الفصل العاشر :

متطلبات الحماية للأجهزة الشخصية

لما تزل الإحصاءات تظهر الخطر الكبير الذي يتهدد المستخدمين لشبكة الإنترنت، سواء على صعيد الأفراد أو المؤسسات، أو الجهات الحكومية وغيرها، ففي إحدى الإحصائيات التي أجرتها وكالة التحقيقات الفيدرالية الأمريكية (FBI) فإن ٥٧٪ من المشاركين في تلك الإحصائية أوضحوا تعرضهم لمحاولة اختراق في أثناء اتصالهم بالإنترنت. وفي إحصائية أخرى أجرتها الوكالة أيضاً بالتعاون مع معهد أمن الحاسبات (CSI) فإن ٩٠٪ من المشاركين في هذه الإحصائية أثبتوا تعرضهم للاختراق.

فيما كشفت أحدث التقارير الذي طرحتها شركة مكافي في مطلع عام ٢٠٠٩م، أن مجرمي الإنترنت غالبًا سيستغلون الأزمة المالية العالمية المتفاقمة بنظام وبراعة أكبر في عام ٢٠٠٩، مما يشكل تهديدًا على جميع المستخدمين. فقد شكلت سنة ٢٠٠٨م، فترة لم يسبق لها مثيل للتهديدات والمخاطر، وتوقعت الشركة المزيد من تلك البرامج في ٢٠٠٩م، أكثر بكثير من السنة الماضية. إذ شهد العام المنصرم المزيد من البرامج الضارة أكثر من أي وقت مضى. فخلال فترة ١٥ عاما الماضية حتى نهاية عام ٢٠٠٧م، تلقت مختبرات مكافي حوالي (٣٥٨٠٠٠) من البرمجيات الخبيثة، في حين أن أكثر من (١٣٥٠٠٠) من تلك البرمجيات الخبيثة المحددة كانت في العام ٢٠٠٧ وحده. وبحلول مارس ٢٠٠٨ زادت البرامج الضارة التي تم تحديدها عن كل ما ظهر عام ٢٠٠٧. وفي عام ٢٠٠٨ ، تلقت مختبرات مكافي تقريبا (١,٥) مليون من البرمجيات الخبيثة ، أي بمعدل (٣٥٠٠) كل يوم.

ومن المفيد معرفة بعض الإحصاءات حول أفكار مستخدمي الإنترنت وطبيعة تصرفهم حيال الأخطار المحتملة، ففي تقرير لمجلة أمن المعلومات ٢٠٠٧م، ذُكر أن حوالي ٦٠ ٪ من الناسِ الذي طُلِبَ منهم كلمة السر الخاصة بالدخول على شركاتهم بشكل مهذب! قاموا بإعطائها لمن طلبها منهم.

ولعل حادثة السيدة السعودية التي وقعت في الشهر العاشر من عام ٢٠١١م، تدلل على سهولة الحصول على كلمة السر بهم، إذ اتصل بها أحد الأشخاص مدعياً أنه موظف المصرف المودع حسابها لديه، وطالباً منها تحديث بياناتها، بعد أن تصل إليها رسالة جوال تظهر بعض المعلومات الخاصة بها، وبعد أن رأت تلك المعلومات وفي أعلى الرسالة النصية اسم المصرف، قامت بإعطاء كلمة السر للمتصل، وما هي إلا ساعات قليلة حتى سحب المحتال رصيدها البالغ (١٠٠) ألف ريال على دفعتين، وأودعه في حساب شركة وهمية في نفس المصرف.

ولهذا أيضاً تبين الأرقام عدم ثقة الكثيرين بالتعاملات المالية عبر الإنترنت، إذ يعتقد ٥٨٪ من المستخدمين أن التعاملات المالية على الإنترنت غير آمنة. ولعل اقتناع العديد من المستخدمين بأن بياناتهم الخاصة عرضة للبيع والشراء يجعلهم يترددون في استخدم الشبكة، وقد أظهرت دراسة نسبة فقدان سرية المعلومات للجمهور، حيث ظهر أن ٣٥٪ من المواقع التجارية تقوم بتقديم معلومات الزبائن الخاصة لشركات الإعلان لكي تقوم بعرض الإعلانات المناسبة لهم.

