حصان طروادة) وهو عادة ما يكون فرد أو موقع أو منظمة لجمع المعلومات.

الاختراق (Hacking): هو قيام شخص أو أكثر بمحاولة الوصول الى جهازك أو الشبكة الخاصة بشركتك عن طريق شبكة الإنترنت وذلك باستخدام برامج متخصصة (سكانرز) في فك الرموز والكلمات السرية وكسر الحواجز الأمنية واستكشاف مواطن الضعف في جهازك أو شبكة معلوماتك وعادة ما تكون المخارج (بوابات العبور للمعلومات) (المنافذ) الخاصة بالشبكة المحلية، وهذه أسهل الطرق للوصول إلى جميع ملفاتك وبرامجك. وبالنسبة للمخترقين أصبحت المهمة عسيرة بعض الشيء وذلك في اختراق المؤسسات والمواقع الكبيرة بعد تطور نظم الدفاع وبرامج الحماية، ولكن بالنسبة لأجهزة الأفراد مازالت الأبواب مفتوحة.

جواسيس البريد الإلكتروني : وهم عادة من المخترقين السابقين لجهازك أو ممن يشاركونك الجهاز فعليا سواءا في المنزل أو العمل أو مستخدم آخر للجهاز خاصة إذا كنت في مقهى للإنترنت ولم تخرج من برنامج البريد بشكل صحيح أو لم تقم بالخروج من برنامج المتصفح.

يتم تداول عدد لا حصر له من المعلومات المهنية والخاصة على الإنترنت يوميا لذا فإنه في بعض الأحيان يصبح من الضروري أن نضع قيودا على وصول بعض المستخدمين إلى أنواع معينة من صفحات الويب أو المواقع. من الممكن أن نضع هذه القيود موضع التطبيق على سبيل المثال لمنع المراهقين من الدخول إلى المواقع الإباحية، هنالك العديد من الطرق لعمل ذلك، بعض المصفحات نفسها تسمح لكل بوضع القيود وأيضا هنالك بعض البرامج الخاصة التي تسمح لك بذلك.

متصفح إنترنت إكسبلورر يسمح لك بوضع بعض القيود وذلك بالنقر على قائمة أدوات ومن ثم اختيار الأمر خيارات الإنترنت (Internet Options → TOOLS)، ومنه تختار صفحة امان.



هذه الشاشة تسمح لك بوضع القيود باستخدام أزرار المواقع الآمنة والمواقع المحظورة. من المشاكل المرتبطة باستعمال الحواسيب والإنترنت تتعلق باستعمال كلمات المرور استعمال كلمات المرور أصبح الآن شيئا شائعا بشكل كبير، فإنك تستخدم واحدة منها للدخول إلى حاسوبك وأخرى للدخول إلى الإنترنت للوصول إلى ملفات معينة أو حتى الدخول إلى موقع خاص لذا ولكي تتمكن من حماية خصوصيتك فإن أمن كلمات المرور هذه هو شيء أساسي. لا يوجد هنالك إستراتيجية كاملة ولكن هنالك احتياطات بسيطة يمكن أن تساعدنا، يجب أن نفعل ما يلي:

- استعمال أنواع مختلفة من كلمات المرور لأغراض وخدمات مختلفة.
- قم بتغيير كلمة المرور بشكل متكرر وبشكل يصعب اكتشافه ولكن بشكل يسهل تذكره (لا تقم باختيار تواريخ الميلاد أو ما شابهها من الأمور الواضحة كاسم طفلك ولكن اجعلها من الممكن لك أن تتذكره). استعمال حالات الأحرف الكبيرة والصغيرة تجعل من الصعب اكتشاف كلمة المرور.
- لا تقم بكتابة كلمة المرور في أي مكان، ولكن إذا اضطررت إلى ذلك فلا تترك الورقة أو نسخا منها في أي مكان حيث يمكن إيجادها بسهولة ومن ثم استخدامها بشكل خاطئ.

