بسمه تعالی

مرکز مدیریت راهبردی افتا

عنوان

آشنایی با راهکارهای تأمین حداقل امنیت کاربر

گروه زیر ساخت امن

تیرماه ۱۳۹۳

فهرست مطالب

۱- مقدمه

در دنیای امروزی حرکت سریع کشورها به سوی جامعه اطلاعاتی موجب رشد وسیع سیستم‌ها و سرویس‌های اطلاعاتی شده است. به این ترتیب از یک طرف گسترش شبکه‌های کامپیوتری و افزایش روزافزون ارتباطات، بسیاری از سازمان‌ها و مراکز تحقیقاتی بزرگ را برای حفظ محرمانگی اطلاعات، دسترسی‌پذیری اطلاعات و همچنین جامعیت آن‌ها با مشکلات فراوانی روبرو کرده است و از طرف دیگر پیچیده شدن بدافزارها و هدفمند شدن حملات مهاجمان باعث شده تا ضد بدافزارها، دیواره‌های آتش و پروتکل‌های امنیتی که پیش‌تر استفاده می‌شدند، پاسخگوی تامین امنیت اطلاعات کاربران نباشند.

شاید مهمترین چالشی که سازمان‌ها با آن مواجه هستند، عدم آگاهی کافی کارمندان آن‌ها با مفاهیم امنیت فناوری‌های مورد استفاده است که می‌تواند زیان‌های غیر قابل جبرانی به آن‌ها وارد کند. به این منظور در این مستند، راهکارهایی برای تامین حداقل امنیت اطلاعات کاربران بیان می‌شود تا بتوان از نقض امنیت سازمان و کاربران و خسارات ناشی از آن تا حد ممکن جلوگیری به عمل آورد. لازم به ذکر است که رعایت نکات مطرح شده در مستند جاری به معنای برقراری امنیت کامل کاربر نبوده، بلکه می‌تواند دامنه تهدیدات مربوط به کاربر را کاهش دهد.

ساختار این مستند به این صورت است که در بخش دوم حوزه‌های مختلفی را که می‌توان دستورالعمل‌های امن‌سازی را در آن اعمال کرد و دستورالعمل‌های کلی هر حوزه را تشریح می‌کند. در بخش سوم برای حوزه‌های بیان شده در بخش دوم چک‌لیست‌های متناسبی ارائه شده و در نهایت در بخش آخر روش پیاده‌سازی و اعمال برخی از بندهای بخش سوم به‌صورت موردی به تفصیل شرح داده شده است.

قبل از مطالعه و اجرای این سند، نکات زیر باید مورد توجه قرار گیرد:

- از آن‌جا که ممکن است تنظیمات امن‌سازی، کارکردهای سیستم را مختل یا غیرفعال کند، لازم است قبل از اجرای تنظیمات، یک نسخه پشتیبان از پیکربندی سیستم تهیه شود.
- برای اجرای الزامات تعیین شده در این سند، اولویت با خط‌مشی‌های سازمان است. به عبارت دیگر اگر برخی از الزامات بیان شده در این سند، با خط‌مشی‌های سازمان تداخل یا تضاد داشت، اولویت با خط‌مشی‌های سازمان است.

- در تهیه این سند، سعی شده است که حداکثر الزامات مرتبط با حوزه‌ی سند، پوشش داده شود. اما این بدان معنا نیست که پس از اجرای این الزامات، سیستم به صورت صد در صد امن خواهد بود. الزامات بیان شده در این سند، حداقل انتظارات برای امن‌سازی در حوزه‌ی تعریف شده در این مستند است.

۱-۱ تهدیدات

عدم رعایت دستورالعمل‌های امنیتی این سند، منجر به سرقت اطلاعات، فروش اطلاعات سازمانی به رقبا، از بین رفتن اطلاعات، دستیابی‌های غیرمجاز به اطلاعات و مواردی از این قبیل خواهد شد و در نتیجه می‌تواند راه نفوذ به سیستم را برای بدافزارها، نفوذگرها و خرابکاران اینترنتی باز کند. این موضوع اهمیت آگاه‌سازی و لزوم رعایت نکات امنیتی از سوی کاربران برای مقابله با تهدیدات ممکن را روشن می‌سازد. از جمله‌ی این تهدیدات می‌توان به موارد زیر اشاره کرد:

۱- بدافزار[۱]ها: به برنامه‌هایی گفته می‌شود که هدف آن بدخواهانه است. از جمله انواع بدافزارها، ویروس کامپیوتری[۲] (قطعه کدی که در برنامه‌ای قانونی جاسازی شده و بقیه برنامه‌ها را آلوده می‌کند)، کرم کامپیوتری[۳] (برنامه‌ای مستقل که با کپی کردن خود، از سیستمی به سیستم دیگر در شبکه منتشر می‌شود) و اسب‌های تروا[۴] (برنامه‌های مستقلی هستند که در کنار عملکرد مفید، فعالیت‌های مخربی را نیز انجام می‌دهند) می‌باشند. به عنوان مثال کرم W32/Leaves به مهاجم اجازه می‌داد تا کنترل شبکه‌ی کامپیوتر قربانی را در دست بگیرد و امکان دسترسی به اطلاعات و تغییر آن‌ها را فراهم کند. بدافزارهای تروا نیز می‌توانند پس از نصب بر روی سیستم، اجازه‌ی دسترسی و تغییر اطلاعات موجود بر روی سیستم را برای مهاجم فراهم کرده و با تغییر پیکربندی نرم‌افزارهایسیستم قربانی، شرایط را برای نفوذهای دیگر فراهم کنند. عدم رعایت نکات زیر موجب بروز این تهدیدات می‌شوند:

- استفاده از نسخه‌های قدیمی مرورگرها
- نصب نسخه‌های آسیب‌پذیر افزایه‌ها[۵] مانند Adobe Flash Player، Adobe Acrobat/Reader یا Java

---

[۱] Malware
[۲] Computer Virus
[۳] Computer Worm
[۴] Trojan Horse
[۵] Plugins

- سیستم‌عامل به‌روزرسانی نشده
- دیواره آتش غیر فعال
- استفاده از نرم‌افزارهای منقضی شده[۶]
- اجرای خودکار درایوهای قابل حمل، به محض اتصال به سیستم
- عدم استفاده از برنامه‌های ضد بدافزار و یا عدم بروزرسانی آن‌ها
- بازدید از وب‌سایت‌های آلوده
- و غیره...

۲- تهدیدات مبتنی بر مهندسی اجتماعی[۷]: مهندسی اجتماعی، هنر استفاده از رفتار کاربران به‌منظور نقض امنیت، حتی بدون اینکه قربانی بفهمد که نقشی در نقض امنیت داشته است. روش‌های مهندسی اجتماعی در دو دسته‌ی اصلی جای می‌گیرند: فریبکاری مبتنی بر کاربر[۸۹] و فریبکاری مبتنی بر کامپیوتر یا فناوری

روش‌های مبتنی بر کاربر، از طریق فریب کاربر و با بهره‌گیری از بی‌خبری (جهل) قربانی انجام می‌شود. به‌عنوان مثال مهاجمان از طریق تلفن با کاربر تماس برقرار کرده و با فریب او به اطلاعات شخصی‌اش دست پیدا می‌کنند.

- **روش‌های مبتنی بر فناوری**، کاربر را به‌گونه‌ای فریب می‌دهد که فکر می‌کند با یک سیستم کامپیوتری واقعی در حال تعامل است و باعث می‌شود تا اطلاعات محرمانه‌اش را فاش کند. به عنوان مثال کاربر پنجره‌ی بالارونده‌ای[۱۰] را مشاهده می‌کند که اعلام می‌دارد مشکلی در برنامه‌ی کاربردی رخ داده و لازم است تا کاربر مجددا تصدیق هویت شود، به این ترتیب کاربر کلمه‌ی کاربری و رمز عبورش را در پنجره‌ی بالارونده وارد می‌کند. به این ترتیب هکری که این پنجره را ایجاد کرده به کلمه کاربری و رمز عبور کاربر دسترسی پیدا می‌کند. از نمونه‌های دیگر حملات مهندسی اجتماعی می‌توان به درخواست از کاربر برای نصب برنامه‌ی فراهم شده به‌منظور مشاهده فیلم موجود در وب سایت یا کلیک بر روی تصویری که به ایمیل الحاق شده است نیز اشاره کرد.

---

[۶] Out-of-date
[۷] Social Engineering
[۸] Human based deception
[۹] Computer or technology based deception
[۱۰] popup

به عنوان مثالی دیگر، یکی از حملاتی که به‌شدت مورد توجه مهاجمان قرار دارد، Spear phishing است که آمارها نشان می‌دهد، حدود ۹۱٪ از حملات هدفمند از این طریق انجام می‌شوند. هدف این دسته از حملات فریب کاربر به‌منظور دانلود پیوست‌های ایمیل و یا کلیک بر روی لینک‌های درون ایمیل است؛ که اغلب دانلود پیوست‌های چنین ایمیل‌هایی منجر به نصب بدافزار بر روی سیستم قربانی و اتصال به یک سرور کنترل و فرمان[۱۱] مخرب شود. همچنین لینک‌های درون چنین ایمیل‌هایی مربوط به سایت‌های مخرب بدافزار است. بنابراین رعایت نکات امنیتی در برخورد با ایمیل‌ها می‌تواند از کاربر در برابر چنین حملاتی محافظت کند.

۳- تهدیدات مبتنی بر وب: یکی از تهدیدات امنیتی در اینترنت، حملات مبتنی بر وب می‌باشند. حملات مبتنی بر وب، شامل اسکریپت‌های مخربی هستند که سعی می‌کنند از طریق وب سایت‌های آلوده، به برنامه‌های اجرایی و سیستم‌عامل کاربران این وب سایت‌ها حمله کنند. پس از بدست گرفتن کنترل سیستم قربانی، مهاجمان قادر هستند از اطلاعات شخصی و قدرت پردازشی سیستم قربانیان سوءاستفاده کنند. این حملات به دسته‌های زیر تقسیم می‌شوند:

- **حملات مبتنی بر دانلود**[۱۲]: از جمله اصلی‌ترین حملات مبتنی بر وب، حملات مبتنی بر دانلود می‌باشد. این نوع از حمله خود به دو دسته دانلود با دخالت کاربر و دانلود بدون دخالت کاربر تقسیم می‌شود. در حملات مبتنی بر دانلود با دخالت کاربر، با استفاده از روش‌های مهندسی اجتماعی از کاربر خواسته می‌شود تا اقدام به دانلود فایلی نماید. به عنوان نمونه به دانلود یک نرم‌افزار برای مشاهده محتویات صفحه وب درخواستی می‌توان اشاره کرد. در حملات مبتنی بر دانلود بدون دخالت کاربر، حملات مبتنی بر دانلود از طریق یک صفحه وب با محتویات مخرب انجام می‌شود که بدون اجازه و آگاهی کاربر منجر به دانلود فایل بدخواه و اجرای آن در سیستم می‌شود.

- **Cross Site Scripting**: حملات Cross Site Scripting گونه‌ای از تهدیدات است که با قرار دادن کدی (مانند کدهای جاوا اسکریپت) در وب‌سایت‌های قربانی، سعی در به‌دست آوردن اطلاعات اعتباری کاربر، کلمه عبور و یا اطلاعات کوکی‌اش را دارد. در این نوع از حملات، زمانی که در مرورگر وب‌سایتی را وارد می‌کنید، علاوه بر آن وب‌سایت، اسکریپت مخربی که در آن جاسازی شده نیز برای شما بارگذاری خواهد شد، موارد زیر می‌تواند موجب بروز این تهدید شود:

---

[۱۱] Command and control

[۱۲] Drive-by-Download

- مرور وب‌سایت‌های نامعتبر، پیام‌های ایمیل یا پست‌های گروه‌های خبری نامعتبر
- استفاده از فرم‌ها بر روی سایت‌های نامعتبر

- **Active Content in Java/Java Script/Activex:** کد فعال[۱۳] و یا محتویات فعال[۱۴] ، کدی است که در صفحات وب قرار داده شده و به زبان Java، JavaScript و ActiveX نوشته می‌شود. وقتی که کاربر صفحه‌ی وبی را مشاهده می‌کند، کد جاسازی شده‌ی آن به طور خودکار دانلود شده و در کامپیوتر کاربر اجرا می‌شود. به این ترتیب نفوذگر می‌تواند عملیاتش را انجام دهد. موارد زیر ممکن است موجب بروز این تهدید شود:
  - فعال بودن ActiveX، Java، Scripting (مانند JavaScript، VBScript و غیره)
  - پیکربندی ضعیف مرورگر

۴- تهدیدات کلمه عبور[۱۵]: کلمات عبور، که برای ورود به سیستم، ورود به ایمیل شخصی و مواردی از این دست استفاده می‌شوند، همواره در معرض افشا شدن و مورد سوءاستفاده قرارگرفتن توسط مهاجمین هستند. در ادامه تهدیداتی که به‌منظور دستیابی به کلمات عبور استفاده می‌شوند، ذکر شده‌اند:

- Shoulder Surfing: یکی از راه‌های دزدی کلمه عبور، مشاهده‌ی پنهانی کلمه عبور در زمانی است که قربانی در حال وارد کردن کلمه‌ی عبورش است. در واقع این روش، همان تکنیک مشاهده مستقیم است، که با مشاهده‌ی بدون اجازه‌ی کلمه عبور و یا سایر اطلاعات حساس و یا استراق سمع صورت می‌گیرد. معمولا این روش در محیط‌های شلوغ انجام می‌شود.
- Brute force attack: حمله‌ای است که در برابر داده‌های رمز شده استفاده می‌شود و در واقع یک روش سعی و خطا برای به دست آوردن اطلاعاتی مانند کلمه‌ی عبور کاربران، شماره شناسایی افراد[۱۶] و غیره می‌باشد. در این حمله تمام حالات ممکن یک کلید، تا رسیدن به کلید صحیح بررسی می‌گردد. هکرها در این روش با حدس کلمه عبور و امتحان کردن تمام ترکیبات ممکن با کمک اطلاعات شخصی فرد، نام حیوان خانگی فرد، تاریخ تولد، شماره تلفن شخص، نام مدرسه و مواردی از این دست، سعی در به‌دست آوردن کلمه عبور شخص می‌کنند.

---

[۱۳] Active Code
[۱۴] Active Content
[۱۵] Password
[۱۶] PIN

- Dictionary attack: در این نوع تهدیدات، هکر با استفاده از کلماتی که در لیستی مشخص شده نظیر لغت‌نامه‌ها وجود دارند، سعی در بدست آوردن کلمه عبور شخص می‌کند. ابزارهایی برای این منظور وجود دارند که با امتحان کردن همه‌ی کلمات موجود در لیست، کلمه عبور را شناسایی می‌کنند.

مواردی که موجب بروز تهدیدات کلمه عبور می‌شوند، عبارتند از:

- وارد کردن کلمه عبور در حضور افراد دیگر
- قرار دادن کلمه عبور سیستم در اختیار افراد دیگر
- یادداشت کلمه عبور برروی کاغذ یا محلی در هارد سیستم
- استفاده از اطلاعات شخصی در کلمات عبور
- استفاده از کلمات رایج و مورد استفاده مانند حیوانات، گیاهان، پرندگان و غیره

۵- به اشتراک‌گذاشتن ناامن فایل‌ها: فعال‌سازی امکان اشتراک‌گذاشتن فایل و پرینتر ممکن است باعث بروز تهدیداتی شود. مهاجمین می‌توانند از این امکان سوءاستفاده کرده و ابزارهایی را بر روی تعداد زیادی از کامپیوترهای متصل به اینترنت قرار دهند؛ بطورکلی به اشتراک‌گذاشتن فایل‌ها، کامپیوتر را مستعد پذیرفتن حملات مختلفی می‌کند. بیشتر این حملات اجازه دسترسی کامل خواندن/نوشتن محتویات هارد دیسک را برای مهاجمین فراهم می‌کنند.

برای مثال در ویندوز می‌توان با استفاده از سرویس اشتراک فایل[۱۷] و سرویس اشتراک پرینتر[۱۸] در شبکه وارد سیستم شد و به سیستم قربانی نفوذ کرد. پروتکلی که دسترسی اشتراکی به فایل‌ها، پرینترها و پورت‌های سریال را فراهم می‌آورد، SMB (Server Message Block) نام دارد؛ این پروتکل در لایه‌ی شبکه و به یکی از روش‌های زیر اجرا می‌شود:

- بر روی پورت ۴۴۵ و از طریق TCP
- از طریق NetBios بر روی پورت‌های ۱۳۷ و ۱۳۸ UDP و بر روی پورت‌های ۱۳۷ و TCP۱۳۹

در سیستم عامل ویندوز دسته‌ای از حملات از پروتکل SMB استفاده می‌کنند؛ در این دسته از حملات مهاجمین با اسکن پورت‌های باز بر روی کلاینت، به سرویس SMB دسترسی یافته و در صورتیکه از

[۱۷] File Sharing
[۱۸] Print Sharing

پورتهای مربوط به SMB، پاسخی دریافت کنند، متوجه وجود این سرویس بر روی ماشین قربانی می‌شوند. مهاجمین با استفاده از آسیب‌پذیری‌های SMB، به کامپیوتر قربانی حمله می‌کنند. از جمله حملاتی که از این طریق انجام می‌شود شنود نشست[۱۹]های SMB بین کلاینت و سرور توسط مهاجم است. به علاوه مهاجم می‌تواند خود را به‌عنوان سرور جا بزند تا کلاینت به جای سرور اصلی با او ارتباط برقرار کند. به این‌ترتیب هکر می‌تواند اطلاعات کلاینت را دریافت کرده و یا اطلاعاتی را به آن ارسال کند. علاوه بر این، مهاجم از این طریق می‌تواند منجر به اجرای سرویس‌های مخربی بر روی ماشین قربانی شده و به آن دسترسی پیدا کند.

۶- دزدی اطلاعات موجود بر روی کامپیوتر: یکی از تهدیداتی که اطلاعات کاربران را هدف قرار می‌دهد، دزدی اطلاعات کاربران به‌صورت فیزیکی و با ورود مستقیم به سیستم آن‌ها می‌باشد. ممکن است اشخاصی با هدف دزدی اطلاعات از سیستم شما سوءاستفاده کنند. آسیب‌پذیری‌های زیر می‌توانند منجر به بروز این تهدید شوند:

- قفل نکردن سیستم در زمان بلااستفاده بودن آن
- عدم استفاده از کلمه عبور برای ورود به سیستم یا استفاده از کلمه عبور ضعیف

۱-۲ دامنه:

تمامی راهکارهای امن‌سازی ارائه شده در این سند، برای آگاهی کلیه کاربران سیستم‌عامل‌های مختلف در بخش‌های مختلف سازمان‌ها بیان شده است تا با رعایت نکات ذکر شده بتوان از نقض امنیت سازمان و خسارات ناشی از آن تا حد ممکن جلوگیری به عمل آورد. با اینکه ضمیمه‌های مطرح شده در بخش ۴ مربوط به کاربران ویندوزی می‌باشد، اما مشابه این امن‌سازی‌ها با کمی تغییر، قابل اعمال به سایر سیستم‌عامل‌ها نیز است.

۱-۳ اصطلاحات:

ضد بدافزار[۲۰]: برنامه‌ی امنیتی که بر روی کامپیوتر نصب می‌شود و با شناسایی، متوقف کردن و حذف بدافزارها از سیستم محافظت می‌کند.

---

[۱۹] session

[۲۰] Antivirus

دیواره آتش[۲۱]: سیستم طراحی شده به‌منظور جلوگیری از دسترسی‌های غیرمجاز به شبکه‌های خصوصی است، که می‌تواند به‌صورت سخت‌افزاری، نرم‌افزاری و یا ترکیبی از این‌دو پیاده‌سازی شود.

وصله امنیتی[۲۲]: تکه کدی است که برای رفع آسیب‌پذیری برخی برنامه‌ها بر روی سیستم نصب می‌شود.

پنجره‌های بالارونده[۲۳]: پنجره‌های تبلیغاتی هستند که حین کار با اینترنت بدون اجازه کاربر و به صورت ناگهانی نمایش داده می‌شوند.

هرزنامه[۲۴]: پیام‌های گروهی و ناخواسته که در پوشه‌ی spam در ایمیل‌ها قرار می‌گیرند.

افزایه: برنامه‌های کمکی که ویژگی‌ها و عملکردهای بیشتری را به برنامه‌های دیگر می‌افزایند.

امحا کردن[۲۵]: پاک‌سازی کامل فایل‌ها و فولدرها به طوری که امکان بازیابی آن‌ها نباشد.