فيما بينت إحصائية أخرى أجريت على الأطفال المتصلين بالإنترنت أن عددهم سيصل إلى (٧٧) مليون طفل في الولايات المتحدة الأمريكية، وأن ١٨٪ منهم قرروا مقابلة أشخاص في الحياة الواقعية، بعد أن تعرفوا عليهم مبدئيا عن طريق الإنترنت.

ومن تلك البيانات والإحصائيات يمكن الحديث عن البرامج والاحتياطات اللازمة للمستخدم الفردي لحماية نفسه عند ارتباطه بالإنترنت. وهذه المتطلبات تتباين من حيث أهميتها وضرورة وجودها. فبعضها مهم جداً، ومن المفترض إن لم يكن من الضرورة استعمالها. أما بعضها الآخر، فهو من باب الاحتياط الزائد ويحبّذ استخدامها لمن لديه معلومات حساسة في جهازه، مما يجعل من الضروري توفير أقصى قدر من الحماية.

١٠-١ برامج الحماية من الفيروسات (Anti-Virus)

وتعدّ هذه البرامج من أهم برامج الحماية، فلا يستغني عنها أي شخص مهما كانت خبرته في مجال الحاسب ، وذلك لأنه لا يوجد طريقة لأي شخص لتمييز الملفات التي تحتوي على الفيروسات ما لم يكن لديه برنامج فاحص الفيروسات (هناك بعض الاستثناءات ولكن لن يجري ذكرها هنا).

وقد تطورت برامج الحماية من الفيروسات في الآونة الأخيرة لتقوم بالتعرف على أنواع الفيروسات المختلفة، سواء كانت:

- فيروسات مدمجة في ملفات تنفيذية.
- فيروسات من نوعية الماكرو (Macro) التي تدمج في برامج الأوفيس غالباً.
- برامج التروجان (حصان طروادة)، وإن كانت برامج التروجان لا تُصنّف كفيروسات، إلا إن برامج الحماية من الفيروسات تقوم باكتشافها أيضاً.

ونظرا لكثرة طرق انتشار الفيروسات في الآونة الأخيرة، فإن برامج الحماية من الفيروسات كان لابد أن تتطور بشكل كبير لكي تقوم بحماية المستخدم. ومن ذلك التطور أن برامج الحماية من الفيروسات تأتي بخيار يسمح لها بالعمل بشكل خفي في الخلفية، بحيث تقوم بفحص أي ملف يتم وضعه على القرص الصلب أو ذاكرة الفلاش مباشرة من دون الحاجة لتدخل المستخدم. وهذه الخاصية تحمي جهاز المستخدم من أن يصاب بالفيروس في حالة نسيان المستخدم أن يقوم بفحص الملف الذي سحبه من الإنترنت قبل تشغيله.

كما أن هذه البرامج تقوم بفحص الملفات الملحقة بالبريد الإلكتروني في أثناء سحب الرسالة، وبذلك يحمي المستخدم من الإصابة بالفيروسات التي تنتقل في البريد الإلكتروني التي في

الغالب تأتي، وكأنها مرسلة من أحد الأصدقاء مما يجعل المستخدم يثق بها ويقوم بفتحها.

ويمتد مستوى الحماية في هذه البرامج لتقوم بحماية المستخدم من الفيروسات التي تنتقل عبر برامج المراسلة اللحظية مثل: (Instant Messaging)، و(MSN Messenger)، و(Yahoo Messenger)، و(AOL Messenger).

ولعل أهم ميزة في برامج الحماية من الفيروسات هو قيامها بالتحديث الذاتي، بحيث تقوم بحماية جهاز المستخدم من أحدث الفيروسات ظهوراً. وغني عن الذكر بأن برنامج الحماية من الفيروسات إذا لم يتم تحديثه فإنها لن تكون ذات فعالية وموثوقية.