فقد أخذنا بعين الاعتبار كلمات المرور ولكنها ليست المشكلة الوحيدة التي يمكن أن نتعرض لها بخصوص الأمن على الإنترنت. في هذه الأيام مع توسع التجارة الإلكترونية فإن شراء الأشياء من الإنترنت أصبح شيئاً سهلاً وشائعاً هنالك العديد من خيارات الدفع عن طريق الإنترنت، ولكن اسرعها وأكثرها مرونة هو استعمال بطاقات الائتمان.

عند الشراء بواسطة بطاقة الائتمان يجب أن تكون حذراً وخاصة في ما يلي:

- تجنب الشراء من مواقع غير معروفة أو من مواقع أمنها تحوم حوله الشكوك.
- تجنب إعطاء تفاصيل بطاقات الائتمان في غرف المحادثات أو في رسائل البريد الإلكتروني.
- تأكد بأن المعلومات المتعلقة بتفاصيل بطاقات الائتمان تتم حمايتها وتشفيرها وذلك لتجنب الوصول إليها من القرصنة.
- جانب آخر يجب أن يحظى بالاعتبار له علاقة بحقوق الملكية لا يقتصر هذا على المواد المطبوعة فقط ولكنه ينطبق على الإنترنت. القوانين المتعلقة بحقوق الملكية (Copy Right) ما زالت غير واضحة بخصوص حماية النصوص على الإنترنت، ولكن هنالك بعض المبادئ الأساسية التي يجب احترامها.
- كل شيء على الإنترنت معمي بحقوق الملكية ما لم يذكر المؤلف غير ذلك على المواد التي قام بتأليفها.
- نسخ النصوص والصور أو عناصر صفحات الإنترنت الأخرى ليس فقط خاطئ وغير أمين ولكن يمكن أن يعتبر جريمة.
- يعزز ويدعم التعريف بحقوق الملكية، بما فيها اسم المؤلف وتاريخ التأليف حماية النصوص بشكل واضح. وحتى مع وجودها لكيلا يمكنك نسخ كل ما تريد، يمكنك الإشارة إلى حقوق الملكية بالعادة باستعمال العبارات التالية:

© 2000 – 2002 John Doe, all right reserve,. If you want to reproduce the contents of this site, in whole or in part, send an email to the following abc@xy.com.

لذلك إذا أردت أن تقوم بنسخ أو إعادة إنتاج شيء من أحد المواقع لا يمكنك الاكتفاء بذكر المصدر ولكن يجب أن تأخذ الإذن مسبقاً لاستعمال تلك المادة. (إنها فكرة جيدة أن تحتفظ بنسخة من طلبك للحصول على حقوق استعمال بعض المواد والردود عليها وذلك لتجنب الإزعاجات القانونية التي يمكن أن تحدث مستقبلاً).

إذا أردت أن تستخدم فقرات قليلة فقط يمكنك ذلك ما دمت قمت بذكر ذلك على موقعك وذكر المؤلف والمصدر وذلك فقط لأغراض غير ربحية، تذكر أنه من السهل جداً أن تنسخ الأشياء من الإنترنت ولكنه أيضاً من السهل تعقب النصوص. إذا اكتشفت أن بعض النصوص الخاصة بك قد تم

نسخها اطلب وبشكل فوري إزالة المواد المسروقة في معظم الحالات يمكن حل المشاكل بهذه الطريقة وتجنب الملاحقات القانونية المكلفة لأن معظم النسخ يتم عمله بنية حسنة.

وباهمية مشكلة خرق قوانين حقوق الملكية هي مشكلة الانتحال (Plagiarism). يعني هذا المصطلح أن يقوم شخص معين بنسب أعمال شخص آخر إليه وادعائه بأنها له. يعتبر هذا العمل غير أخلاقي وغير قانوني كذلك. تتضمن بعض التصرفات الغير قانونية الأخرى التذف والتشهير، الاستعمال الغير مسموح به للبيانات، والتهديدات الجسدية أيضاً.