۲- امن‌سازی

با توجه به مطالب بیان شده در مقدمه، کاربران سازمان‌ها که مهمترین دارایی‌های سازمان هستند، در معرض تهدیدات امنیتی متعددی قرار دارند. با انجام تدابیر لازم و استفاده از برخی روش‌های ساده می‌توان اقداماتی را در خصوص ایمن‌سازی سیستم‌های مربوط به این کاربران، انجام داد. به این منظور در این بخش به ارائه‌ی راهکارهایی در راستای امن‌سازی منابع اطلاعاتی می‌پردازیم، که لازم است توسط کاربران رعایت گردد. این راهکارها در حوزه‌های مختلفی نظیر پیکربندی سیستم، پیکربندی مناسب ضد بدافزارها، نصب نرم‌افزارها، کلمه عبور مناسب، استفاده از مرورگر وب، راهکارهای امنیتی در استفاده از ایمیل‌ها، پشتیبان‌گیری و امحای فایل‌ها، برقراری امنیت فیزیکی سازمان، اشتراک‌گذاری فایل‌ها و فولدرها و استفاده صحیح از رسانه‌های قابل حمل است که در ادامه هر یک از آن‌ها تشریح خواهد شد.

۲-۱ پیکربندی سیستم

---

[۲۱] Firewall
[۲۲] Security patch
[۲۳] Pop-up Windows
[۲۴] Spam
[۲۵] Wipe

به‌منظور بالابردن امنیت سیستم لازم است به پیکربندی امن برنامه‌های کاربردی و سیستم‌عامل توجه شود. یکی از تنظیماتی که جهت افزایش امنیت، لازم است در سیستم اعمال شود، تغییر نام حساب-های پیش فرض مانند Administrator و حذف حساب‌های غیر ضروری می‌باشد، بعضی از حساب‌های کاربری مانند Administrator با نصب سیستم‌عامل، بر روی سیستم ایجاد می‌شوند که معمولا هم امکان حذف اینگونه حساب‌ها، از سیستم وجود ندارد؛ بنابراین مهاجمان با داشتن کلمه عبور آن‌ها می‌توانند در سطح مدیریتی به اطلاعات سیستم دسترسی پیدا کرده و یا منجر به تغییرات مخربی در سیستم شوند، با تغییر نام این دست از حساب‌ها و یا حساب‌های غیر ضروری دیگری که ممکن است بر روی سیستم وجود داشته باشند، می‌توان تا حد ممکن جلوی سوء استفاده از آن‌ها را گرفت.

همچنین نباید از سطح دسترسی مدیریتی[۲۶] برای عملیات عادی سیستم استفاده کرد، به عبارت بهتر حساب کاربری که برای عملیات عادی در سیستم استفاده می‌شود، نباید از نوع admin تعریف شود، زیرا درصورتی‌که مهاجم بتواند به این حساب دست‌یابد، می‌تواند با حق دسترسی مدیریتی عملیات مخربی را در سیستم انجام دهد. همچنین جهت افزایش ایمنی حساب‌های کاربری سیستم، کلمه عبوری که برای آن‌ها درنظر گرفته می‌شود باید به گونه‌ای باشد که حدس زدن و دست‌یافتن به آن مشکل باشد.

از موارد دیگری که لازم است در پیکربندی سیستم‌ها لحاظ شود نصب حداقل سرویس‌ها و پکیج‌های مورد نیاز، برروی سیستم است. اگر تعداد سرویس‌ها و برنامه‌های در حال اجرا بر روی سیستم زیاد باشد، خطر سوء استفاده از سیستم افزایش می‌یابد، بنابراین در زمان نصب سیستم‌عامل باید سعی شود که حداقل پکیج‌ها/اجزایی که برای اجرای سرویس‌ها یا برنامه‌های کاربردی[۲۷] مورد نیاز است، نصب شود؛ همچنین در صورتی‌که برنامه‌ی کاربردی یا سرویسی از سیستم حذف می‌شود، باید اجزای سیستم‌عامل که مربوط به آن سرویس یا برنامه می‌باشند نیز حذف[۲۸] شوند. علاوه بر موارد ذکر شده، سرویس‌های غیر ضروری که برروی سیستم در حال اجرا هستند نیز باید به این منظور حذف شوند.

علاوه بر موارد ذکر شده، هر پورت TCP/UDP باز می‌تواند راهی برای نفوذ مهاجمان به سیستم باشد، بنابراین باید جلوی پورت‌های باز نالازم گرفته شود و پورت‌های بلااستفاده TCP/UDP بسته شوند.

---

[۲۶] admin

[۲۷] Application

[۲۸] Uninstall

از تنظیمات دیگری که لازم است در سیستم اعمال گردد، غیرفعال کردن اجـرای خودکـار فایـل‌هـای اجرایی و باینری است، زیرا تعدادی از بدافزارها با استفاده از ویژگی اجـرای خودکـار خـود را بـر روی سیستم قربانی اجرا کرده و سیستم را مورد حمله قرار می‌دهند، با غیرفعال کردن این ویژگی می‌تـوان جلوی چنین بدافزارهایی را گرفت.

همچنین به‌روز رسانی سیستم‌عامل و برنامه‌های کاربردی دیگر، منجر به از بین رفتن آسیب‌پذیری‌های احتمالی موجود در آن‌ها که هکرها از آن برای حمله به سیستم استفاده می‌کنند، مـی‌شـود؛ بنـابراین لازم است تا سیستم‌عامل و برنامه‌های کاربردی به صورت دوره‌ای به‌روز شوند.

از تنظیمات دیگری که لازم است در سیستم لحاظ شود، فعالسازی دیواره آتش است، دیواره آتـش بـا تشخیص ترافیک‌های مشکوک، به کاربر هشدار داده و می‌تواند جلـوی تعـدادی از حمـلات را بگیـرد؛ همچنین می‌توان آن را طوری تنظیم کرد که فقط اجازه دهد ipهای خاصی به سیستم وارد شوند و به این تریتب جلوی دستیابی به سیستم از طریق ipهای غیرمجاز گرفته می‌شود.

از موارد دیگر، استفاده از محافظ صفحه نمایش[۲۹] است که در صـورتی‌کـه کـاربر از سیسـتم اسـتفاده نکند، بعد از مدت زمان مشخصی فعال شده و در صورتیکه برای آن رمز عبور تنظیم شده باشد، با وارد کردن رمز آن، کاربر می‌تواند دوباره به سیستم خود دست یابد؛ استفاده از این ویژگی باعث می‌شود که افراد دیگر نتوانند در زمانی که کاربر پشت سیستم حضور نـدارد، بـه سیسـتم او راه یابنـد. عـلاوه بـر محافظ صفحه نمایش کاربر نیز باید در هنگام ترک کردن کامپیوتر، سیستم را با استفاده از کلیـدهای Alt+Ctrl+Del یا کلید ویندوز + L قفل کند تا مانع از دسترسی غیرمجاز به سیستم شود.

۲-۲ پیکربندی مناسب ضد بدافزارها

به‌منظور جلوگیری از نفوذ بدافزارها به سازمان لازم است تا بر روی رایانه‌های موجود در سازمان از ضد بدافزارهای مناسب استفاده شود، ضد بدافزارهای استفاده شده در سازمان، باید دارای یک سیستم مدیریت متمرکز باشند که از وضعیت و عملکرد ضدبدافزار اطلاع یابد و امکان راهبری متمرکز و یکپارچه‌سازی ضدبدافزار در سطح شبکه، جهت مقابله با هرگونه تهدید و واکنش به موقع در برابر آن‌ها را داشته باشد. سیستم مدیریت متمرکز ضدبدافزار باید دارای ویژگی‌های زیر می‌باشد:

[۲۹] Screen saver

- نصب و مدیریت (تنظیم، به روز رسانی، اجرا، حذف) نسخه سمت کاربر ضدبدافزار
- به روز رسانی نسخه سمت کاربر ضدبدافزار به دو صورت زمان بندی شده[۳۰] و آنی[۳۱]
- امکان به روز رسانی نسخه سمت کاربر ضدبدافزار بر روی مجموعه ای از دستگاه (Server/Client)های انتخاب شده
- دریافت بروزرسانی بدون ارتباط با اینترنت[۳۲] بصورت فایل(های) به روز رسانی و از طریق اینترنت[۳۳]
- امکان تنظیم نشانی به روز رسانی (از نشانی قابل تعریف بطور محلی[۳۴] یا بر روی اینترنت)
- قابلیت اعمال اصلاحیه‌های[۳۵] بر روی نسخه سمت کاربر ضدبدافزار
- امکان تعریف دستوراتی نظیر Update و Scan
- امکان تعریف تنظیمات[۳۶] نسخه سمت کاربر ضدبدافزار
- مستثنی کردن[۳۷] برخی دستگاه ها از اعمال قواعد فراگیر
- امکان تعیین نحوه ارتباط بین ابزار مدیریتی و دستگاه های تحت پوشش
- امکان نمایش خلاصه عملکرد نسخه های سمت کاربر ضدبدافزار و وضعیت شبکه تحت پوشش[۳۸]
- دریافت وقایع[۳۹] از دستگاه های تحت پوشش برای تهیه گزارش
- قابلیت تهیه گزارش
- تهیه نسخه پشتیبان[۴۰] از قواعد و تنظیمات
- ارسال هشدار[۴۱]
- اطلاع رسانی درباره آخرین نسخه های سمت کاربر ضدبدافزار ، اصلاحیه های آنها و فایل های بروزرسانی

به‌علاوه لازم است تا ضد بدافزارها به‌طور دوره‌ای به‌روزرسانی شوند، تا با افزوده شدن امضاهای بدافزارهای جدید به پایگاه داده، توانایی شناسایی آن‌ها را پیدا کنند. به روز رسانی ضد بدافزار باید از طریق مجاری امن صورت گیرد و نباید از طریق اینترنت انجام شود.

---

[۳۰] Scheduled
[۳۱] On-Demand
[۳۲] Off-line
[۳۳] On-line
[۳۴] local
[۳۵] Patch
[۳۶] Settings
[۳۷] Exclude
[۳۸] Dashboard
[۳۹] log
[۴۰] Backup
[۴۱] Notification

همچنین بایستی کل سیستم بعد از به‌روزرسانی ضد بدافزارها پویش شود و به‌منظور جلوگیری از انتشار بدافزارها لازم است تا درایوهای دیسک سخت، وسایل جانبی متصل شده به سیستم و همچنین فایل‌های موجود در سیستم توسط ضدبدافزار پویش شوند؛ بخصوص فایل‌هایی که می‌توانند خاصیت بدخواهانه داشته باشند نظیر فایل‌های exe.، bat.، pif.، vbs.، و غیره باید پیش از باز کردنشان توسط ضد بدافزار پویش شوند.

به‌طور کلی یک ضدبدافزار خوب، باید ویژگی‌های زیر را داشته باشد:

- بررسی در هنگام دسترسی[۴۲]
- قابلیت استفاده از روش‌های رفتاری و هیوریستیک
- تنظیم روش مقابله با بدافزارهای شناخته شده
- سیستم مدیریت متمرکز ضدبدافزار

در ادامه ویژگی‌های بیان شده برای یک ضدبدافزار خوب به تفصیل شرح داده شده‌اند.

ضدبدافزار مورد استفاده باید قابلیت "بررسی در هنگام دسترسی" در بخش‌های زیر را داشته باشد:

- حافظه
- داده‌های روی دیسک‌ها
- ابزارهای ذخیره سازی قابل نقل و انتقال
- درایوهای شبکه

به عنوان مثال، بررسی همه پیوست‌های ایمیل‌های دریافتی و ارسالی نمونه‌ای از بررسی در هنگام دسترسی می‌باشد که ضد بدافزارها بایستی به نحوی پیکربندی شوند که هر فایل دانلود شده، باز شده و یا اجرا شده را به‌صورت بلادرنگ پویش کنند.

از قابلیت‌های دیگری که لازم است ضد بدافزارهای مورد استفاده در سازمان داشته باشند تنظیم روش مقابله با بدافزارهای شناخته شده شامل حذف بدافزار، بازسازی اثرات تخریبی بدافزارها، قرنطینه‌سازی فایل‌ها که به معنای نگهداری فایل حاوی بدافزار در مکانی مجزا و ایزوله برای اعمال پاکسازی و یا آزمون‌های بیش‌تر در آینده است، می‌باشد.

---

[۴۲] On-Access Scan

همچنین ضدبدافزار باید دارای قابلیت استفاده از روش‌های رفتاری و هیوریستیک برای شناسایی بدافزارهای جدید و هم‌خانواده باشد. منظور از روش‌های رفتاری امکان اجرای برنامه‌های مشکوک در محیط‌های کنترل شده و ثبت عملیات آن‌ها برای تعیین اینکه آیا برنامه مشکوک واقعا بدافزار است یا خیر و انجام اقدامات بعدی متناسب با نوع آن برنامه‌ی مشکوک، می‌باشد. از روش‌های هیوریستیک هم بیشتر برای شناسایی بدافزارهای هم‌خانواده استفاده می‌شود. یک بدافزار جدید در ابتدا منحصر به فرد است و با تهیه‌ی یک امضا برای آن، ضدبدافزار قادر به شناسایی آن خواهد بود، ولی به‌تدریج به دلایل مختلف (نظیر پخش شدن برنامه بدافزار، تکثیر ناقص بدافزار، بهینه‌سازی بدافزار اولیه و ...) ممکن است گونه‌های جدیدی از بدافزار اولیه، ایجاد شوند. در این‌گونه موارد، از یک امضای عمومی‌تر که بر اساس مشخصه‌های اصلی و مشترک بین گونه‌های مختف بدافزار تهیه شده، برای شناسایی گونه‌های مختلف آن، استفاده می‌شود.

۲-۳ نصب نرم‌افزارها

باید فهرست نرم‌افزارهای مجاز و مورد تائید سازمان و نسخه‌ی مناسب آن‌ها در اختیار کاربران قرارگیرد و کاربران از نصب نرم‌افزارهای دیگر خودداری نمایند تا آلوده‌سازی از طریق نرم‌افزارهای آسیب‌پذیر و مخرب به حداقل برسد. علاوه بر آن برخی از نرم‌افزارها و برنامه‌های کاربردی نظیر برخی از ضد بدافزارها، در هنگام نصب و یا بعد از آن، از کاربر می‌خواهند تا برای بهبود کیفیت کالا در آینده و مسائلی مشابه آن، اجازه انتقال اطلاعات و بازخورد از سوی سیستم را فراهم کند؛ که این امکان، نباید توسط کاربر فراهم شود، زیرا ممکن است مهاجمین از این طریق بتوانند سیستم کاربر را مورد حمله قرار دهند.

همچنین احتمال وجود برنامه‌های مخرب در نرم‌افزارهایی که به صورت رایگان از اینترنت قابل دانلود هستند، زیاد است. بنابراین در صورت نیاز به نصب چنین برنامه‌هایی حتماً لازم است مجوز مناسب از مدیر شبکه اخذ گردد.

۲-۴ کلمه عبور مناسب

هر سیستم می‌بایستی دارای کلمات عبور مناسب باشد. استحکام کلمات عبور، ساده‌ترین و در عین حال متداول‌ترین روش، به منظور اطمینان از این موضوع است که صرفاً افراد تائید شده و مجاز قادر به استفاده از کامپیوتر و یا بخش‌های خاصی از شبکه هستند. اکثر کاربران در زمان انتخاب کلمه عبور، از

اعداد و یا کلماتی استفاده می‌کنند که بخاطر آوردن آنان ساده باشد (نظیر تاریخ تولد، شماره تلفن و مواردی از این دست). برخی دیگر از کاربران علاقه‌ای به تغییر منظم کلمات عبور خود در مقاطع زمانی خاصی نداشته و همین امر می‌تواند زمینه تشخیص کلمات عبور توسط مهاجمان را فراهم نماید. در زمان تعریف کلمه عبور می‌بایست تمهیدات لازم در خصوص استحکام و نگهداری مطلوب آنان اندیشیده شود. به‌عنوان مثال پیشنهاد می‌شود از کلمات عبور دارای حروف بزرگ و کوچک، اعداد و علایم با طول بلند استفاده شود. علاوه بر آن لازم است تا برای هر حساب کاربری یک رمز عبور در نظر گرفته شود، به عنوان مثال رمز عبوری که برای ورود به سیستم استفاده می‌شود باید با رمز عبور حساب ایمیل کاربر متفاوت باشد، چون در غیر اینصورت مهاجم با تشخیص رمز عبور یکی از حساب-های کاربری می‌تواند به حساب‌های دیگر کاربر دست یابد.

از موارد دیگری که لازم است به آن توجه شود، استفاده از رمزهای عبور برای حساب‌های کاربری اینترنتی است (مانند ایمیل و ..) بعضی از مرورگرها در زمان وارد کردن رمز عبور در آن‌ها از کاربر سوالی مبنی بر ذخیره کلمه‌ی عبور کاربر در مرورگر می‌پرسند (گزینه‌هایی نظیر remember، remember me و مانند آن) در صورتی‌که کاربر آن را تایید کند در ورودهای بعدی لزومی به وارد کردن رمز عبورش ندارد. این امر موجب می‌شود تا اگر سیستم کاربر مورد سوءاستفاده توسط افراد غیرمجاز قرار گیرد، این افراد بدون نیاز به دانستن کلمه‌عبور کاربر بتوانند به اطلاعات حساب‌های کاربری اینترنتی شخص، دسترسی یابند.

همچنین رمز عبور نباید در اختیار افراد دیگر قرار گیرد یا در مکان‌های شلوغ و در حضور افراد دیگر نباید رمز عبور را وارد کرد زیرا امکان دستیابی مهاجمان به کلمات عبور، در این موارد زیاد است.

۲-۵ استفاده از مرورگر وب به صورت امن

بیشترین درصد حملات و صدمات نرم‌افزاری و امنیتی که ممکن است متوجه یک سیستم شود، از جانب اینترنت خواهد بود و در کنار آن بیشترین نرم‌افزارهایی که در یک سیستم با اینترنت در ارتباط هستند، مرورگرها می‌باشند. بنابراین هکرها و افرادی که قصد کلاهبرداری‌های اینترنتی و یا آسیب رساندن به کامپیوترها را دارند، بیشتر بر روی مرورگرها تمرکز می‌کنند. پس استفاده از مرورگری مناسب و امن در کنار دقت و توجه به جزئیات، از عوامل امنیت مرورگر، سیستم‌عامل و مهمتر از همه اطلاعات شما و سازمان به حساب می‌آید. از طریق هک کردن فایل اصلی اجرایی مرورگر، افزونه‌های

مرورگر، شنود تبادلات شبکه‌ای مرورگر و مواردی دیگر می‌توان مرورگرها را مورد حمله قرار داد. به این‌منظور لازم است از مرورگرهای مناسب و به‌روز استفاده شود، مثلا نسخه‌های قدیمی مرورگر IE آسیب‌پذیر هستند. بنابراین همواره توصیه می‌شود تا از مرورگرهای Chrome یا firefox و یا نسخه-های جدید IE استفاده شود.

از موارد دیگری که تهدیدی برای مرورگرها محسوب می‌شوند، نوار ابزارهایی هستند که بر روی مرورگر نصب می‌شوند(دسته‌ای از این نوارابزارها با نصب برنامه‌های رایگان از اینترنت به‌صورت خودکار بر روی مرورگر نصب می‌شوند).اگرچه نوارابزارها ویروس نیستند، اما می‌توانند ویژگی‌های بدخواهانه‌ی بسیار زیادی را از خود نشان دهند، بنابراین لازم است تا از نصب نوارابزارها بر روی مرورگر خودداری شود. افزایه‌ها نیز می‌توانند به‌عنوان تهدید دیگری برای مرورگرها مطرح شوند؛ اگرچه افزایه‌ها جز مرورگر نیستند، اما می‌توانند دامنه حملات به مرورگر را افزایش دهند، Adobe (acrobat) reader، Adobe flash player، Java applet و ... نمونه‌هایی از افزایه‌های مرورگر هستند که ممکن است توسط مهاجمین هک شوند. به‌علاوه ممکن است تروجان‌ها به‌عنوان یک افزایه بر روی مرورگر اجرا شوند. بنابراین حتی‌المقدور باید از نصب افزایه‌ها بر روی مرورگر جلوگیری شود.

دسته‌ای از حملات فیشینگ با استفاده از پنجره‌های بالارونده صورت می‌گیردکه در آن‌ها مهاجم سعی می‌کند تا اطلاعاتی مانند شماره‌های اعتباری و کلمات عبور یا سایر اطلاعات شخصی کاربران را با متقاعد کردن آن‌ها به دادن این اطلاعات تحت ادعاهای دروغین بدست آورد، به این صورت که پنجره-ی بالارونده‌ای که حاوی پیغام ترغیب کننده‌ای برای وارد کردن اطلاعات در آن است به کاربر نمایش داده می‌شود و کاربر با وارد کردن کلمات عبور و یا سایر اطلاعاتش، آن‌ها را در اختیار مهاجم قرار می-دهد. تعدادی دیگر از این پنجره‌ها کاربر را ترغیب به کلیک بر روی آن‌ها می‌کنند و با انتقال کاربر به صفحاتی مشابه با صفحات بانکی و یا سایت‌های دیگر به دزدی اطلاعات قربانی می‌پردازند؛ بنابراین لازم است تا از وارد کردن اطلاعات و یا کلیک کردن بر روی پنجره‌های بالا رونده خودداری شود.