ومن أشهر برامج الحماية من الفيروسات ما تقدمه شركتي سيمانتك (www.symantec.com)، وشركة مكافي (www.mcafee.com) ، وشركة كاسبر سكاي...إلخ، ويمكن للمستخدم الحصول على نسخة تجريبية من هذين الموقعين وتجربتها ومن ثم شراؤها منهم. كما أن أغلب الأجهزة الحديثة تأتي مدعمة بهذه البرامج عند شراء الجهاز.

شكل ١٠-١: قسم التحكم في برنامج Norton AntiVirus ويظهر فيه خاصية مسح الملفات السريع في أثناء عمله.

١٠-٢ برامج جدر الحماية الشخصية

هذه النوعية من البرامج تقوم بتركيب نفسها كطبقة وسيطة بين الشبكة وبين نظام التشغيل، بحيث تكون على علم بأي اتصال شبكي يكون صادراً أو وارداً إلى جهاز المستخدم، وتقوم بإخبار المستخدم بماهية هذه الاتصالات والبرامج التي تقوم بها، لكي يقرر المستخدم بعد ذلك فيما كان يرغب بالسماح بذلك أم لا.

تقوم هذه البرامج بحماية المستخدم على ثلاثة أوجه:

حماية خصوصيته، حيث إنها تخبر المستخدم في حين محاولة أحد البرامج القيام بإرسال معلومات من جهاز المستخدم إلى الشبكة. ومن هنا يتمكن المستخدم من معرفة هذه البرامج ومنعها في حالة كونها برامج دعائية أو تجسسية. ولقد عانت شركة ريال (RealPlayer) من دعوى قضائية رفعت عليها لكونها تتبع اختيارات المستخدمين وتحاول معرفة المقاطع الصوتية التي يستمع لها المستخدمون بكثرة، وهذا فيه اختراق لخصوصية المستخدمين. ولقد تم اكتشاف المعلومات التي يرسلها برنامج ريال بلاير بواسطة أحد برامج جدر الحماية الشخصية.

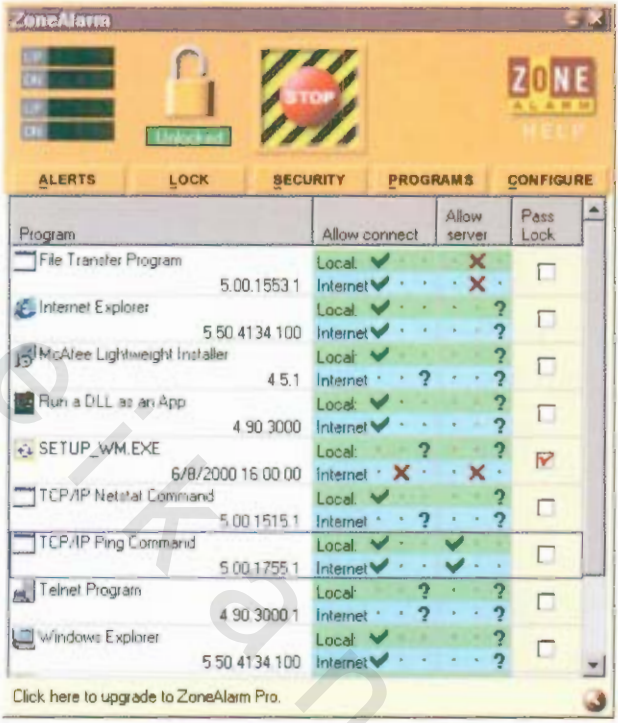
حماية ملفات المستخدم، حيث إن معظم المستخدمين يتجاهلون إلغاء خاصية مشاركة الملفات في أجهزتهم، أو قد يقومون بفتح مشاركة الملفات دون علم منهم، مما قد يفتح الباب على مصراعيه لمن أراد الحصول على هذه الملفات. وتقوم برامج جدر الحماية الشخصية بتحذير المستخدم وتعطيل خاصية مشاركة الملفات، لمن هم في خارج نطاق الشبكة المحلية الموثوقة.

حماية المستخدم من برامج التروجان، أو من الثغرات الموجودة في أنظمة التشغيل التي تعمل عن طريق الشبكة. حيث إنه لو لم يقم برنامج الحماية من الفيروسات باكتشاف ملف التروجان، فإن برنامج جدار الحماية سيقوم باكتشاف محاولة التروجان فتح منفذ على جهاز المستخدم وإخباره بذلك. ويجب عليه في تلك الحالة ألا يقوم بالسماح لها. وهناك أيضاً ثغرات

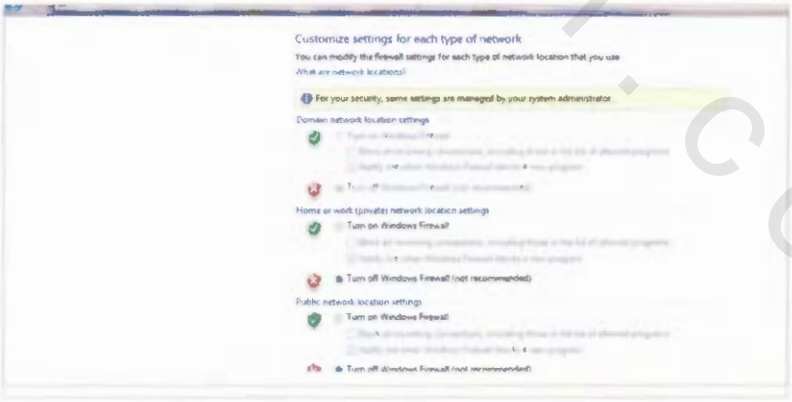
في أنظمة التشغيل لا يمكن تصنيفها على أنها فيروسات، ولكنها ثغرات تسمح لأي شخص باختراق جهاز المستخدم عن طريق تكوين اتصال على منفذ معين (Port) في جهاز المستخدم. وهذه النوعية من الثغرات لا يمكن لبرامج الحماية من الفيروسات اكتشافها على الإطلاق، ولكن برامج جدر الحماية الشخصية تكتشفها وتخبر المستخدم بذلك.

أشهر برامج الحماية من هذه النوعية هو برنامج زون الآرم (ZoneAlarm) الذي ظهر بقوة منذ بدايته ولازال يحتل صدارة البرامج من هذه النوعية. ويتميز هذا البرنامج بسهولة استخدامه وإعداده لضمان سلامة الجهاز. والجدير بالذكر أن هذا المنتج يتبع لشركة (CheckPoint) الإسرائيلية وأغلب أنظمة هذه الشركة تأتي على شكل منتج متكامل (Internet Security suite).

كما أنه من الجدير بالذكر أن أنظمة مايكروسوفت للتشغيل (ويندوز٧، وفيستا، xp) لديها خاصية جدار الحماية، وتسمى ICF) Internet Connection Firewall) من دون الحاجة لوجود برنامج إضافي، وإن كانت هذه الخاصية في نظام ويندوز أقل مرونة منها في برنامج زون الآرم، إلا أنها تفي بالغرض لمن لا يريد تركيب برامج إضافية.



شكل ١٠-٢: برنامج زون الآرم



شكل ١٠-٣: تمكين خاصية جدار الحماية في نظام ويندوز ٧

١٠-٣ برامج التشفير

تقوم برامج التشفير أو التعمية بتحويل النصوص المقروءة إلى نصوص غير مقروءة إلا لمن لديه المفتاح الخاص بفك التشفير، ولكثرة اختراق الأجهزة والحواسيب الشخصية في هذا الوقت، فإنه من المفيد تشفير بعض المجلدات على القرص الصلب، فيوضع عليه ما هو حساس من معلومات أو صور خاصة ضمن هذه المجلدات، وبذلك لا يستطيع المخترق من اختراق الجهاز وسرقة هذه الملفات.