از موارد دیگری که در وارد کردن اطلاعات بانکی و کلمات عبور باید به آن توجه شود استفاده از صفحه کلید مجازی برای وارد کردن اطلاعات در سایت بانک‌ها می‌باشد که با استفاده از آن، امکان دزدیده شدن کلمات عبور تا حد زیادی کاهش می‌یابد. به‌علاوه به‌منظور وارد کردن اطلاعات حساس مانند اطلاعات کارت‌های اعتباری لازم است حتما به آدرس وب‌سایتی که قصد وارد کردن اطلاعات در آن را

دارید، دقت نمایید. گاهی اوقات مهاجمان با تغییرات کوچکی در آدرس URL منجر به فریب کاربران شده و آن‌ها را وادار می‌کنند تا اطلاعات حسابشان را در فرم‌هایی که مشابه به فرم‌های بانکی است وارد کنند و به اطلاعات آن‌ها دست یابند.

علاوه بر موارد ذکر شده، لازم است بر روی پیغام‌های خطا و یا پنجره‌های بالارونده و یا عبارات "Agree"، "OK" و "I accept" بر روی بنرهای تبلیغاتی یا پنجره‌های بالارونده و یا سایت‌های مشکوک کلیک نشود، چون ممکن است حاوی بدافزارهایی باشند که با کلیک بر روی آن‌ها این بدافزارها بر روی سیستم اجرا شوند.

همچنین برای اینکه ردی از فعالیت‌های انجام شده در اینترنت باقی نماند و مورد سوء استفاده قرار نگیرد، می‌توان از ویژگی private tab که در IE11 قرار داده شده است، استفاده کرد. به وسیله‌ی این ویژگی می‌توان صفحات وب را بدون اینکه ردی از فعالیت‌های بر روی وب‌سایت‌ها قرار بگیرد ملاقات کرد. این ویژگی کمک خواهد کرد تا تاریخچه‌ی مرور، فایل‌های موقت اینترنت، داده‌های نوشته شده در فرم‌ها، کوکی‌ها، نام کاربری و کلمات عبور باقی نمانند. همچنین با استفاده از ویژگی SmartSceern Filter که در IE وجود دارد می‌توان تا حدی وب‌سایت‌های فیشینگ را شناسایی کرد و از دانلود و نصب بدافزارها جلوگیری به‌عمل آورد، بنابراین استفاده از این ویژگی توصیه می‌شود.

۲-۶ راهکارهای امنیتی در استفاده از ایمیل‌ها

ایمیل‌ها یکی از قدیمی‌ترین و پرکاربردترین سرویس‌های موجود در اینترنت هستند که فقدان معیارهای امنیتی مناسب در آن‌ها منجر به دستیابی‌های غیر مجاز به منابع، انتقال بدافزارها و دزدی اطلاعات می‌گردد. بنابراین لازم است در استفاده از ایمیل‌ها نکات امنیتی رعایت شود، برای این منظور بایستی ایمیل‌های ارسالی توسط منابع ناشناس همواره حذف شوند، زیرا ممکن است این ایمیل‌ها حاوی بدافزارهایی باشند. همچنین لازم است به پیوست یک ایمیل توجه شده و حتی‌الامکان از دانلود آن‌ها جلوگیری به عمل آید و در صورت لزوم حتما قبل از دانلود بر روی آن‌ها پویش انجام گردد؛ زیرا برخی از فایل‌ها مسئولیت توزیع بدافزارها را برعهده داشته و می‌توانند باعث بروز اشکالات فراوانی شوند. هرگز نمی‌بایست، قبل از حصول اطمینان از ایمن بودن ایمیل‌ها، اقدام به ارسال[۴۳] ایمیل برای سایر کاربران نمود. همچنین ممکن است ایمیل‌ها حاوی موضوعات جذابی مانند موقعیت‌های شغلی،

[۴۳] Forward

استفاده از اینترنت برای درآمد[۴۴]، رژیم غذایی، کاهش وزن و سلامتی، وام تضمینی، درآمد آسان، با یک کلیک پولدار شوید[۴۵]، تخفیف محصولات مختلف به‌ویژه محصولات نرم‌افزاری و موضوعات فکاهی و طنز باشند که لازم است چنین ایمیل‌هایی نادیده گرفته شده و حذف شوند؛ زیرا اکثر این ایمیل‌ها سعی در فریب کاربر را دارند تا کاربران با کلیک بر روی لینک موجود در این ایمیل‌ها هدف حمله فیشینگ قرار بگیرند.

همچنین ایمیل‌ها ممکن است حاوی پیوست‌های مشکوکی باشند که طبق گزارش FireEye معمولاً در نام پیوست‌های ایمیل‌های مشکوک کلماتی مانند "ups"،"details" ، "document"، "fedex" و "myups" مشاهده می‌شود. علاوه بر آن مهاجمین معمولا از فایل‌هایی با پسوند zip. استفاده می‌کنند. چون این فایل‌ها معمولاً توسط ضد بدافزارها مسدود نمی‌شوند. همچنین مهاجمان از انواع دیگری از فایل‌ها مانند PDFها، zip/RARها، مستندات آفیس و RTF بجای exe در پیوست‌های ایمیلشان استفاده می‌کنند، که در برخورد با چنین پیوست‌هایی لازم است تا از دانلود آن‌ها جلوگیری به عمل آید.

به‌علاوه برای تبادل اطلاعات سازمان، نباید از ایمیل‌های شخصی استفاده شود و باید از ایمیل سازمانی استفاده گردد تا امکان هک کردن آن و دستیابی به اطلاعات آن کاهش یابد، به‌علاوه نباید در سازمان از نرم‌افزارها و ابزارهای ارتباطی نظیر Yahoo messenger، Google Talk، Skype، Oovoo و مانند آن استفاده شود، چون انتقال اطلاعات سازمان از طریق این ابزارها ناامن بوده و ممکن است منجر به فاش شدن اطلاعات سازمان گردد.

۲-۷ پشتیبان‌گیری و امحای فایل‌ها

به منظور حفظ اطلاعات ارزشمند، لازم است در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر نسخه پشتیبانی تهیه شده و بر روی رسانه‌های ذخیره‌سازی نظیر لوح‌های فشرده و یا مکان‌های امن دیگر ذخیره شود؛ تا در صورتی که یکی از این نسخه‌ها از بین رفت، این اطلاعات درمکان‌های دیگری قرار داشته باشند و از دست رفتن یک نسخه از اطلاعات، منجر

[۴۴] Use the internet to make money

[۴۵] Get Rich Click

به از بین رفتن اطلاعات سازمان نشود. همچنین برای پشتیبان‌گیری اسناد با ارزش لازم است تا از سیاست‌های سازمان پیروی شود. موارد زیر نمونه‌ای از این سیاست‌ها می‌باشد:

- داشتن نسخه پشتیبان[۴۶] از هر سند و اطلاعات مهم، به‌طور منظم
- نگهداری آرشیوی از نسخه‌های قدیمی اسناد و اطلاعات مهم با مشخص‌سازی تاریخ و شماره نسخه سند و فایل
- نگهداری حداقل سه نسخه و کپی از فایل‌ها و اسناد الکترونیکی مهم، یک نسخه اصلی و دو نسخه پشتیبان
- نگهداری فایل‌ها در دو حافظه مختلف (در صورت امکان) و یا در دو درایو مختلف دیسک سخت (به‌عنوان مثال درایو :C و :D).
- نگهداری یک نسخه در سیستم دیگر به‌طور مثال نزد مدیر و مسئول مربوطه.

همچنین در صورتی‌که نیاز به حذف اسناد طبقه بندی شده در سازمان باشد، لازم است تا اسناد و فایل‌های مهم امحا[۴۷] شده و صرفاً به پاک کردن[۴۸] آن‌ها اکتفا نشود؛ زیرا با پاک کردن فایل‌ها و اسناد امکان بازیابی آن‌ها وجود دارد اما درصورتی‌که علاوه بر پاک کردن اسناد و فایل‌های مهم، اقدام به امحای آن‌ها نمود، دیگر امکان دستیابی به آن‌ها توسط افراد بدخواه وجود ندارد.

۲-۸ برقراری امنیت فیزیکی کاربران

علاوه بر اسناد الکترونیکی، اطلاعات ارزشمند سازمان ممکن است بر روی نسخه‌های فیزیکی قرار داشته باشند به این ترتیب لزوم حفظ اسناد فیزیکی و جلوگیری از افشای آن‌ها اهمیت می‌یابد. به همین منظور لازم است اطلاعات، اسناد محرمانه و غیر محرمانه، اسناد آموزشی و وسایل شخصی که می‌توانند معرف علایق، هویت، نوع کار و وظیفه مورد انجام، تخصص و اطلاعاتی از این دست باشند، بر روی میز کار و در معرض توجه و دید قرار نگیرند که اصطلاحا به رعایت این موارد، استفاده از " میز تمیز[۴۹] " گفته می‌شود. برای نگهداری اسناد فیزیکی بهتر است، از کمدها و کشوهای قفل‌دار استفاده

---

[46] Backup
[۴۷] Wipe
[۴۸] Delete
[۴۹] Clean Desk

شود. همچنین نباید به افراد خارج از سازمان اجازه داده شود تا از کامپیوترهای شخصی سازمان استفاده کنند زیرا ممکن است از این طریق به اطلاعات سازمان دست یابند.

همچنین ملاقات با افراد خارجی در صورت امکان باید در اتاق کنفرانس انجام شود و از ملاقات آن‌ها در اتاق کار جلوگیری به عمل آید، زیرا معمولا در اتاق کار، اطلاعات یا اسنادی از سازمان وجود دارد که ملاقات افراد خارجی در اتاق کار، راه دستیابی آن‌ها به این اطلاعات را ساده می‌کند.

۲-۹ اشتراک فایل‌ها و فولدرها

سیستم‌عامل نصب شده بر روی یک کامپیوتر، ممکن است امکان به اشتراک گذاشتن برخی منابع موجود نظیر فایل‌ها را با سایر کاربران شبکه، فراهم نماید. ویژگی فوق، می‌تواند زمینه بروز تهدیدات امنیتی خاصی را فراهم نماید. به عنوان مثال دسته‌ای از ویروس‌ها به‌طور اختصاصی برای شبکه‌های کامپیوتری طراحی شده‌اند بیشترین انتقال این دسته از ویروس‌ها با استفاده از فایل‌ها و فولدرهای به اشتراک گذاشته شده در شبکه‌های LAN می‌باشد. بنابراین می‌بایست در صورت عدم نیاز ضروری نسبت به غیرفعال نمودن ویژگی اشتراک‌گذاری فایل‌ها و فولدرها اقدام کرد. همینطور لازم است بلافاصله بعد از استفاده از یک منبع اشتراکی، ارتباط با آن قطع شود زیرا برقراری ارتباط با منابع اشتراکی زمینه آلوده‌سازی سیستم را فراهم می‌کند.

۲-۱۰ استفاده صحیح از رسانه‌های قابل حمل

به‌منظور جلوگیری از انتشار بدافزارها از طریق رسانه‌های قابل حمل، لازم است سیاست‌هایی به‌منظور استفاده و بکارگیری این رسانه‌ها در سازمان تعیین گردد تا کاربران با رعایت آن‌ها، آسیب‌های ناشی از استفاده از این رسانه‌ها را به حداقل برسانند. به این منظور لازم است کاربران از رسانه‌های قابل حمل سازمان کنند و از استفاده از رسانه‌های قابل حمل شخصی و یا ناشناس خودداری کنند، زیرا ممکن است این رسانه‌ها حاوی بدافزارهایی باشند که در صورت استفاده از آن‌ها، کامپیوترهای سازمان آلوده شوند.

همچنین برای استفاده از رسانه‌های قابل حمل، می‌بایست از رسانه‌هایی با قابلیت write-protect و یا رسانه‌های قابل حمل فقط خواندنی مانند CD و DVD استفاده کرد، زیرا امکان نوشتن بر روی چنین

رسانه‌هایی وجود ندارد و درصورتی‌که از این‌گونه رسانه‌ها در کامپیوتری که آلوده است استفاده شود، بدافزار موجود بر روی کامپیوتر آلوده، نمی‌تواند خود را بر روی این رسانه‌ها منتقل کند.

در مورد انتقال اطلاعات حساس سازمان نیز، باید توجه داشت که حتی‌الامکان از ذخیره‌سازی اطلاعات حساس سازمان در رسانه‌های قابل حمل جلوگیری شود و در صورت نیاز به ذخیره این اطلاعات در این رسانه‌ها، حداقل اندازه این اطلاعات ذخیره شود و پس از انتقال آن‌ها از روی رسانه‌های قابل حمل، باید در اسرع وقت امحا شوند (به‌عبارت بهتر، فایل‌ها به‌گونه‌ای از روی رسانه‌های قابل حمل حذف شوند، که امکان بازیابی آن‌ها نباشد) که در صورت گم شدن و یا دزدیده شدن این رسانه‌ها، از دستیابی به اطلاعات پاک شده‌ی درون آن‌ها (که معمولا اطلاعات سازمان هستند) جلوگیری به‌عمل آید.

علاوه بر مواردی که پیش‌تر به آن‌ها اشاره شده، باید به امنیت فیزیکی رسانه‌های قابل حمل نیز توجه شود. به این منظور لازم است رسانه‌های قابل حمل در مکان‌های امنی نظیر کمدها یا کشوهای قفل‌دار نگهداری شوند؛ همچنین چون این رسانه‌ها حاوی اطلاعات سازمان هستند، در صورت نیاز به انتقال اطلاعات به خارج از سازمان با استفاده از این رسانه‌ها لازم است، لازم است کاربران طی روالی ماهیت و نوع داده‌های انتقالی را مشخص سازند. همچنین به منظور جلوگیری از گم شدن این رسانه‌ها و نشت اطلاعات آن‌ها، می‌بایست از اطلاعات موجود در آن‌ها نسخه پشتیبان تهیه شود.

ممکن است رسانه‌های قابل حمل، خود، آلوده به بدافزار باشند که استفاده نادرست از آن‌ها در سازمان می‌تواند منجر به انتشار بدافزار از این طریق گردد؛ به این منظور لازم است خاصیت اجرای خودکار این رسانه‌های قابل حمل در سیستم‌عامل غیرفعال گردد، تا با بدافزارهایی که با استفاده از این ویژگی منتشر می‌شوند، مقابله شود. همچنین به‌منظور مقاوم‌سازی سیستم در برابر بدافزارهایی که از طریق رسانه‌های قابل حمل انتشار می‌یابند، لازم است وصله‌های مورد نیاز، به منظور جلوگیری از

سوءاستفاده از آسیب‌پذیری‌های مربوطه، بر روی سیستم نصب گردد. برای مثال با نصب وصله‌ی مربوط به آسیب‌پذیری LNK. و PIF (MS10-046) می‌توان جلوی بدافزارهایی (مانند Flame) که از این آسیب‌پذیری‌ها برای حمله به سیستم استفاده می‌کنند را گرفت.

همچنین لازم است دسترسی اجرای برنامه‌ها از طریق رسانه‌های قابل حمل نیز گرفته شود تا از اجرای بدافزارها از داخل این رسانه‌ها جلوگیری شود.

همچنین کاربران باید قبل از استفاده و اقدام به باز نمودن رسانه‌های قابل حمل، با استفاده از آنتی-ویروس‌ها، پویشی بر روی چنین حافظه‌هایی انجام دهند؛ تا اگر بدافزاری بر روی آن‌ها وجود دارد، شناسایی شده و با حذف آن از روی رسانه قابل حمل، از انتشار آن، بر روی کامپیوترهای سازمان جلوگیری شود. همچنین به‌منظور مشاهده‌ی محتویات رسانه‌های قابل حمل از ویژگی Explore استفاده شود، زیرا بازکردن حافظه‌های قابل حمل از این طریق مانع از اجرای بدافزارهایی می‌شود که به طور خودکار به‌وسیله‌ی بازکردن این رسانه‌ها به‌صورت autorun اجرا می‌شوند.

به علاوه کاربران نباید فایل‌های مشکوک و یا فایل‌هایی که از محتویات آن اطلاعی ندارند را باز نکنند زیرا ممکن است این فایل‌ها مربوط به بدافزار باشند. خارج کردن رسانه‌های قابل حملی که از طریق USB به سیستم متصل می‌شوند، نیز باید به صورت امن[۵۰] انجام گیرد زیرا جدا کردن این رسانه‌ها به یک‌باره از سیستم، ممکن است موجب از دست رفتن اطلاعات آن‌ها شود.

[۵۰] safe

۳- چک لیست

بند	توصیه امنیتی	وضعیت
۱	**پیکربندی امن سیستم‌عامل مورد استفاده**	□بلی □خیر
۱-۱	تغییر نام حساب‌های پیش فرض مانند Administrator و حذف حساب‌های غیر ضروری	□بلی □خیر
۱-۲	عدم استفاده از سطح دسترسی مدیریتی برای انجام عملیات متداول و روزمره (به بخش ۴ رجوع شود)	□بلی □خیر
۱-۳	ایجاد و استفاده از کلمه عبور مناسب برای ورود به سیستم (در بخش کلمه عبور توضیحات بیشتری داده شده است)	□بلی □خیر
۱-۴	نصب فقط بسته‌ها و اجزای ضروری مورد نیاز سرویس‌ها و برنامه‌های کاربردی، در زمان نصب سیستم‌عامل (در زمان نصب سیستم‌عامل جدید، لازم نیست همه‌ی اجزای آن نصب شوند).	□بلی □خیر
۱-۵	حذف و غیر فعال‌سازی سرویس‌های ناخواسته و غیر ضروری بر اساس سیاست-های سازمان، خصوصاً سرویس‌های شبکه که می‌توانند بردارهایی برای انتشار بدافزارها باشند. (به بخش ۴ رجوع شود)	□بلی □خیر
۱-۶	حذف نرم‌افزارها و برنامه‌های بلااستفاده با تائید مدیر سیستم	□بلی □خیر
۱-۷	حصول اطمینان از غیر فعال بودن امکان اجرای خودکار فایل‌های اجرایی باینری و اسکریپتی نظیر AutoRunها (حصول اطمینان از طریق تأیید و کسب اطلاع از مسئول شبکه)	□بلی □خیر
۱-۸	به‌روزرسانی سیستم‌عامل و برنامه‌های کاربردی به‌طور منظم و دوره‌ای بر اساس سیاست‌های سازمان (به بخش ۴ رجوع شود)	□بلی □خیر
۱-۹	قفل کردن سیستم با کلیدهای Alt+Ctrl+Del یا کلید ویندوز + L در زمان بلااستفاده بودن رایانه.	□بلی □خیر
۱-۱۰	استفاده از محافظ صفحه نمایش همراه با رمز عبور(به بخش ۴ رجوع شود)	□بلی □خیر
۱-۱۱	غیر فعال‌سازی و uninstall کردن اجزای سیستم‌عامل مرتبط با سرویس‌ها و یا برنامه‌های حذف شده از سیستم	□بلی □خیر

۱-۱۲	فعال بودن و استفاده از دیواره آتش (به بخش ۴ رجوع شود)	□بلی □خیر
۱-۱۳	بستن پورت‌های TCP/UDP بدون استفاده بر اساس سیاست‌های سازمان (به بخش ۴ رجوع شود)	□بلی □خیر
۱-۱۴	پذیرفتن اتصال به سیستم فقط از طریق ipهای مجاز، در صورتیکه ورود به سیستم از راه دور انجام گیرد (به بخش ۴ رجوع شود).	□بلی □خیر
۲	**استفاده و پیکربندی مناسب ضد بدافزار**	□بلی □خیر
۲-۱	نصب و استفاده از ضد بدافزار مورد تأیید سازمان	□بلی □خیر
۲-۲	استفاده از ضد بدافزار دارای ابزار مدیریتی متمرکز	□بلی □خیر
۲-۳	ثبت وقایع[۱] و ارسال آن به ابزار مدیریت متمرکز	□بلی □خیر
۲-۴	بروزرسانی پایگاه داده امضا و موتور[۲] ضد بدافزار به‌طور دوره‌ای بر اساس سیاست سازمان؛ به‌طور مثال روزانه	□بلی □خیر
۲-۵	عدم بروزرسانی ضد بدافزار از مجرای اینترنت و انجام بروزرسانی صرفاً از طریق سرورهای داخلی سازمان	□بلی □خیر
۲-۶	پویش کل سیستم بعد از نصب یا به‌روزرسانی ضد بدافزار	□بلی □خیر
۲-۷	پویش فایل‌ها برای شناسایی بدافزارهای شناخته شده، بخصوص فایل‌هایی که می‌توانند خاصیت بدخواهانه داشته باشند نظیر فایل‌های exe.، bat.، pif.، vbs.، و غیره پیش از باز کردن آن‌ها	□بلی □خیر
۲-۸	پویش اجزای مهم و حیاتی یک سیستم نظیر فایل‌های startup و رکوردهای بوت به‌صورت منظم و تعریف شده	□بلی □خیر
۲-۹	بررسی در هنگام دسترسی[۳] به اجزای یک سیستم به منظور شناسایی رفتار مشکوک؛	□بلی □خیر
۲-۱۰	استفاده از روش‌های رفتاری و هیوریستیک برای شناسایی بدافزارهای جدید و هم خانواده	□بلی □خیر