كما أنه يمكن استخدام تقنية التشفير للحفاظ على سرية البريد الإلكتروني المتبادل، حيث إنه من المعروف أن البريد الإلكتروني عند انتقاله في الإنترنت معرض لأن تتم قراءته من قبل أشخاص آخرين غير المرسل والمستقبل. لذلك تم إيجاد تقنية (Public Key Cryptography) التي تمكن كل مستخدم من الحصول على وثيقة إلكترونية يكون الهدف منها تمييز الشخص بنفس الطريقة التي تميزه بها بطاقة الأحوال المدنية في الحياة الواقعية. وتحتوي هذه الوثيقة على مفتاح عام يسمح لكل من يريد إرسال رسالة لذلك الشخص أن يقوم بتشفيرها باستخدام ذلك المفتاح. وبعد تشفير الرسالة فإنه لن يتمكن أحد من قراءتها غير الشخص المستقبل، وذلك لأن فك تشفير الرسالة يتم بواسطة المفتاح الخاص (Private Key) الذي لا يمتلكه أي شخص آخر غير صاحب الوثيقة الإلكترونية.

بالنسبة لتشفير الملفات، فيوجد الكثير من البرامج التي تقوم بذلك، ويمكن الحصول عليها من مواقع الإنترنت المختلفة، كذلك أيضا فهذه الخاصية أيضا موجودة في نظام (ويندوز٧، وفيستا، و XP) الذي يمكن الشخص من تشفير ملفاته في القرص الصلب.

أما بالنسبة لتشفير البريد الإلكتروني، فمعظم برامج قراءة البريد تدعم ذلك، وكل ما يلزم الشخص هو الحصول على وثيقة إلكترونية خاصة به عن طريق أحد المواقع المشهورة، مثل: (ViriSign أو Thawte) أو غيرها من الشركات الأخرى.

شكل ١٠-٤: خاصية تشفير المجلدات في ويندوز ٧

١٠-٤ الحماية من الشبكات اللا سلكية (WiFi)

أعطى التقدم المستمر في تقنية الشبكات المستخدم العادي حدا عاليا من الرفاهية جعله يعتاد على وجود الإنترنت في كل زمان ومكان. فالشبكات اللاسلكية متوفرة في أغلب الأماكن الآن من جامعات وأماكن عمل ومقاهي ومطارات وغيرها. ولكن هذه الزيادة في الرفاهية لا تخلو من الشوائب التي تعكر صفوها. فاعتياد الناس على توفر الإنترنت أعطى فرصة كبيرة للمخترقين للتعدي على خصوصياتهم !

فمن أحد أشهر طرق الاختراق ما يسمى، برجل المنتصف (Man in the middle) والتي يقوم فيها المخترق باستلام البيانات منك، دون علمك، وتمريرها للطرف الآخر، دون علم أي منكما عن وجوده. وسبب خطورة هذه الطريقة هي صعوبة اكتشافها (وأحيانا استحالة اكتشافها !) بحيث يحصل المخترق على جميع البيانات التي أرسلتها أو استقبلتها مثل كلمات السر، والبريد الإلكتروني، و التعاملات الإلكترونية أو غيرها. وانتشرت هذه الطريقة للاختراق مؤخرا، حيث يقوم المخترق بتكوين شبكة لاسلكية وهمية، ويقوم بإعطائها أسماء وهمية ومغرية، مثل، إنترنت مجانية (FreeInternet). بحيث يغري المستخدم العادي بالاتصال بها واستخدامها للوصول للإنترنت. ويقوم المخترق في هذه الحالة بتمرير البيانات عن طريق الشبكة التي قام بإنشائها، مطبقا طريقة (رجل المنتصف) دون علم المستخدم! بالطبع فهناك أكثر من طريقة للقيام بذلك، حيث يمكن للمخترق أن يقوم بذلك عن طريق كرت الشبكة اللاسلكي في جهازه أو ما يسمى بـ (Ad hoc network) أو بإحضار جهاز نقطة اتصال لا سلكية وتكوينها بالشكل الذي يريد. ومن الممكن تجنب الطريقة الأولى بشكل بسيط وذلك بمنع جهازك من الاتصال بأي شبكة من نوع Ad hoc network. أما الطريقة الثانية فهي صعبة الاكتشاف، حيث يصعب تمييز شبكة المخترق من غيرها! لا سيما

بأن المخترقين يقومون باختيار أسماء تبدو مشابهة، أو مطابقة، للشبكات الأصلية المقدمة من قبل المقهى أو المطار. ولتجنب ذلك يجب على المستخدم أن يقوم بالاستفسار من صاحب المكان عن اسم الشبكة وإعداداتها، حتى يتمكن من الاتصال بالشبكة الصحيحة. أيضا فيجب على مقدمي هذه الخدمة من وضع إعدادات تشفير للشبكة من أجل حماية المستخدمين بعضهم من بعض وأيضا ليحتاج لها المستخدم ويقوم بالسؤال عنها، ومن ثم يتم تعويد المستخدم على عدم الاتصال بأي شبكة ما لم تكن الشبكة الصحيحة.

١٠-٥ الحماية من المواقع غير الأخلاقية

الهدف من الحماية من المواقع غير الأخلاقية هو حماية المستخدمين صغار السن، من المخاطر التي تحتويها الإنترنت لهم (سبق الحديث عن ذلك في الفصل الثاني) فهؤلاء يحتاجون نوعية خاصة من البرامج توفر لهم الحماية على المستوى الأخلاقي. حيث توجد الكثير من البرامج في الإنترنت التي تسمح لولي أمر الطفل بالتحكم في دخول الطفل للإنترنت، وتحديد نوعية المواقع التي يستطيع أو لا يستطيع الدخول عليها. وتسمى هذه النوعية من البرامج بالتحكم الأبوي، وكذلك تساعد هذه البرامج الأبوين على تحديد تطبيقات الإنترنت التي يسمح للطفل باستخدامها، مثل المحادثة أو سحب البريد أو سحب الملفات أو غيرها من التطبيقات الأخرى.

هذه البرامج منتشرة بشكل كبير في الإنترنت، ومن أمثلتها برنامج (Cyber Patrol) وبرنامج (Cyber Nanny) وغيرها. ولكن هذه البرامج في الغالب تكون متبعة لتقاليد البلد المنتجة لها، التي تختلف بشكل كبير عن تقاليد مجتمعاتنا الإسلامية والعربية، لذا فقد كانت هناك عدة محاولات لإيجاد حلول لهذا النوع من المشاكل، ولعل من أبرزها خدمة الشبكة الخضراء التي تؤمن حماية المحتوى وتتفادى الدخول للمواقع ذات المحتوى غير اللائق أو الداعي إلى تفشي الرذيلة أو التطرف والغلو. كما يتم تقديم خدمة الشبكة الخضراء حاليا عن طريق

خدمة (نقاء) التي تقدمها شركة الاتصالات السعودية مع اشتراكات الإنترنت ذات النطاق العريض (DSL).

١٠-٦ أخطاء شائعة

يوجد العديد من الأخطاء الشائعة التي يقع فيها الكثير من المستخدمين، إما لعدم علمهم أو لتساهلهم. وهذه الأخطاء، وإن تكن بسيطة فقد تتسبب في اختراق أجهزتهم وضياع بياناتهم المهمة.

ويتطرق هذا القسم لبعض هذه الأخطاء وبيان كيفية تلافيها.

١٠-٦-١ كلمة السر الواضحة أو القصيرة

عند تكوين حساب بريد إلكتروني أو عند إعداد الملف الشخصي في أحد المواقع على الإنترنت، فإن بعض الأشخاص يقومون باختيار كلمة سر بسيطة قد تكون اسم مدينة، أو اسم شخص أو أي كلمة أخرى توجد في القاموس. وبعضهم الآخر يقوم باختيار أقصر كلمة سر ممكنة، أو جعل كلمة السر هي نفس اسم المستخدم بزيادة رقم أو عدة أرقام.

بالطبع فهذا فيه ميزة وهي أن كلمة السر يمكن تذكرها بسهولة من قبل صاحبها، ولكن العيب يكمن في سهولة اختراقها لمن أراد ذلك.

إن برامج كسر كلمة السر تعمل في الغالب بطريقتين:

القاموس: وذلك يعني أن هذه البرامج تتضمن ملفاً يحتوي على عدد كبير من الكلمات، وهذا الملف يسمى القاموس، وقد تكون هذه الكلمات هي كلمات إنجليزية أو عربية معروفة، أو قد

تكون أسماء أشخاص أو مدن أو غيرها من الكلمات الشائعة. ويقوم البرنامج بتجربتها واحدة تلو الأخرى، حتى يتمكن من كسر كلمة السر. بالطبع فإن الحظ يلعب دوراً كبيراً في الوقت الذي يستغرقه البرنامج للوصول لكلمة السر.