[۱] log

[۲] Engine

[۳] On-Access Scan

۲-۱۱	پاکسازی بدافزارهای شناسایی شده	□بلی □خیر
۲-۱۲	عدم غیرفعال کردن و یا حذف نرم‌افزار ضد بدافزار و یا تغییر تنظیمات کلیدی آن	□بلی □خیر
۳	**نصب نرم‌افزار**	□بلی □خیر
۳-۱	نصب و استفاده از نرم‌افزارهای مجاز و مورد نیاز با استفاده از نسخه مورد تأیید سازمان و عدم نصب و اجرای سایر نرم‌افزارهای خارج از فهرست مجاز سازمان و یا نرم‌افزارهای غیرضروری	□بلی □خیر
۳-۲	عدم موافقت با دادن بازخورد[۴] و اطلاعات به سازمان تولیدکننده نرم‌افزار در حین نصب و یا پس از آن	□بلی □خیر
۳-۳	جلوگیری از نصب نرم‌افزارهای رایگان قابل دانلود از اینترنت تا حد ممکن و استفاده از سایت‌های مورد تایید سازمان در صورت لزوم	□بلی □خیر
۴	**کلمه عبور مناسب**	□بلی □خیر
۴-۱	عدم استفاده از کلمات عبور ضعیف و قابل حدس نظیر کلمات بامعنا، عبارات رایج، اسم، تاریخ تولد، اعداد متوالی (مانند اعداد ۱ تا ۶)، کلمه Password، اطلاعات شخصی نظیر شماره تلفن، نام فرزند و یا همسر و مانند آن	□بلی □خیر
۴-۲	استفاده از کلمه عبور دارای حروف بزرگ و کوچک، اعداد و علایم با طول بلند (به عنوان مثال، معمولا پیشنهاد می‌شود که حداقل از ۱۴ کارکتر برای رمز عبور استفاده گردد) که مشخصات بند ۴-۱را نداشته باشد.	□بلی □خیر
۴-۳	استفاده از کلمات عبور مختلف برای حساب‌های مختلف و برای دسترسی‌های متفاوت؛ به‌طور مثال کلمه عبور سیستم و ایمیل بایستی متفاوت باشند.	□بلی □خیر
۴-۴	عدم استفاده از گزینه‌هایی نظیر remember، remember me و مانند آن برای به خاطر سپاری کلمه عبور توسط مرورگر و مانند آن. چنانچه یک صفحه وب و مانند آن گزینه‌ای مبنی بر به خاطر سپاری کلمه عبور ارائه نمود، جواب منفی را انتخاب نمایید.	□بلی □خیر
۴-۵	عدم استفاده از کلمات عبور شخصی در محیط‌های عمومی به‌عنوان مثال وارد	□بلی □خیر

[۴] Feedback

	کردن کلمات عبور در سیستم‌های عمومی و در معرض عموم	
۶-۴	عدم افشای کلمه عبور برای دیگران	□بلی □خیر
۷-۴	تغییر دوره‌ای کلمات عبور؛ به‌طور مثال به‌طور ماهانه کلمه عبور تغییر نماید و تکراری نباشد.	□بلی □خیر
۵	**استفاده از مرورگر وب به صورت امن**	□بلی □خیر
۱-۵	عدم استفاده از مرورگرهای آسیب‌پذیر و به‌ویژه نسخه‌های قدیمی IE[۵] (نسخه‌های قبل از نسخه ۱۰) یا استفاده از مرورگرهای Google Chrome و Mozilla Firefox	□بلی □خیر
۲-۵	بروزرسانی مرورگر و دریافت وصله‌های جدید	□بلی □خیر
۳-۵	عدم نصب نوار ابزار[۶] و ابزار جست و جو نظیر Ask برروی مرورگر	□بلی □خیر
۴-۵	عدم نصب افزایه بدون تأیید مسئول شبکه	□بلی □خیر
۵-۵	عدم وارد کردن کلمه‌ی عبور و PIN و یا هر کد دسترسی دیگر در پنجره‌های بالارونده مشکوک مرورگر	□بلی □خیر
۶-۵	استفاده از On-Screen Keyboard برای وارد کردن نام کاربری و کلمات عبور در سایت‌هایی نظیر بانک‌ها و سایت‌های معتبری که نیاز به کلمات عبور و نام کاربری دارند (به بخش ۴ رجوع شود).	□بلی □خیر
۷-۵	غیرفعال‌سازی popup windows، ActiveX، Active Scripting و Java در مرورگر و استفاده از پیکربندی امن مرورگر در صورت عدم نیاز ضروری. برای امن‌سازی مرورگرها و پیکربندی امن به مسئول شبکه مراجعه نمایید (راهنمایی ارائه شده در بخش ۴ می‌تواند در امن‌سازی مرورگر مؤثر باشد).	□بلی □خیر
۸-۵	توجه به آدرس سایت‌ها قبل از وارد کردن اطلاعات مهم و حساس در فرم‌ها و صفحات وب، به عنوان مثال توجه داشته باشید که آدرس فرم مربوطه صحیح باشد، حتما با https شروع شود و کنار آن علامت قفل قرار داشته باشد (به بخش ۴ رجوع شود).	□بلی □خیر

[5] Internet Explorer
[6] Toolbar

۹-۵	عدم کلیک بر روی پیغام‌های خطا، پنجره‌های بالارونده و یا عبارات "Agree"، "OK" و "I accept" بر روی بنرهای تبلیغاتی یا پنجره‌های بالارونده و یا سایت-های مشکوک، به‌منظور بستن پیغام‌های خطا و پنجره‌های بالارونده از CTRL+F4 و برای بستن وب‌سایت‌های مشکوک از ALT+F4 استفاده نمائید (به بخش ۴ رجوع شود).	□بلی □خیر
۱۰-۵	وارد کردن فقط اطلاعات ضروری در فرم‌های ثبت‌نام[۷] که با علامت "*" مشخص می‌شوند و عدم وارد کردن اطلاعات اضافی در این فرم‌ها	□بلی □خیر
۱۱-۵	عدم ارسال اطلاعات سازمان به صورت برخط و از طریق اینترنت	□بلی □خیر
۱۲-۵	استفاده از ویژگی private tab در اینترنت اکسپلورر برای مرور در سایت‌ها (به بخش ۴ رجوع شود).	□بلی □خیر
۱۳-۵	استفاده از ویژگی SmartScreen Filter برای شناسایی سایت‌های مخرب (به بخش ۴ رجوع شود).	□بلی □خیر
۶	**استفاده از ایمیل**	□بلی □خیر
۱-۶	استفاده از ایمیل سازمانی جهت فعالیت‌های سازمان و عدم استفاده از آن برای امور شخصی	□بلی □خیر
۲-۶	عدم توجه به ایمیل‌هایی که فرستنده آن‌ها ناآشنا است و حذف آن‌ها	□بلی □خیر
۳-۶	عدم پاسخ به ایمیل‌هایی که در آن‌ها اطلاعات شخصی و یا مالی پرسیده شده است.	□بلی □خیر
۴-۶	عدم ایجاد ارتباط با شماره‌ای که در ایمیل به آن اشاره شده است	□بلی □خیر
۵-۶	عدم توجه به هرزنامه‌ها و پاک کردن آن‌ها	□بلی □خیر
۶-۶	عدم بازکردن پیوست‌های مشکوک ایمیل‌ها و آگاهی از میزان مجاز و مطمئن بودن آن‌ها در صورت دریافت از فرستنده‌های آشنا با روشی غیر از پاسخ به نامه (نظیر تلفن) یا باز کردن آن‌ها در صورتی‌که انتظار دریافت ایمیل مشخص به‌همراه پیوست خاصی را دارید	□بلی □خیر

[۷] Registration

۶-۷	پویش پیوست‌های[8] ایمیل‌ها پیش از بازکردنشان	□بلی □خیر
۶-۸	عدم کلیک بر روی لینک‌های ناآشنا فرستاده شده از طرف فرستنده‌های آشنا و ناآشنا	□بلی □خیر
۶-۹	عدم وارد کردن کلمه‌ی عبور و PIN و یا هر کد دسترسی دیگر در پاسخ به ایمیل‌ها	□بلی □خیر
۶-۱۰	عدم استفاده از نرم‌افزارها و ابزار ارتباطی نظیر Yahoo messenger، Google Talk، Skype، Oovoo و مانند آن در سازمان	□بلی □خیر
۷	**پشتیبان‌گیری و امحای فایل‌ها**	□بلی □خیر
۷-۱	داشتن نسخه پشتیبان[9] از هر سند و اطلاعات مهم، به‌طور منظم و بر اساس سیاست‌های پشتیبان‌گیری سازمان	□بلی □خیر
۷-۲	نگهداری آرشیوی از نسخه‌های قدیمی اسناد و اطلاعات مهم با مشخص‌سازی تاریخ و شماره نسخه سند و فایل	□بلی □خیر
۷-۳	امحای اسناد و فایل‌های مهم و نه صرفاً پاک کردن آن‌ها و پیروی از سیاست‌های خاص سازمان برای امحای فایل	□بلی □خیر
۸	**برقراری امنیت فیزیکی کاربران**	□بلی □خیر
۸-۱	استفاده از میز تمیز	□بلی □خیر
۸-۲	استفاده از کمدها و کشوهای قفل‌دار برای نگهداری رسانه‌ها و حافظه‌های قابل حمل، اسناد سازمان و حتی وسایل شخصی	□بلی □خیر
۸-۳	تنها نگذاشتن افراد خارج سازمان در دفترکار	□بلی □خیر
۸-۴	عدم اجازه به افراد خارجی در استفاده از کامپیوترهای سازمان	□بلی □خیر
۸-۵	عدم تایپ کلمه عبور در حضور افراد خارج سازمان	□بلی □خیر
۸-۶	عدم کپی فایل‌ها و اطلاعات سازمان بر روی موبایل‌ها و دستگاه‌های شخصی که مربوط به سازمان نیستند.	□بلی □خیر
۸-۷	ملاقات افراد خارجی در اتاق کنفرانس یا اتاق جلسات. حتی‌الامکان از ملاقات	□بلی □خیر

[8] Attachment
[9] Backup

	آن‌ها در اتاق کار جلوگیری شود.	
۹	**عدم به اشتراک گذاری فایل‌ها و فولدرها**	□بلی □خیر
۹-۱	غیرفعالسازی ویژگی اشتراک‌گذاری منابع در صورت عدم نیاز به این ویژگی. در صورت نیاز به فعالسازی، استفاده از ویژگی‌های امنیتی (مانند کلمه عبور) (به بخش ۴ رجوع شود).	□بلی □خیر
۹-۲	قطع ارتباط پس از استفاده از منابع اشتراکی، به عنوان مثال بلافاصله بعد از استفاده از پرینتر تحت شبکه لازم است تا ارتباط با آن قطع شود.	□بلی □خیر
۱۰	استفاده صحیح از رسانه‌های قابل حمل	□بلی □خیر
۱۰-۱	استفاده از رمزنگاری برای ذخیره‌ی داده‌ها در رسانه‌های قابل حمل	□بلی □خیر
۱۰-۲	استفاده از کلمه‌ی عبور برای دسترسی به رسانه‌ی قابل حمل و داده‌های آن و عدم نوشتن کلمه عبور بر روی رسانه‌ی قابل حمل	□بلی □خیر
۱۰-۳	استفاده از رسانه‌های قابل حمل فقط خواندنی (ROM) نظیر CD و DVD به منظور انتقال اطلاعات به خارج از سازمان ویا استفاده از رسانه‌های قابل حمل با قابلیت write-protected	□بلی □خیر
۱۰-۴	انتقال داده‌های درون رسانه‌های قابل حمل باید در اسرع وقت انجام شود و امحای[۱۰] این اطلاعات از حافظه قابل حمل پس از انتقال آن انجام گردد.	□بلی □خیر
۱۰-۵	نگهداری رسانه‌های قابل حمل در مکان‌های امن (کمدهای قفل دار)	□بلی □خیر
۱۰-۶	عدم خروج رسانه‌های قابل حمل از سازمان	□بلی □خیر
۱۰-۷	اطلاع‌رسانی سریع به سازمان در صورت مفقود شدن رسانه‌های قابل حمل	□بلی □خیر
۱۰-۸	امحای امن CD و DVD و سایر رسانه‌های ذخیره‌سازی (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۹	داشتن کپی از اطلاعات داخل رسانه‌های قابل حمل در یک مکان امن	□بلی □خیر

[۱۰] Wipe

۱۰-۱۰	غیرفعال‌سازی اجرای خودکار (Autorun, Autoplay) برای کلیه تجهیزات و رسانه‌های قابل حمل (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۱۱	نصب وصله‌ها بر روی سیستم به منظور جلوگیری استفاده از آسیب‌پذیری‌های مربوط به رسانه‌های قابل حمل؛ برای مثال نصب وصله‌ی مربوط به آسیب‌پذیری LNK. و PIF (MS10-046) برای جلوگیری از استفاده از این آسیب‌پذیری که یکی از روش‌های حمله به سیستم از طریق رسانه‌های قابل حمل بوده است (مانند حمله Flame)	□بلی □خیر
۱۰-۱۲	حذف حق دسترسی اجرایی از دستگاه‌های ذخیره‌سازی قابل حمل برای جلوگیری از اجرای بدافزار (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۱۳	پویش رسانه‌ها و حافظه‌های جانبی نظیر حافظه فلش و دیسک سخت خارجی، CD، DVD و انواع دیگر رسانه‌های ذخیره‌سازی قابل حمل با استفاده از ضدبدافزارها پیش از استفاده و بازکردن آن‌ها (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۱۴	استفاده از ویژگی Explore و یا تایپ نام درایو به منظور بازکردن رسانه‌های قابل حمل و عدم کلیک بر روی درایو متصل شده به کامپیوتر (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۱۵	عدم بازکردن فایل میانبر مشکوک پس از ورود به رسانه قابل حمل (به مستند امن‌سازی رسانه‌های قابل حمل رجوع شود).	□بلی □خیر
۱۰-۱۶	خارج کردن امن (safe) حافظه‌های جانبی از سیستم.	□بلی □خیر

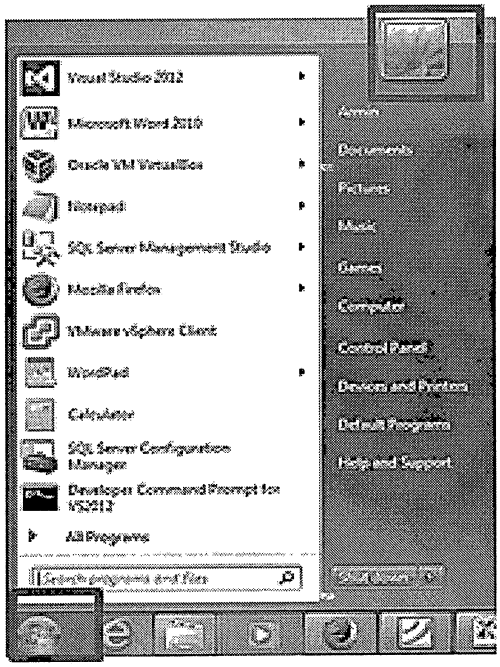
منابع

1. Data Backup Options, US-CERT, 2012
2. Recognizing and Avoiding Email Scams, US-CERT, 2008
3. Information Security Instructions for Personnel, MINISTRY OF FINANCE,2009
4. The Critical Security Controls for Effective Cyber Defense, COUNCIL ON CYBER SECURITY,2013
5. Password Security, Protection, and Management, US-CERT, 2012
6. The Risk of Using Portable Devices, US-CERT, 2012
7. Technical Trends in Phishing Attacks, CERT Coordination Center,2005
8. www.us-cert.gov/Web browser/Securing Your Web Browser _ US-CERT.htm
9. The Importance of Security Awareness Training, SANS Institute InfoSec Reading Room, 2008
10. Today's New Breed of Email-based Cyber Attacks-and What it Takes to Defend Against Them, Fire Eye, 2012
11. Protecting Your Computer, CYBER SECURITY newsletter, 2011
12. Beyond Autorun: Exploiting vulnerabilities with removable storage, IBM X-Force Advances R&B, 2011
13. The Stuxnet Worm and Options for Remediation, 2010
14. Removable Media Security for Healthcare Organizations, CREDANT, 2010
15. Data Leakage – Threats and Mitigation, SANS Institute, 2007
16. https://gosafeonline.sg/computer-security·%E2%80%93-installation-and-usage-devices-and-software
17. http://windowssecrets.com/category/in-the-wild
18. http://www.net-security.org/malware_news.php?id=1407
19. http://www.fiercecio.com/topics/security-and-privacy
20. http://www.enigmasoftware.com/computer-security
21. http://www.microsoft.com/security/default.aspx
22. https://www.checkpoint.com/index.html

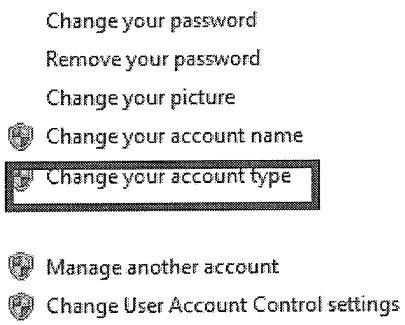
۴- ضمیمه

بند ۱-۲ : چگونگی کاهش سطح دسترسی درسیستم عامل Windows 7

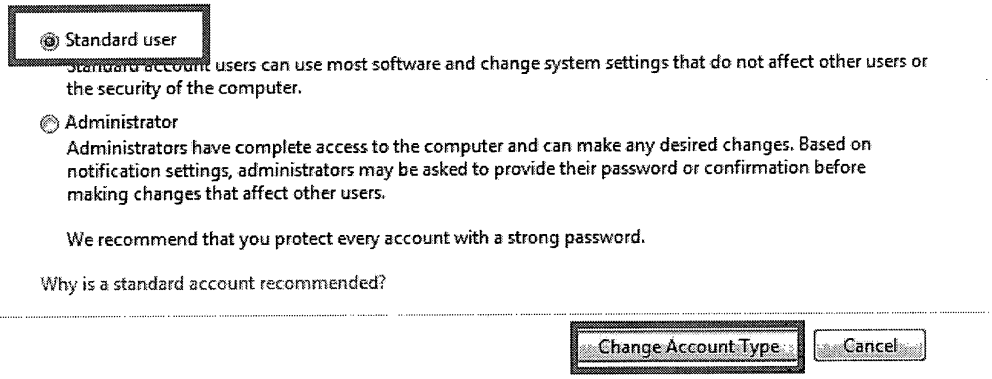
۱- منوی start را باز کنید و سپس بخش مدیریت حساب را باز کنید:



۲- گزینه Change your account type را انتخاب نمایید:

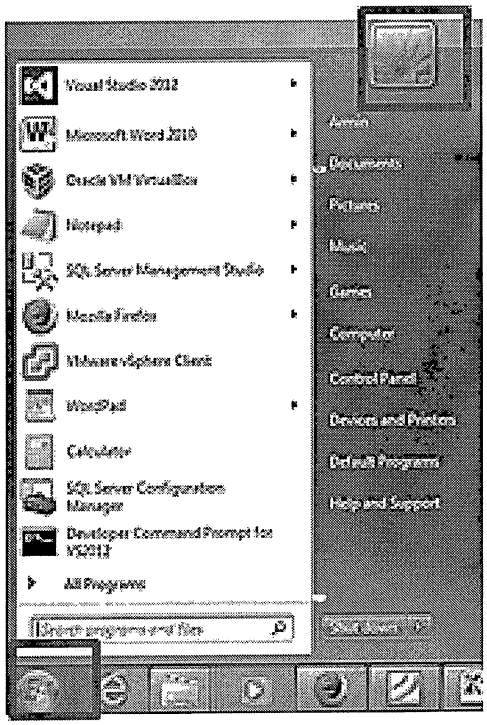


۳- تغییر زیر را اعمال نمایید و کلید Change Account Type را فشار دهید:



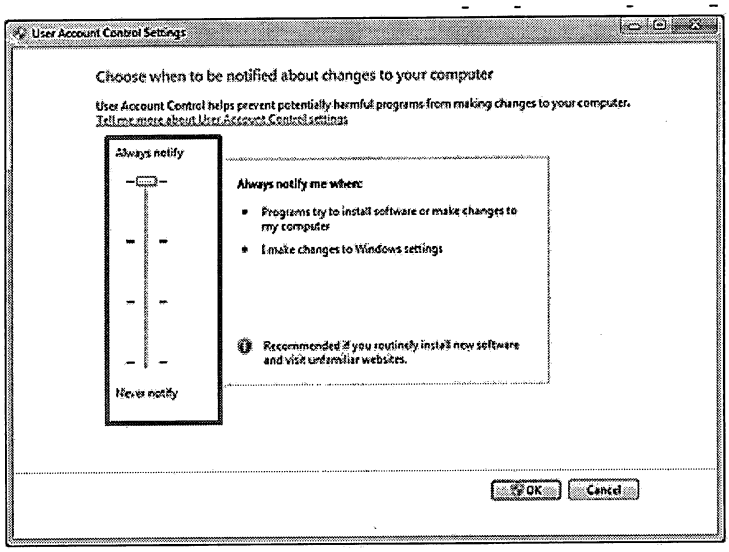
سپس تنظیمات زیر را انجام دهید:

۱- منوی start را باز کنید و سپس بخش مدیریت حساب را باز کنید:



۲- گزینه Change user account control settings را انتخاب نمایید:

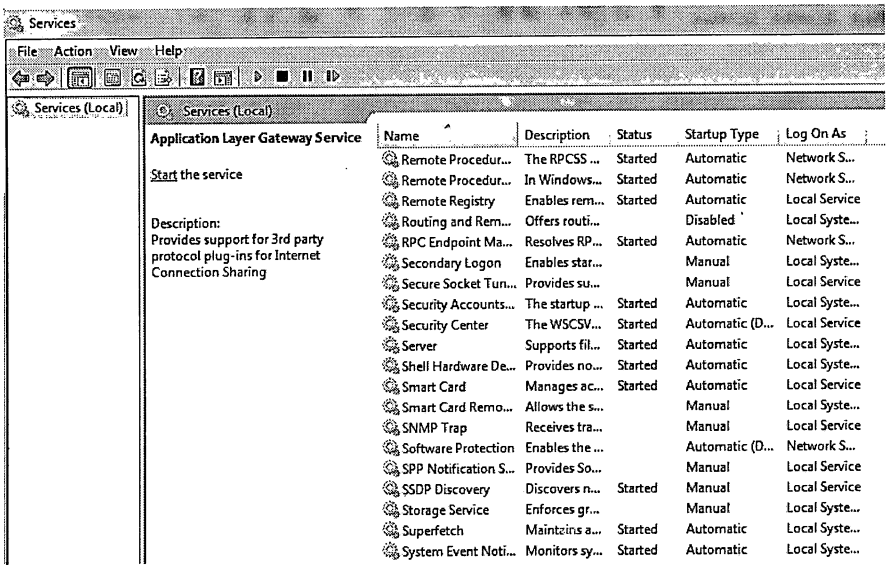
۳- تغییر زیر را اعمال نمایید و کلید OK را فشار دهید:


User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify
Always notify me when:
Programs try to install software or make changes to my computer
I make changes to Windows settings
Recommended if you routinely install new software and visit unfamiliar websites.
OK
Cancel

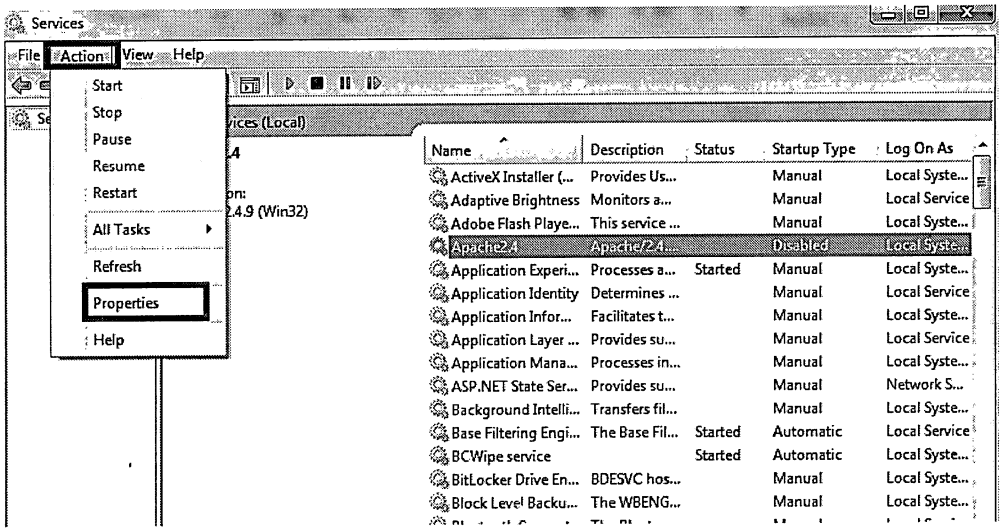
بند ۱-۵: مشاهده و غیرفعال‌سازی سرویس‌ها

سرویس‌های در حال اجرا بر روی سیستم را می‌توان با استفاده از دستورات بیان شده در زیر مشاهده کرد و موارد مشکوک یا غیرضروری را غیرفعال نمود:

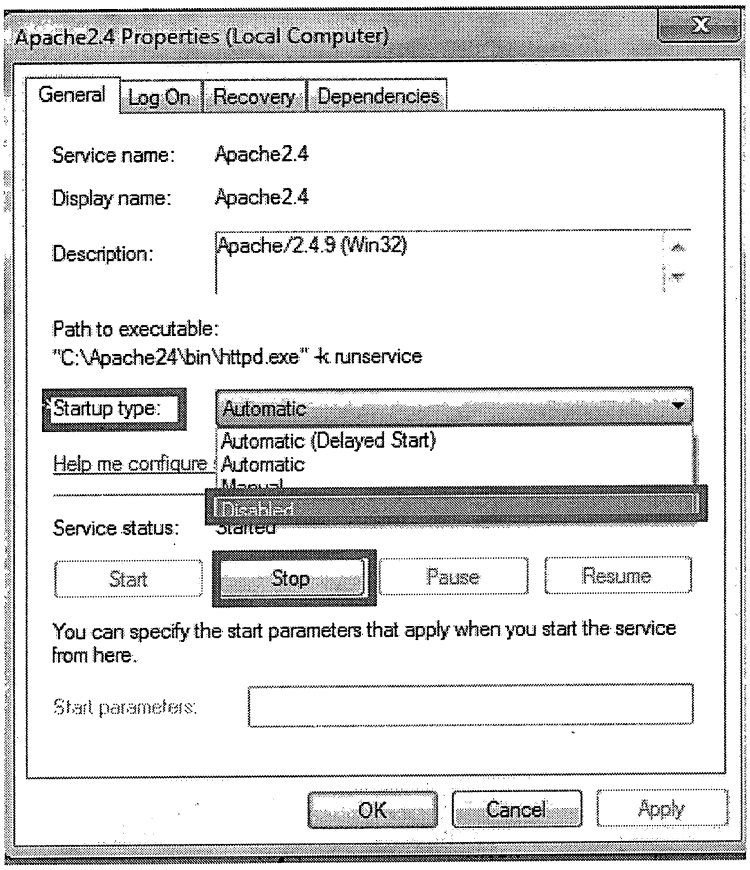
۱- ابزار "Services"را باز نمائید، در ویندوز ۷ با وارد کردن عبارت Services در بخش جستجوی start می‌توان این ابزار را مشاهده کرد:



۲- از لیست سرویس‌های نمایش داده شده، سرویس مورد نظر را انتخاب کرده و وارد Action>Properties شوید:



۳- از قسمت Startup Type، Disable و از قسمت Service statuse، Stop را انتخاب نمائید:

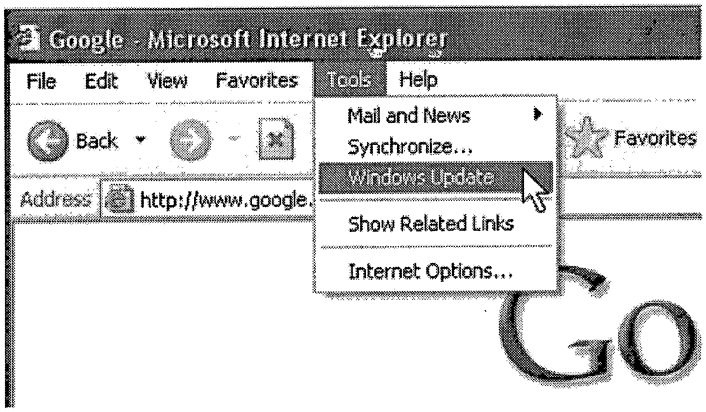


بند ۱-۸: به‌روزرسانی سیستم‌عامل و Internet Explorer

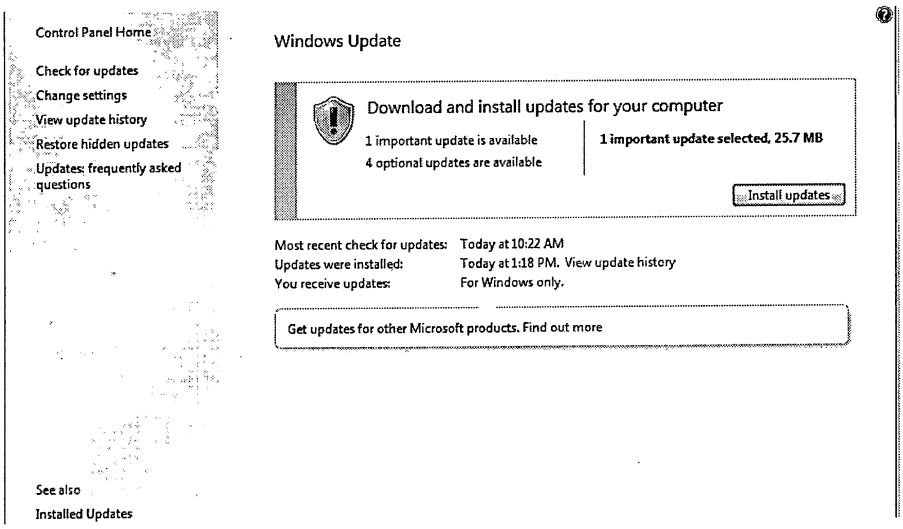
لازم به یادآوری است که بهتر است به‌روزرسانی سیستم‌عامل و اینترنت اکسپلورر از طریق سرور به روز رسانی سازمان صورت گیرد. در ادامه مراحل به‌روزرسانی سیستم عامل و اینترنت اکسپلورر نمایش داده شده است:

به روزرسانی Internet Explorer

Internet Explorer را باز کنید و وارد مسیر Tools>Windows Update شوید.

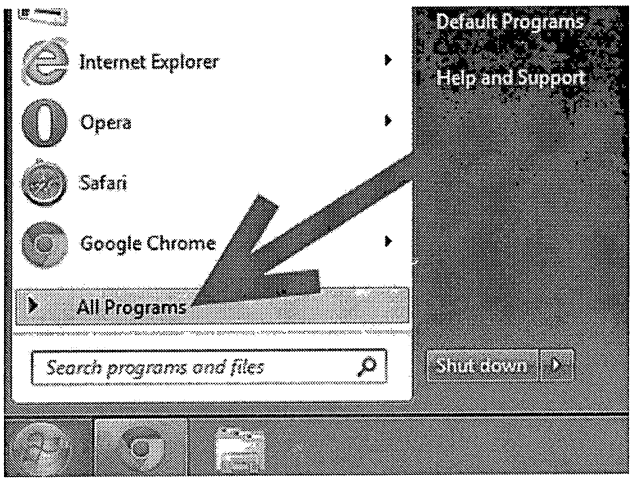


با انتخاب Windows Update صفحه‌ی زیر ظاهر می‌شود که با انتخاب install updates می‌توانید IE را به‌روز-رسانی کنید.

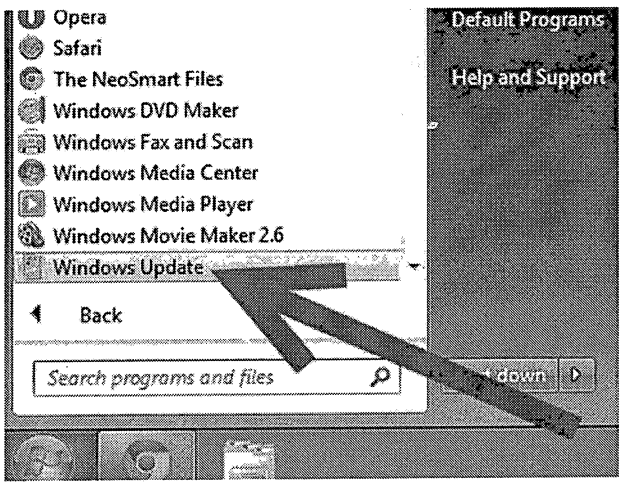


به‌روز رسانی ویندوز

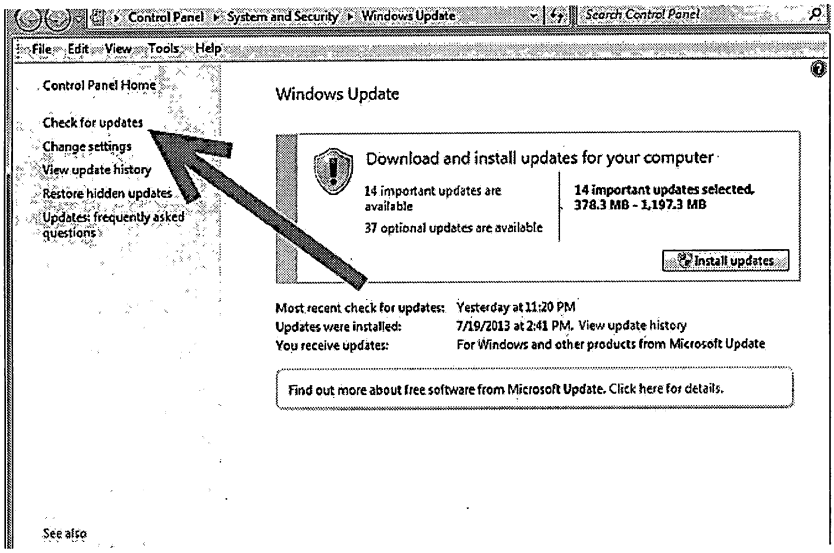
۱- از قسمت start، All Program را انتخاب نمایید.



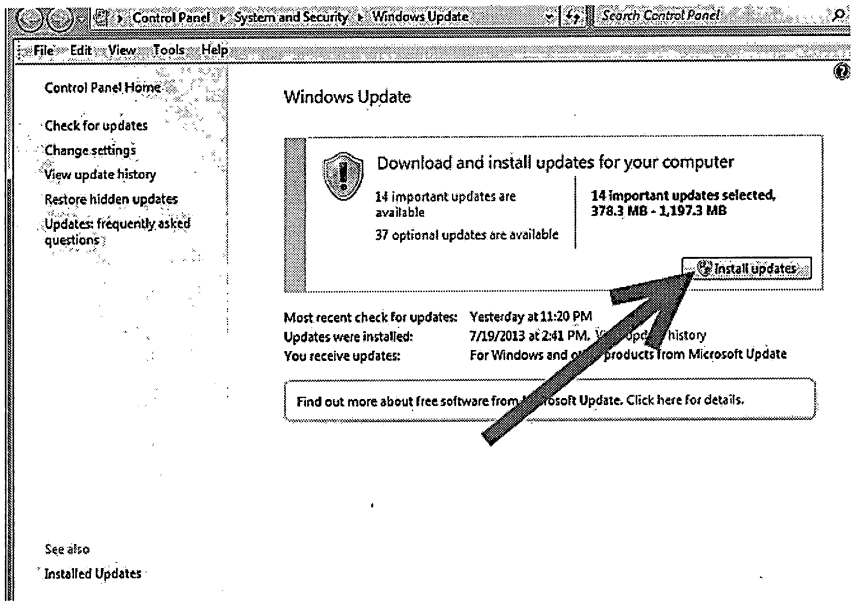
۲- سپس Windows update را انتخاب نمائید.



۳- پس از اینکه صفحه‌ی Windows Update نمایش داده شد، بر روی Check For Updates کیک نمائید تا به‌روز رسانی‌های جدید سیستم‌عامل را بررسی نماید.



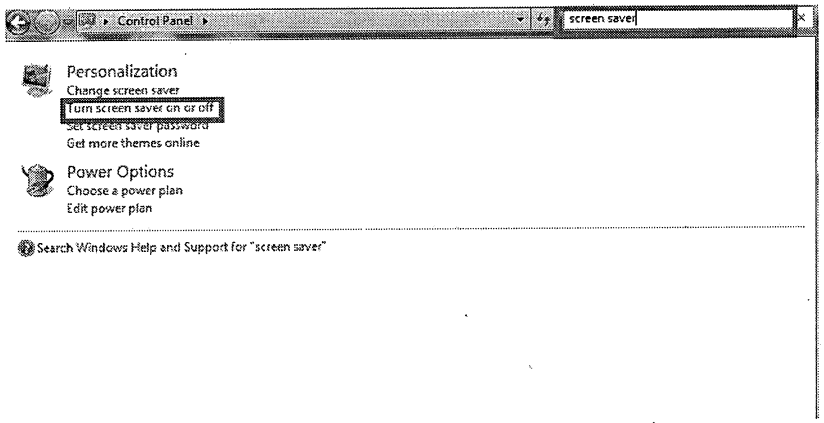
۴- سپس install updates را انتخاب نمائید تا به‌روز رسانی‌ها نصب شوند.



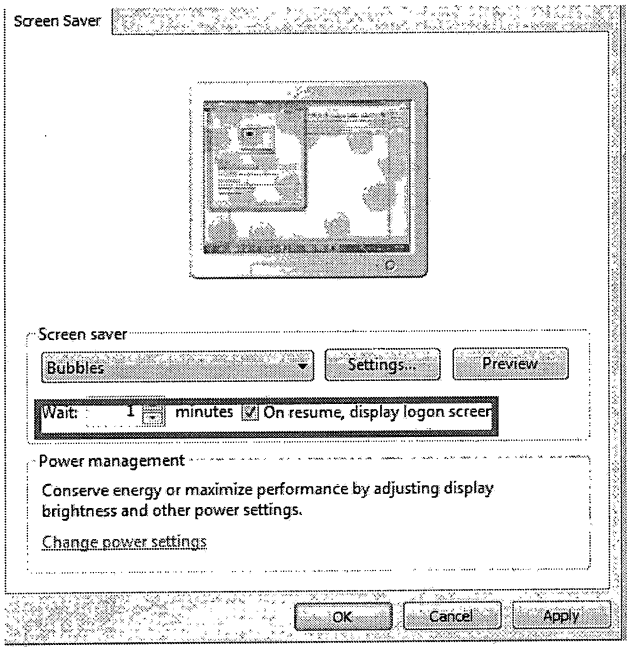
بند ۱-۱۰: استفاده از محافظ صفحه نمایش

۱- از قسمت start وارد control panel شوید.