تجربة جميع الاحتمالات، وهو ما يعرف بالتخمين الاستنزافي (Brute Force)، حيث يقوم البرنامج بتجربة جميع الكلمات من حرف واحد، ومن ثم من حرفين، ومن ثم من ثلاثة حروف، مرورا بجميع الحروف. بالطبع فإن هذه البرامج ستأخذ وقتا أطول للتنفيذ من القاموس. حيث إن القاموس يحتوي على كلمات لها معنى، أما هذه الطريقة فتقوم بتجربة كل شيء، سواء كانت الكلمة لها معنى أو لم يكن لها معنى على الإطلاق، وهذا ما يجعل هذه النوعية أشمل من نوعية القاموس، ولكنها في الجانب المقابل أبطأ بكثير.

لذا فإن اختيار المستخدم لكلمة سر بديهية، مثل اسم، أو كلمة إنجليزية معروفة سيزيد من احتمالية اكتشافها من قبل طريقة القاموس. أما كلمة السر القصيرة، فلن تحتاج لوقت طويل لاكتشافها.

الحل هنا هو اختيار كلمة سر طويلة وتتكون من حروف صغيرة وكبيرة، ويكون معها أرقام أو رموز خاصة. في الغالب فإن كلمة السر التي تحتوى على أكثر من ثمانية حروف، وليست من ضمن القاموس وبها رقم أو رمز، تكون آمنة.

١٠-٦-٢ عدم تغيير كلمة السر بشكل دوري

يعتقد بعض المستخدمين أن اختيار كلمة السر يتم مرّة واحدة فقط، وهذا اعتقاد خاطئ. فكلمة السر يجب تغييرها بشكل دوري. حيث إن بعض المخترقين يتمكنون بشكل أو بآخر من الحصول على كلمة السر الخاصة بالمستخدم، ومن ثم يقومون بقراءة بريده الإلكتروني دون أن يعلم. أي أنهم لا يقومون بإيذاء المستخدم أو مسح بريده، بل يقومون بالتجسس عليه بشكل خفي. وهذا أخطر أنواع الاختراق، وهو أن يكون الشخص أو الجهة مخترقاً من دون أن يعلم. فعند إبقاء كلمة السر دون تغيير، فإن ذلك يعني استمرار المخترق في الحصول على معلومات المستخدم. أما عندما يقوم المستخدم بتغيير كلمة السر بشكل دوري، فإن ذلك يعني أن المخترق سيضطر لمحاولة الحصول عليها مرة أخرى، وقد لا ينجح في ذلك.

السبب الآخر لضرورة تغيير كلمة السر هو أن برامج كسر الحماية من نوع (التخمين الاستنزافي) التي تقوم بتجربة جميع الاحتمالات ستصل إلى كلمة السر لا محالة. صحيحٌ أنها ستستغرق وقتاً طويلاً، ولكنها في النهاية ستصل لكلمة السر. هذا بافتراض أن المستخدم لا يقوم بتغيير كلمة السر الخاصة به. ولكن في حالة تغيير المستخدم لكلمة السر بشكل دوري، فإن ذلك يلغي فاعلية برامج تخمين كلمة السر.

١٠-٦-٣ استخدام كلمة سر واحدة لجميع المواقع

بعض المستخدمين يقومون باستخدام كلمة سر واحدة لجميع المواقع التي يزورونها، وهذا خطر جداً. وكما قيل «لا تضع بيضك كله في سلة واحدة». فالذي يحصل على كلمة السر الخاصة بالمستخدم لموقع واحد يستطيع التحكم في حساب المستخدم في جميع المواقع التي اشترك بها.

كما أن بعض أصحاب المواقع يقومون بتكوين مواقع وهمية وإلزام المستخدمين بالاشتراك فيها. وبعد أن يقوم المستخدم بالاشتراك في الموقع، يقوم صاحب الموقع بمحاولة الدخول على بريد المستخدم واستخدام كلمة السر التي أدخلها المستخدم في موقعه. وهذه الطريقة غالباً ما تنجح.

لذا يجب على المستخدم أن يقوم باختيار كلمة سر مختلفة للمواقع المختلفة، وخصوصا في المنتديات التي تدار من قبل أفراد قد لا يثق المستخدم بهم. وذلك لضمان أكبر قدر من الحماية لمعلوماته. كما أنه أيضا يمكن للمستخدم أن يقوم باختيار كلمة السر بشكل ذكي، بحيث يكون هناك جزء ثابت لا يتغير وجزء يتغير، وله علاقة باسم الموقع بحيث يكون لديه كلمة سر مختلفة بين المواقع المختلفة، وفي نفس الوقت لا يحتاج لأن يحفظ الكثير من كلمات السر، بل يكتفي بحفظ الجزء الثابت ومن ثم إدخال الجزء المتغير على حسب الموقع الذي دخل به.

١٠-٦-٤ عدم تغيير كلمة السر الافتراضية

تأتي بعض البرامج أو أنظمة التشغيل في بعض الأحيان مع كلمة سر افتراضية، يعرفها كل من قام بتركيب البرنامج. ويغفل الكثير من المستخدمين عن تغيير كلمة السر تلك، التي تعد أول كلمة يقوم المخترق بتجريبها في الغالب.

١٠-٦-٥ خلل في الاعدادات

يقوم بعض الأفراد بتركيب برامج الحماية المختلفة ولكنهم لا يعدونها بشكل صحيح، وهذا كما ذكرنا مسبقا يلغي فعالية تلك البرامج. فمن قام بتركيب برامج الحماية من الفيروسات، وقام بتعطيل خاصية الفحص التلقائي، فإن برنامج حماية الفيروسات لن يتمكن من فحص جميع

الملفات التي يتم سحبها من الإنترنت مباشرة. وهذا يعني احتمالية قيام المستخدم بتشغيل الملف ومن ثم إصابة جهازه بالفيروس.

وينطبق الشيء نفسه على برامج جدر الحماية الشخصية، فلو قام الشخص بتركيب جدار الحماية الشخصي وسمح للبرامج بأن تقوم بإرسال ما تريد من بيانات، وسمح لبرامج التروجان بفتح المنافذ المختلفة في جهازه، فلن تكون هناك أي فاعلية لتلك البرامج. بل انقلب دورها من الحارس إلى الخادم المطيع لبرامج التروجان.

ويشكل الخلل في الإعدادات مشكلة كبيرة، يجب الحذر منها عند استخدام أي برنامج يتطلب إعداداً من المستخدم. والحل لهذه المشكلة هو عدم قيام المستخدم بتحديد أيه إعدادات ما لم يكن واثقاً مما يفعله. وفي حالة عدم تأكده فيجب عليه سؤال من هو أعلم منه في تلك البرامج، وسيجد بالتأكيد من يمد يد العون له.

١٠-٦-٦ عدم تحديث البرامج وأنظمة التشغيل بشكل دوري

يتم اكتشاف الثغرات في أنظمة التشغيل وفي التطبيقات المختلفة بشكل يومي. وتقوم الشركات المنتجة للبرامج وأنظمة التشغيل بتزويد المستخدمين بتحديثات لتغطية تلك الثغرات وإصلاحها. ولكن، ما لم يقم المستخدم بسحب تلك التحديثات وتركيبها، فستبقى تلك الثغرات مفتوحة لكل من أراد اختراق الجهاز والعبث به. ونظراً لأهمية هذه المشكلة ولنسيان الكثير من المستخدمين تحديث أجهزتهم بشكل دوري، فإن معظم مصنعي البرامج يقومون بتوفير خاصية التحديث التلقائي لبرامجهم، بحيث لا يتحمل المستخدم عناء البحث عن التحديثات وتركيبها يدوياً، بل كل ما يلزمه هو توفير اتصال إنترنت للبرنامج الذي يقوم بزيارة موقع الشركة المصنعة للبرنامج وسحب آخر التحديثات. انظر الشكل ٨-٥

شكل ١٠-٥: إعدادات التحديث التلقائي في نظام ويندوز