۲- در قسمت جستجو، "screen saver" را تایپ کنید و وارد صفحه‌ی turn screen saver on or off شوید:

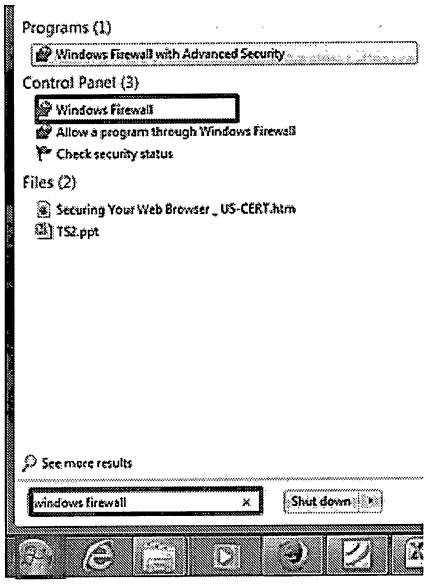


۳- سپس محافظ صفحه نمایش را فعال و مدت زمانی را برای انتظار تعیین کنید:

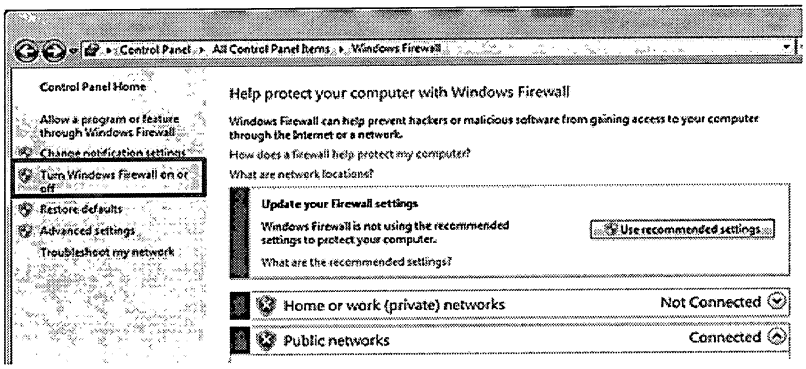


بند ۱-۱۲: چگونگی فعال‌سازی دیوار آتش در سیستم عامل Windows 7

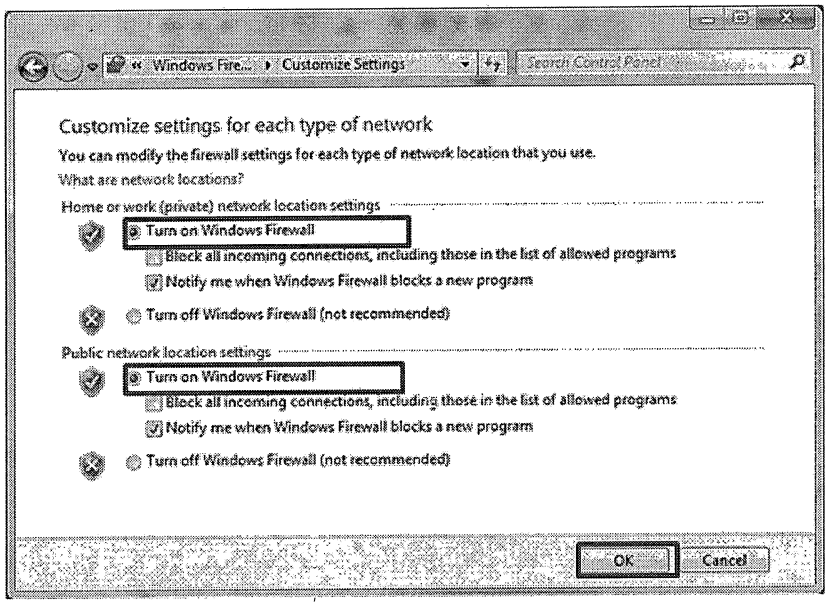
۱- منوی start را باز کرده و عبارت Windows firewall را در بخش جست‌وجو (Search) تایپ نموده و سپس گزینه Windows firewall را انتخاب نمایید:



۲- در صفحه باز شده گزینه Turn Windows Firewall on or off را انتخاب نمایید:



۳- تنظیمات زیر را اعمال نمایید و کلید OK را فشار دهید:


Windows Fire... ▸ Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network location that you use.
What are network locations?
Home or work (private) network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
Public network location settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed programs
Notify me when Windows Firewall blocks a new program
Turn off Windows Firewall (not recommended)
OK
Cancel

بند ۱-۱۳: بستن پورت‌های TCP/UDP بلااستفاده

به‌منظور بستن پورت‌های بلااستفاده دو روش وجود دارد: ۱- بستن سرویسی که از آن پورت استفاده می‌کند.
۲- بلاک کردن پورت مورد نظر از طریق فایروال

روش اول: بستن سرویس استفاده کننده از پورت

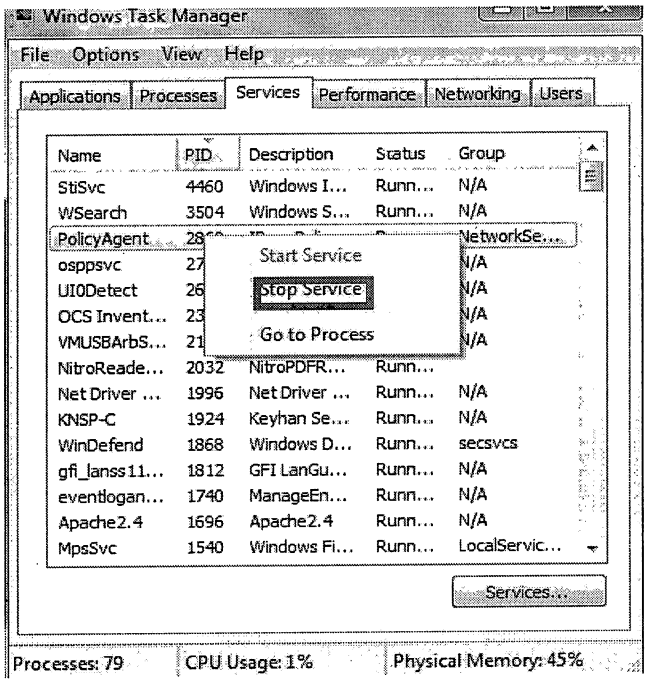
۱- از قسمت "start"، command prompt را باز کنید و دستور netstat –anob را به‌منظور مشاهده‌ی پورت‌ها و سرویس‌هایی که از آن‌ها استفاده می‌کنند، وارد کنید:

```
C:\Users\       >netstat -anob

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       1696
 [httpd.exe]
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       716
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:8400           0.0.0.0:0              LISTENING       1916
 [java.exe]
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       416
 [wininit.exe]
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       840
  eventlog
 [svchost.exe]
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       1044
  Schedule
```

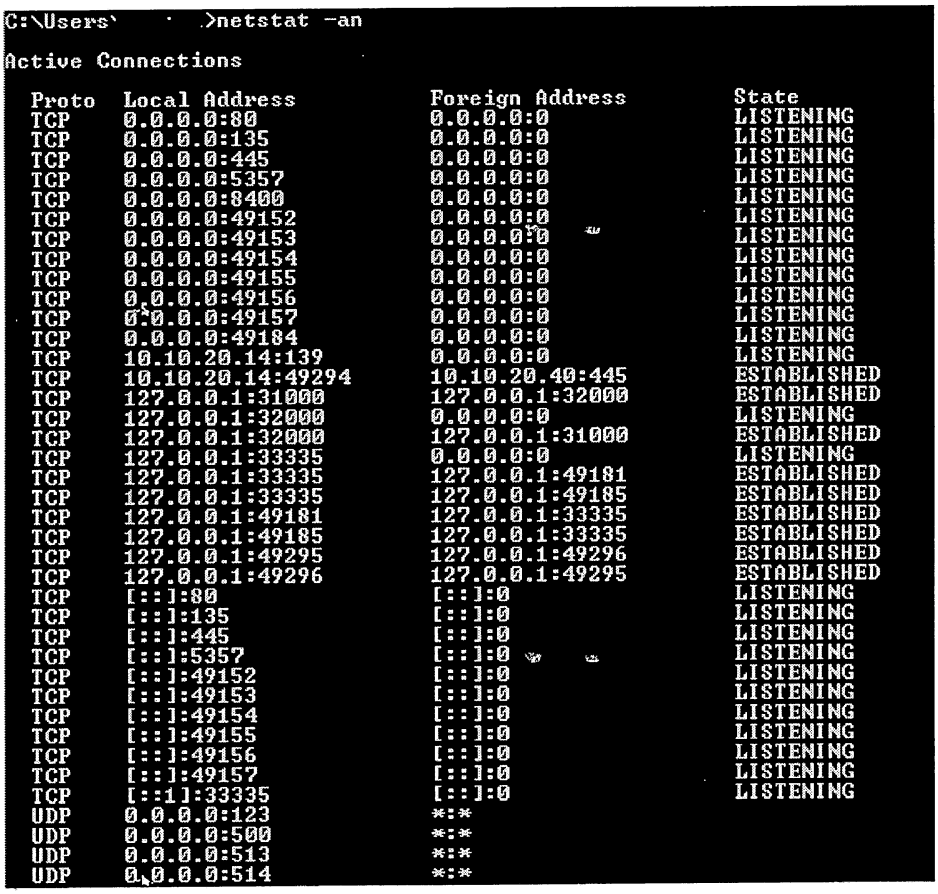
۲- با استفاده از کلیدهای ALT+CTRL+DEL، "task manager"را اجرا کرده و از تب services، PID سرویس مورد نظر را انتخاب کرده و آن را متوقف کنید:



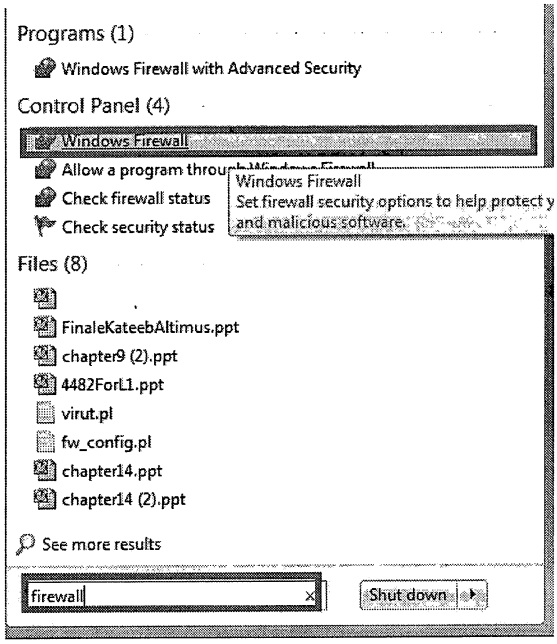
۳- با استفاده از روش بیان شده در بخش ۴ بند ۱-۶ سرویس مورد نظری که از این پورت استفاده می‌کند را نیز متوقف کنید.

روش دوم: بلاک کردن پورت از طریق تنظیمات فایروال

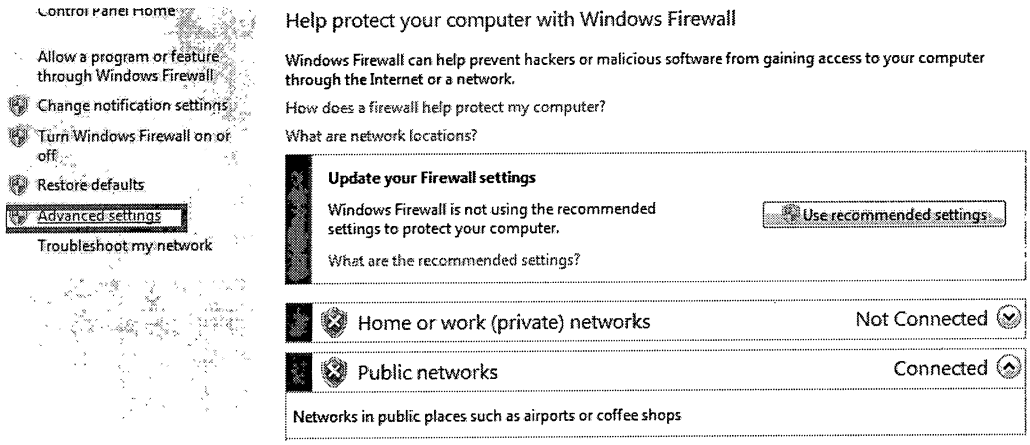
۱- از قسمت "start"، command prompt را باز کرده و دستور netstat –an را به‌منظور مشاهده‌ی پورت‌های TCP/UDP سیستم وارد کنید:



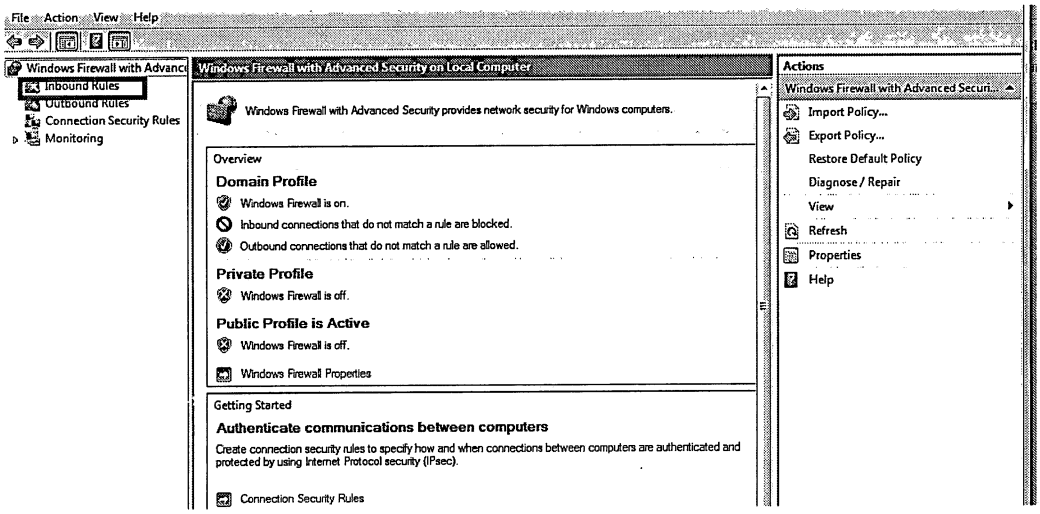
۱- به این ترتیب می‌توانید لیست پورت‌های TCP/UDP را مشاهده کنید و در صورتی که از پورتی استفاده نمی‌کنید در قسمت "start" عبارت "firewall" را تایپ کرده و وارد windows firewall شوید:



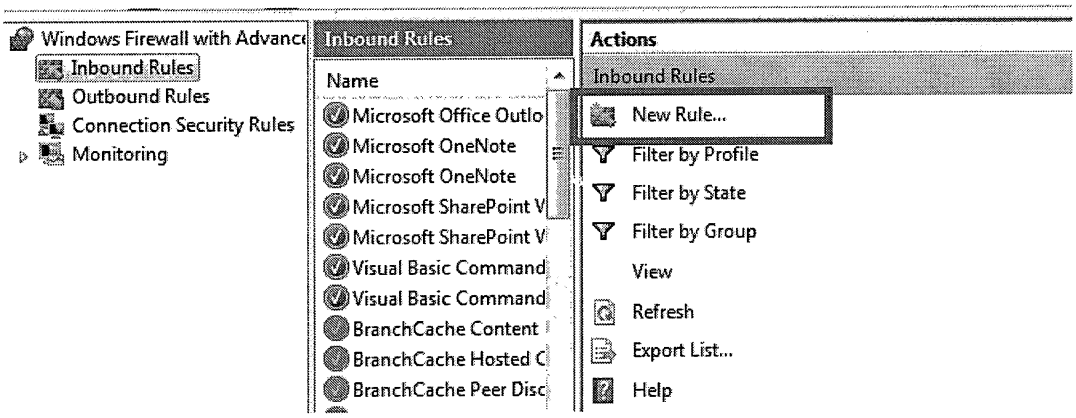
۱- از منوی سمت چپ "Advanced setting" را انتخاب کنید:



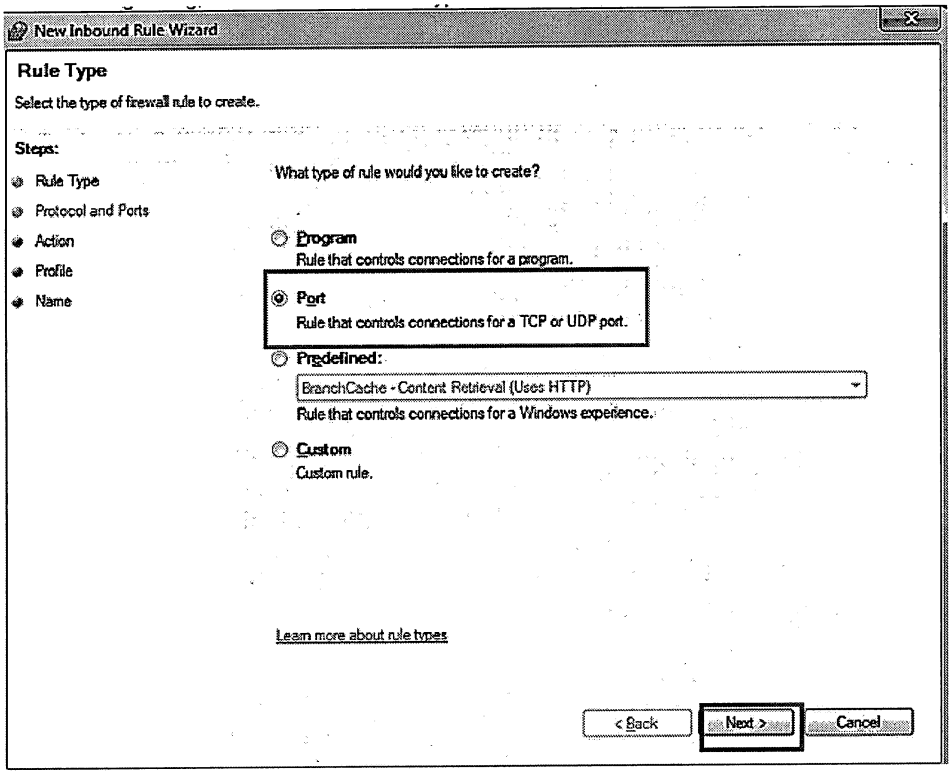
۱- از منوی سمپ چپ "Inbound Rules" را انتخاب کنید: (مراحل بیان شده را برای "Outbounded Rules" نیز به همین ترتیب انجام دهید)



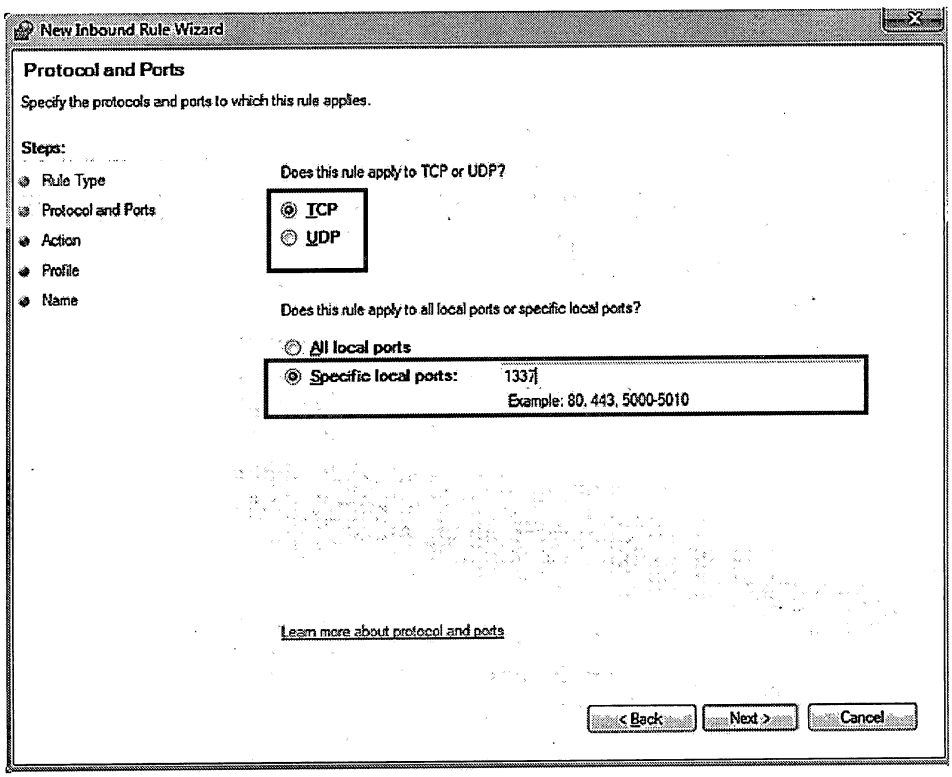
۲- از منوی سمت راست، بر روی "New Rule" کلیک نمائید:



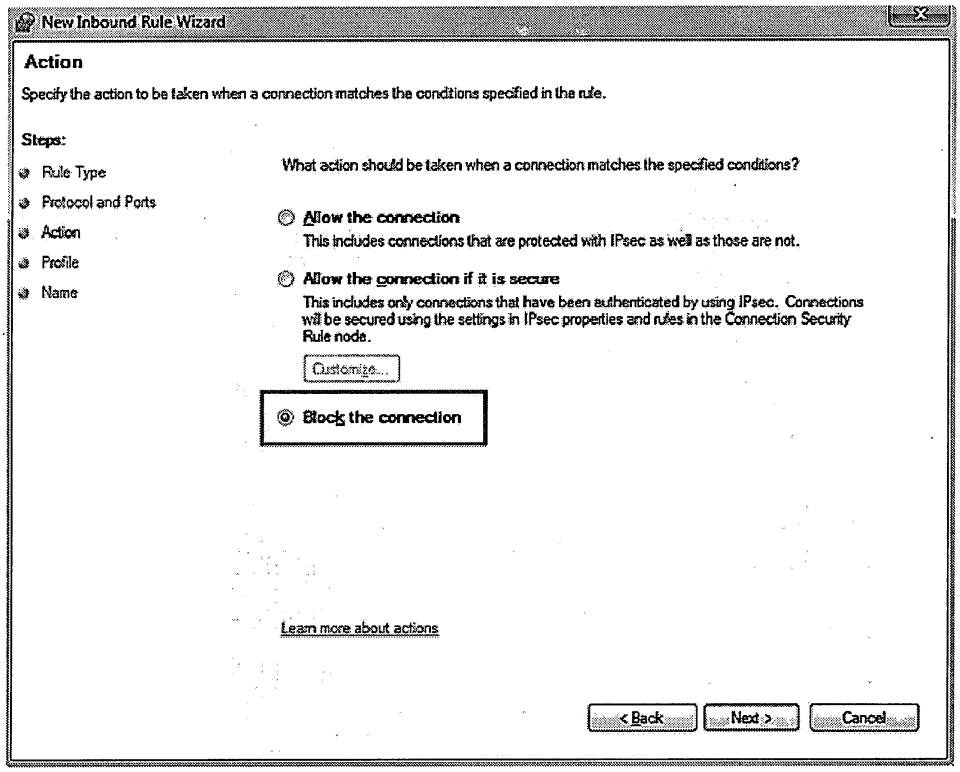
۳- گزینه‌ی port را از منوی سمت راست انتخاب کرده و بر روی Next کلیک کنید:



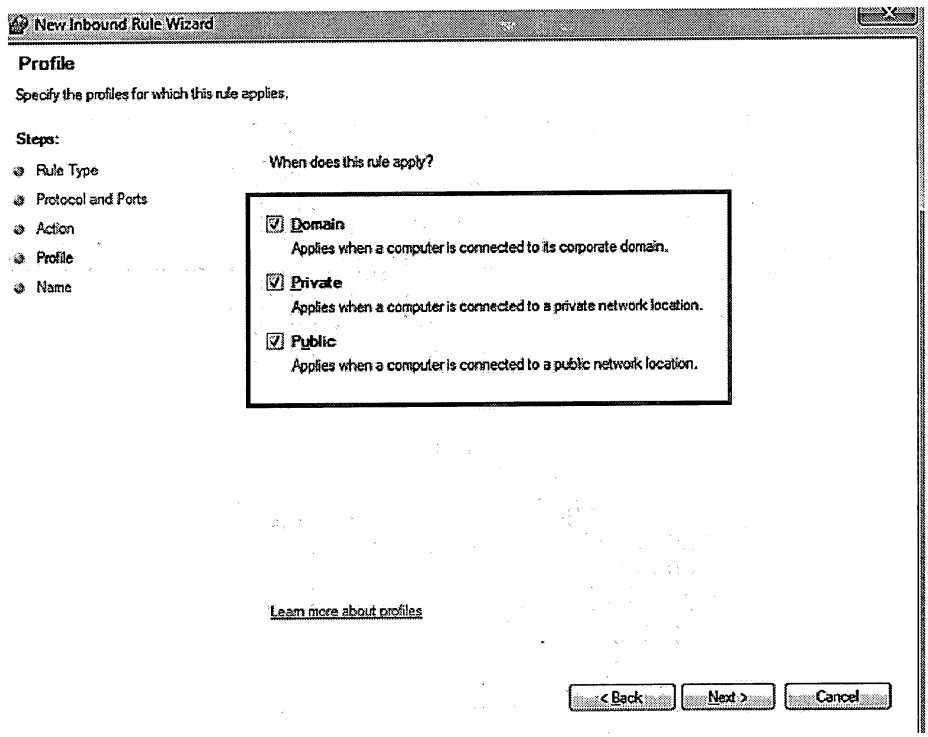
۴- بسته به اینکه پورت TCP یا UDP را می‌خواهید ببندید، یکی از گزینه‌های TCP یا UDP را انتخاب کرده و پس از وارد کردن شماره پورت در قسمت specific port ، بر روی Next کلیک کنید:



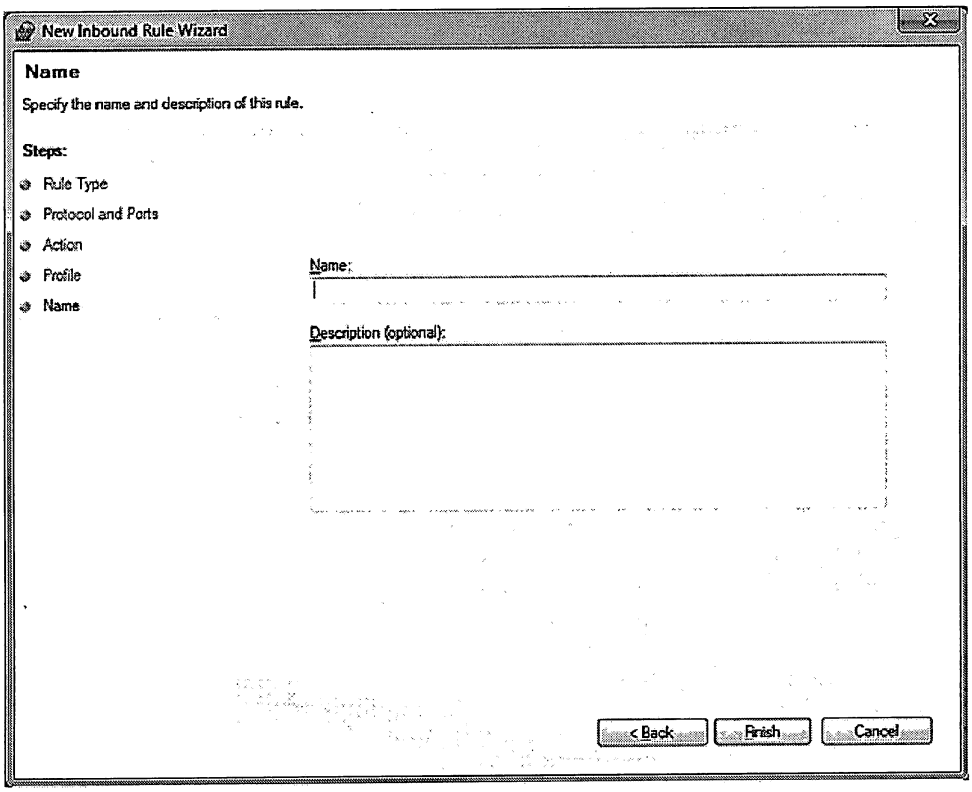
۵- سپس گزینه‌ی Block the connection را انتخاب کرده و Next را بزنید:



۶- در این مرحله محدوده‌ای که این قانون قرار است بر روی آن اعمال شود را با انتخاب گزینه‌های Domain، Private و Public مشخص کنید:

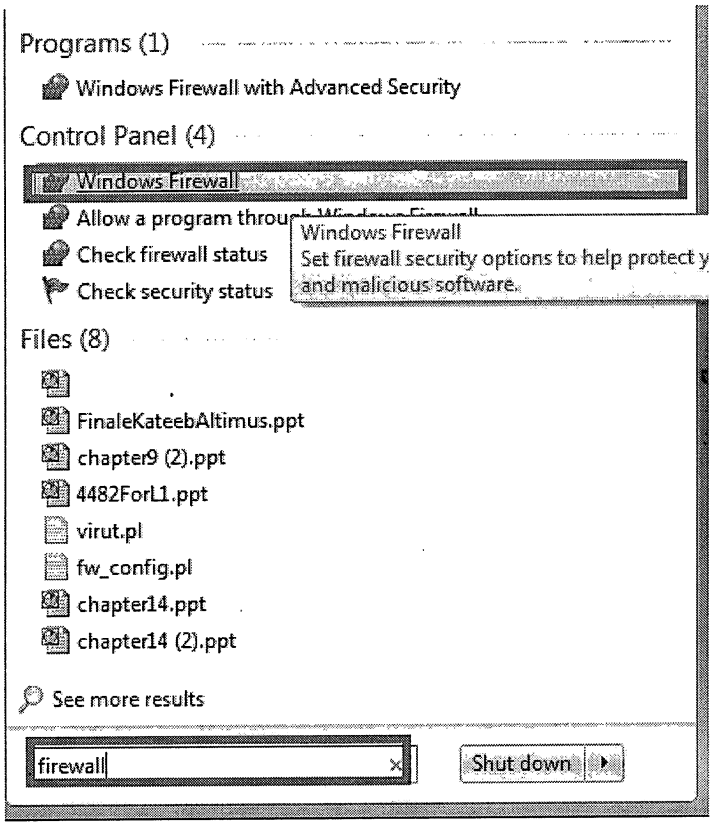


۷- در مرحله بعد نامی برای قانون تعریف شده مشخص کرده و finish را انتخاب کنید:

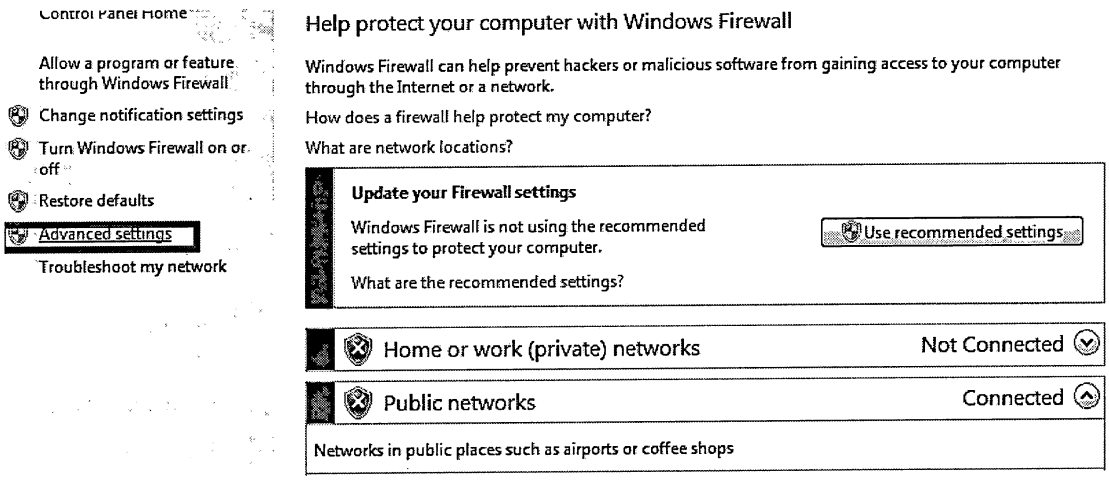


بند ۱-۱۴: پیکربندی فایروال در قبول کردن ipهای مجاز

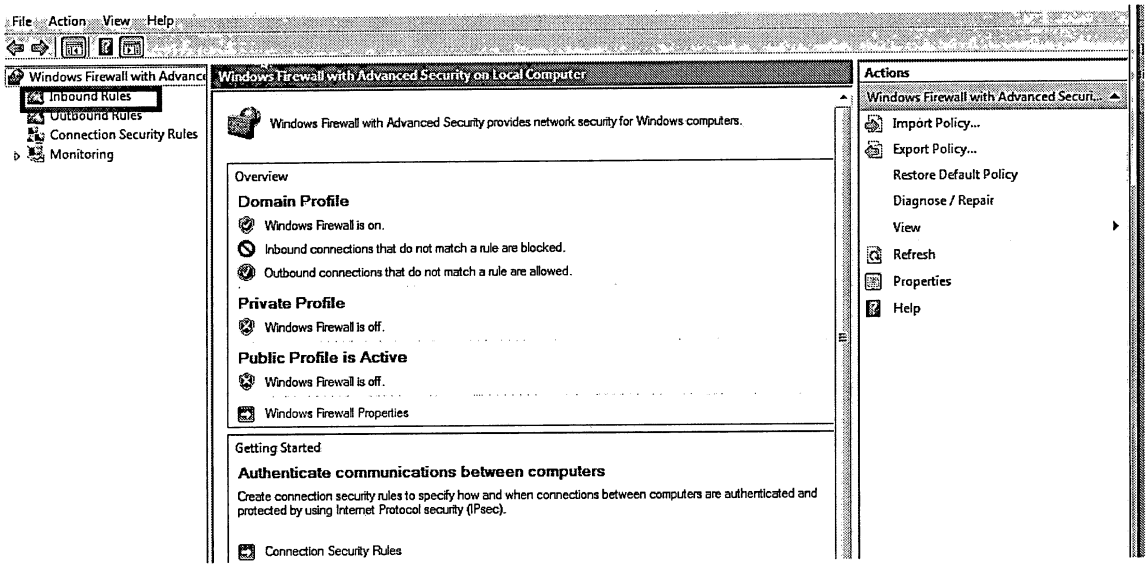
۱- در قسمت "start" عبارت "firewall" را تایپ کرده و وارد windows firewall شوید:



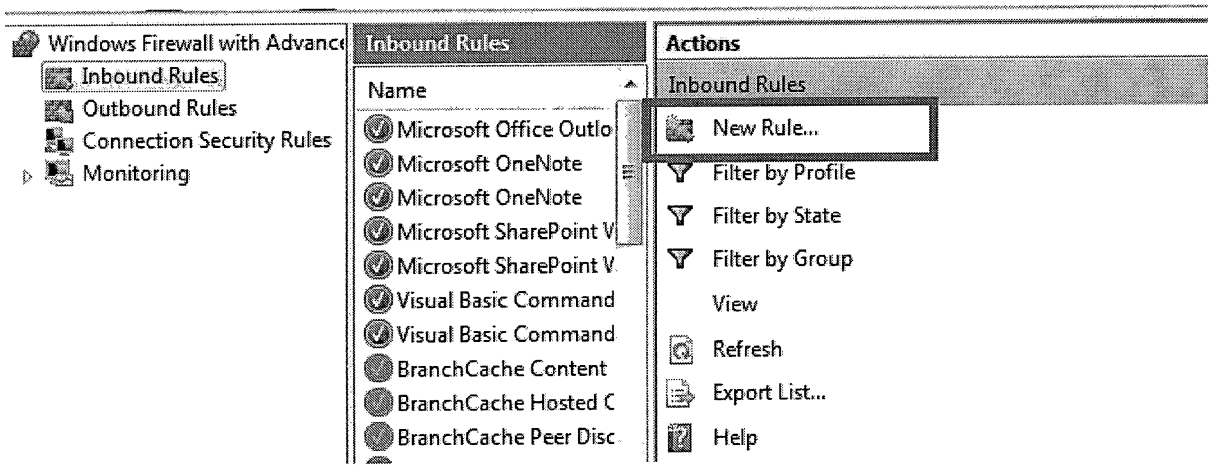
۲- از منوی سمت چپ "Advanced setting" را انتخاب نمائید:



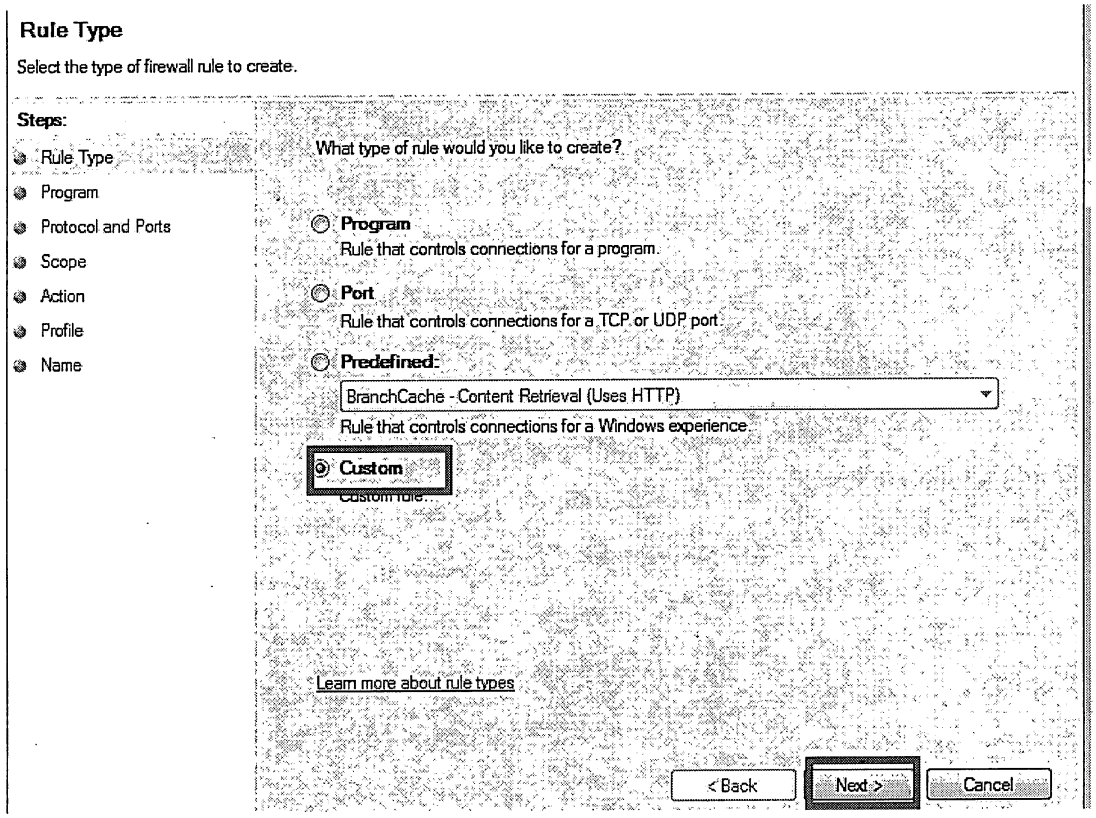
۳- از منوی سمت چپ "Inbound Rules" را انتخاب کنید: (برای "Outbounded Rules" نیز این موارد را انجام دهید)



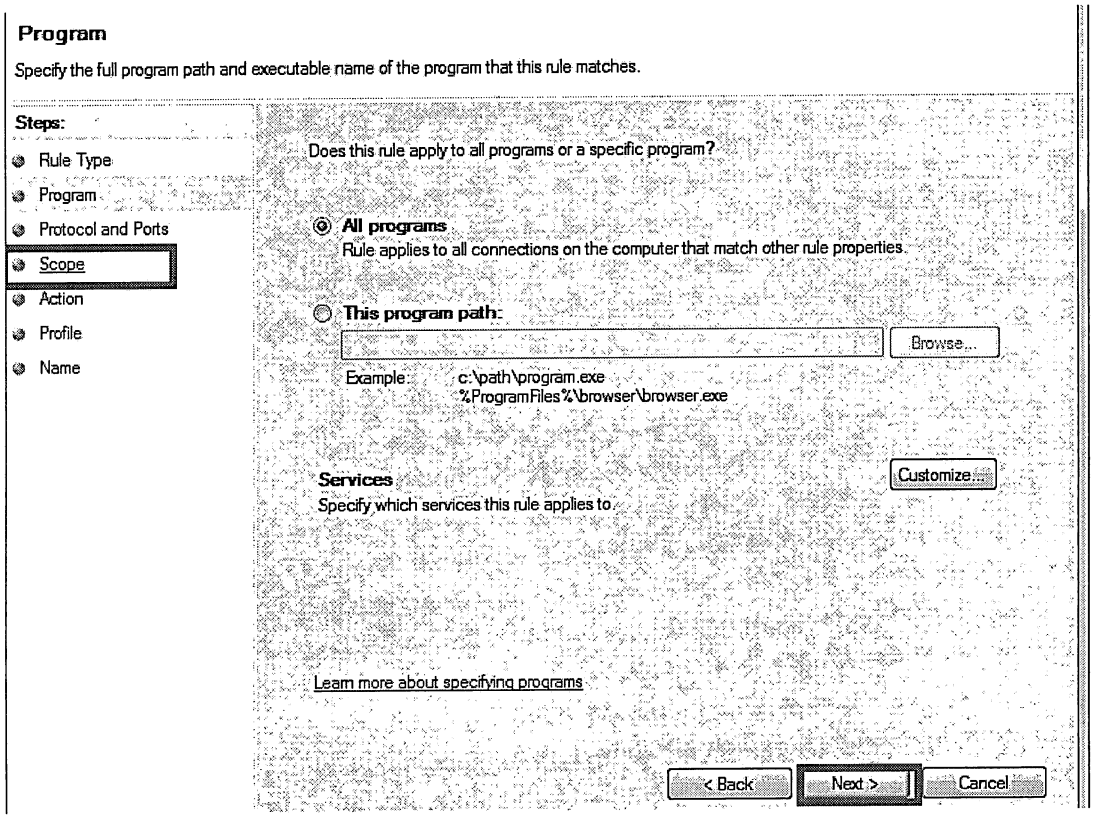
۴- از منوی سمت راست، بر روی "New Rule" کلیک کنید:



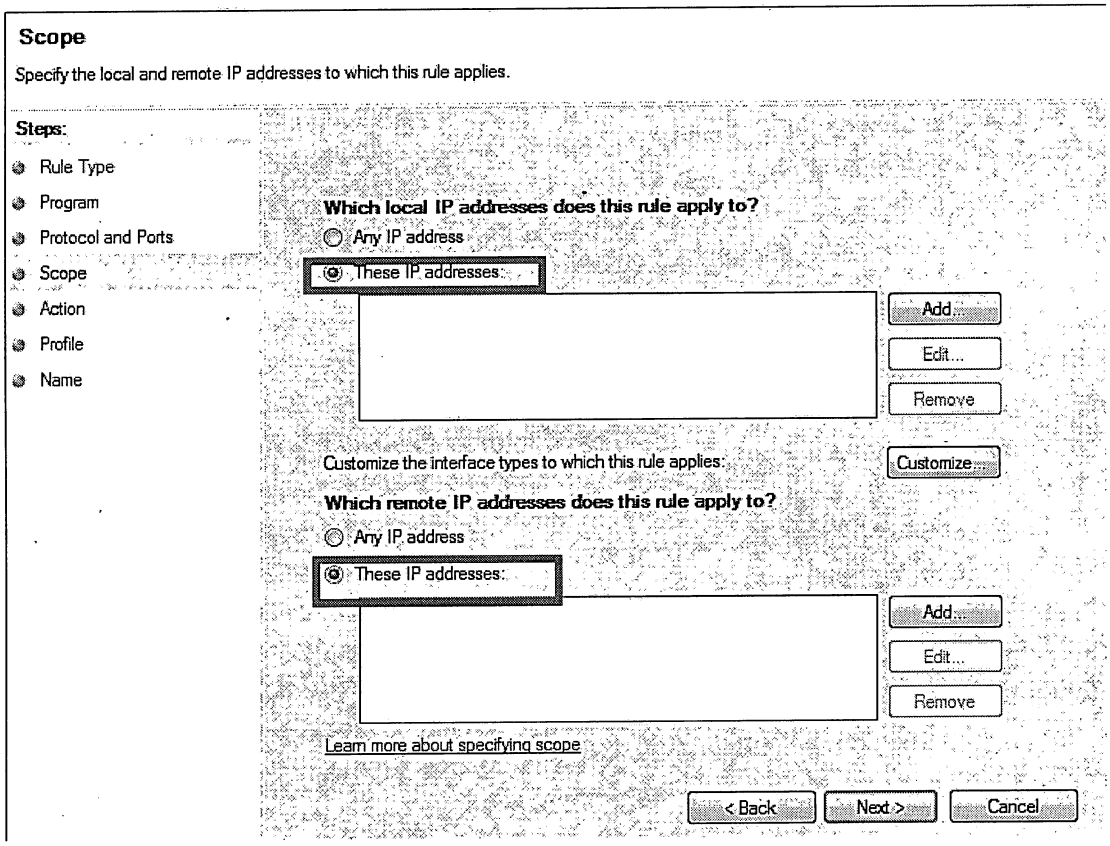
۵- سپس گزینه‌ی "custom" را انتخاب کرده و بر روی"Next" کلیک کنید:



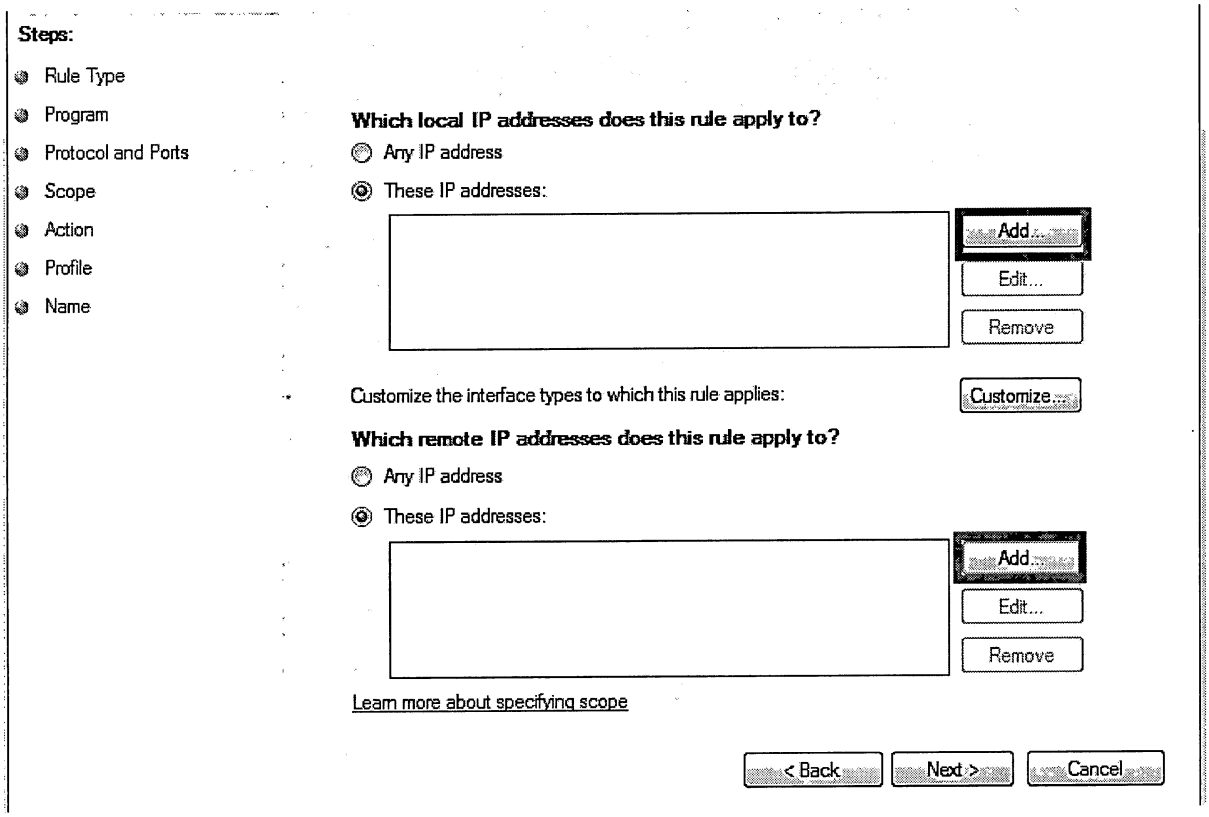
۶- در صفحه نمایش داده شده، از منوی سمت چپ، "Scop" را انتخاب کـرده و بـر روی "Next" کلیـک کنید:



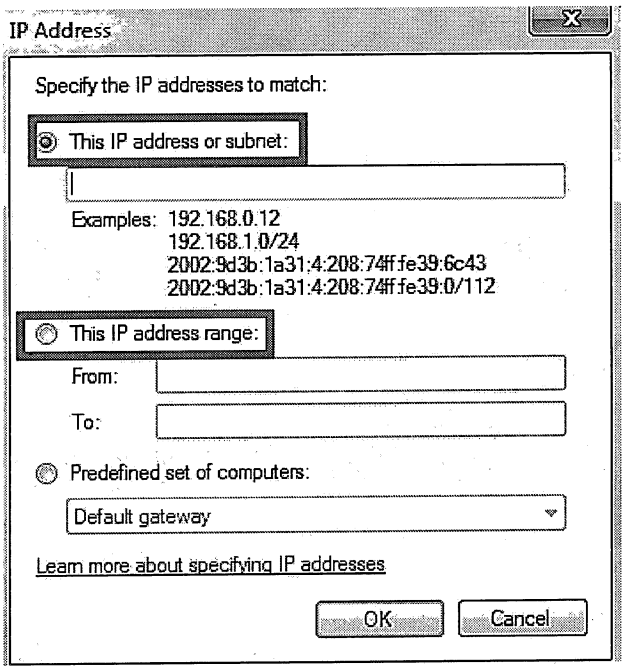
۷- به این ترتیب می‌توانید ادرس‌های ip محلی و آدرس‌های ip راه دور مشخصی را وارد کنید، برای این منظور لازم است گزینه‌ی "These ip address" را انتخاب کنید:



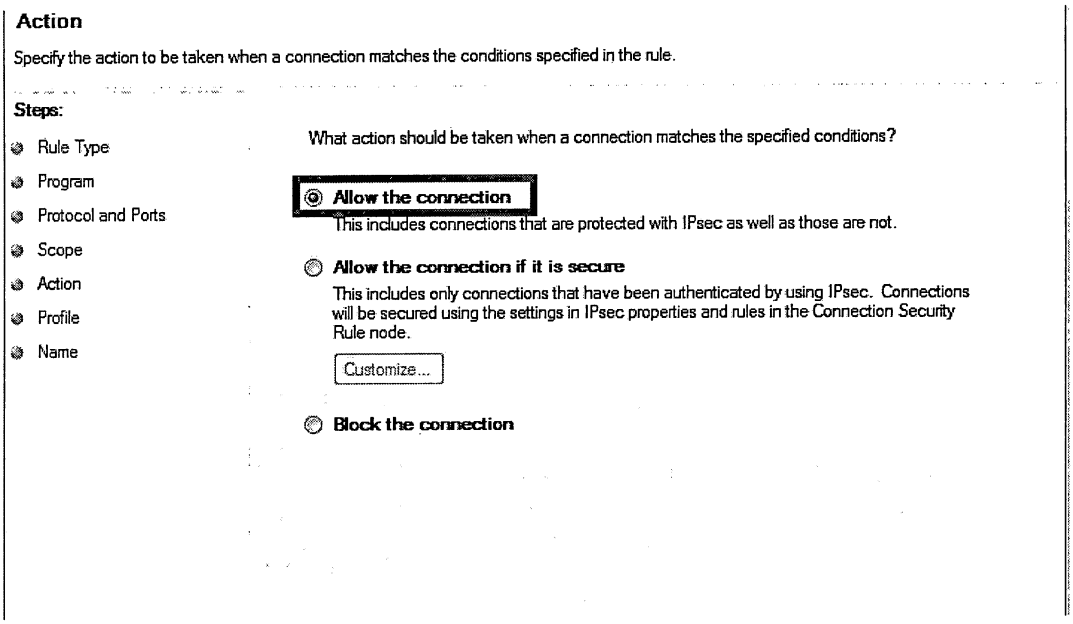
۸- برای اضافه کردن آدرس ip در هر بخش add را انتخاب کنید:



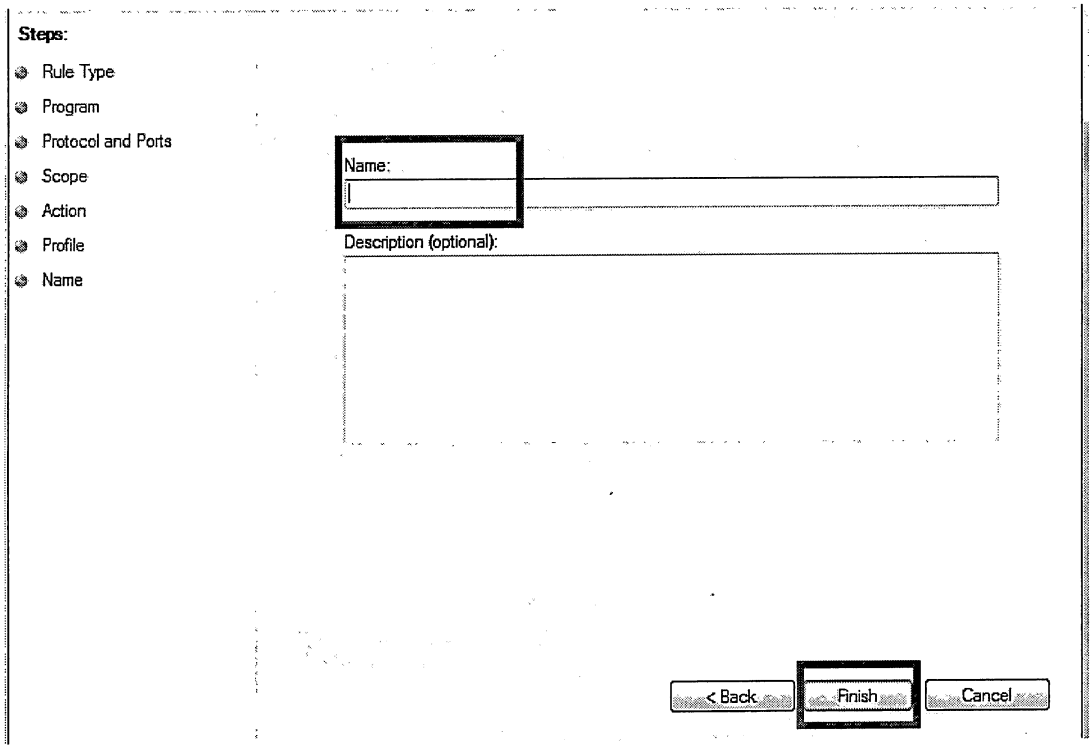
۹- در صفحه‌ی نمایش داده شده با انتخاب "This IP address or subnet" می‌توانید ip مشخصی را انتخاب یا با انتخاب گزینه "This IP address range" بازه‌ای را برای آدرس‌های ip، مشخص کنید و سپس OK را بزنید:



۱۰- در صفحه‌ی نمایش داده شده "allow connection" را انتخاب کنید:



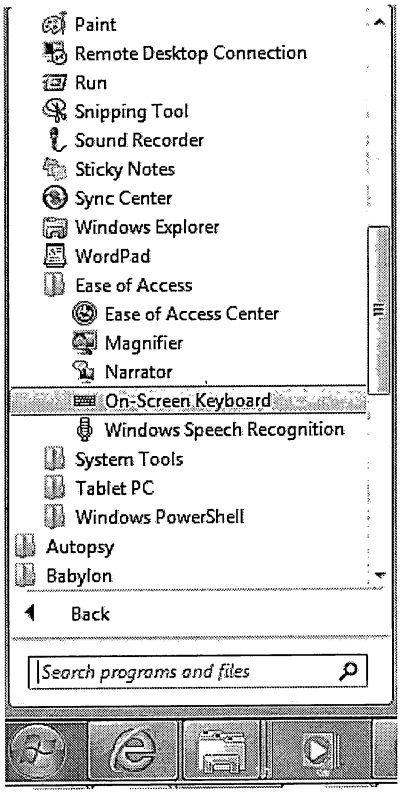
۱۱- سپس با انتخاب "next"نامی برای آن تعریف کرده و finish را انتخاب کنید:



بند ۵-۶: استفاده از On-Screen Keyboard

بهتر است در سایت‌هایی که نیاز به حساب‌های کاربری و کلمات عبور است (مانند سایت‌های بانک‌ها) از On-Screen Keyboard که در ادامه تشریح شده است، استفاده کرد.

۱- از قسمت Access start>All program> Accessories>Ease of ، On-Screen Keyboard را انتخاب کنید.



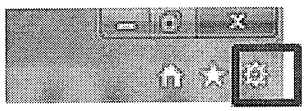
۲- صفحه کلید مجازی به صورت زیر بر روی صفحه نمایش نشان داده می‌شود که می‌توان با استفاده از موس، کلمات عبور و نام کاربری را با کمک آن وارد کرد.

بند ۵-۷ : پیشنهاداتی جهت افزایش امنیت در پیکربندی مرورگرها

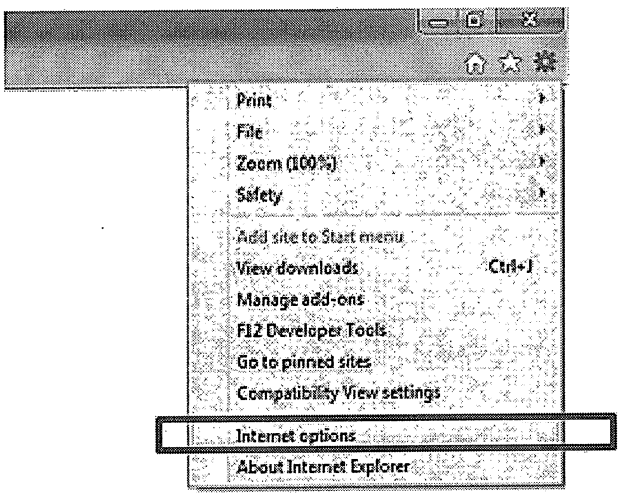
مرورگر IE

۱- مرورگر IE را باز کنید.

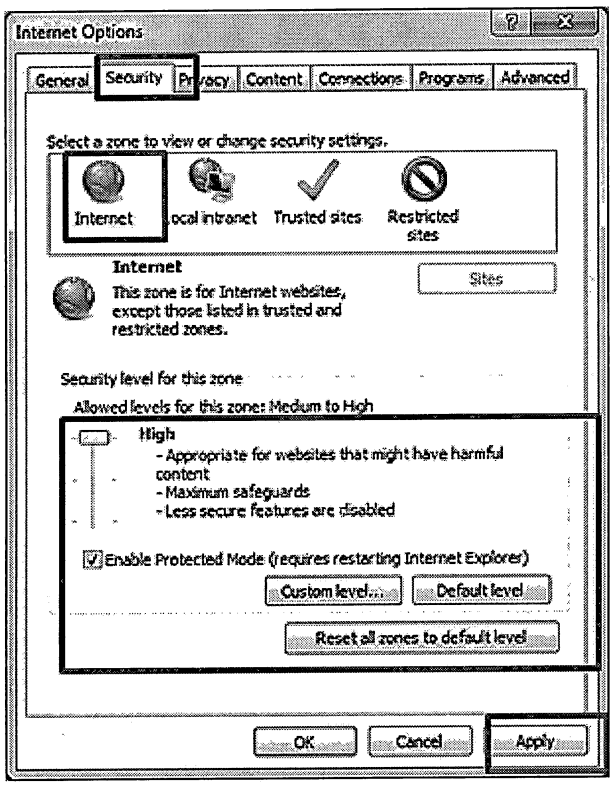
۲- گزینه Tools را انتخاب کنید (یا کلید Alt و x را با هم فشار دهید و یا علامت مشخص‌شده زیر را انتخاب کنید):



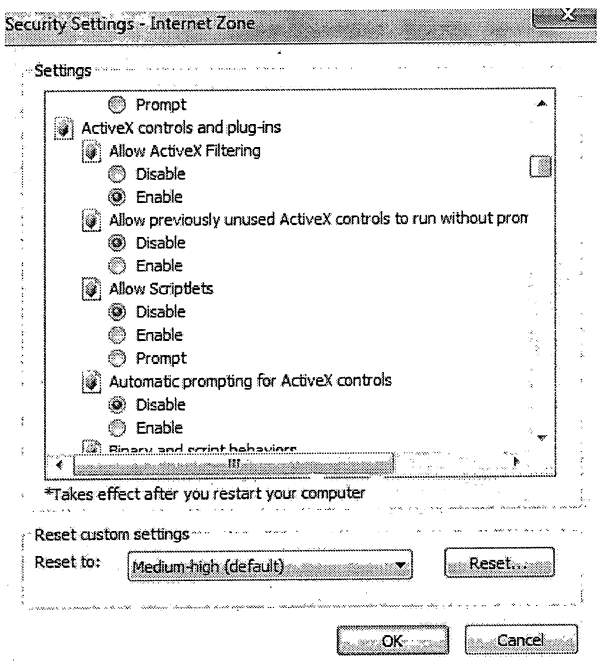
۳- گزینه Internet Options را از منوی بازشده انتخاب کنید:



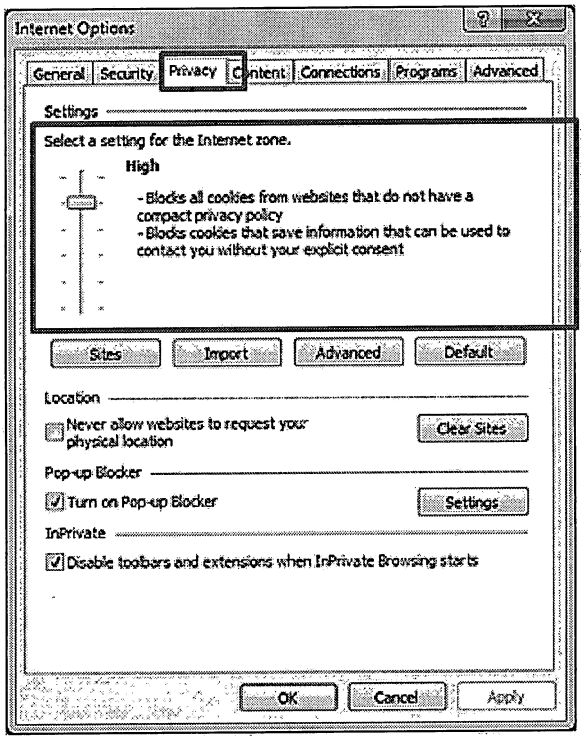
۴- در بخش Security مطابق شکل زیر گزینه Internet را انتخاب کرده ، پس از انتخاب مقدار High کلید Apply را بزنید:



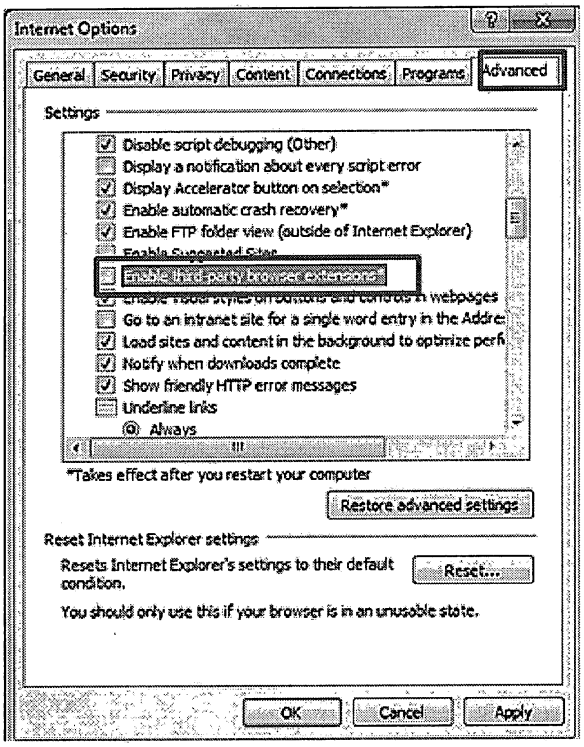
سپس وارد Custom level شوید و برای اطمینان از غیرفعال بودن activex از وجود موارد زیر اطمینان یابید:



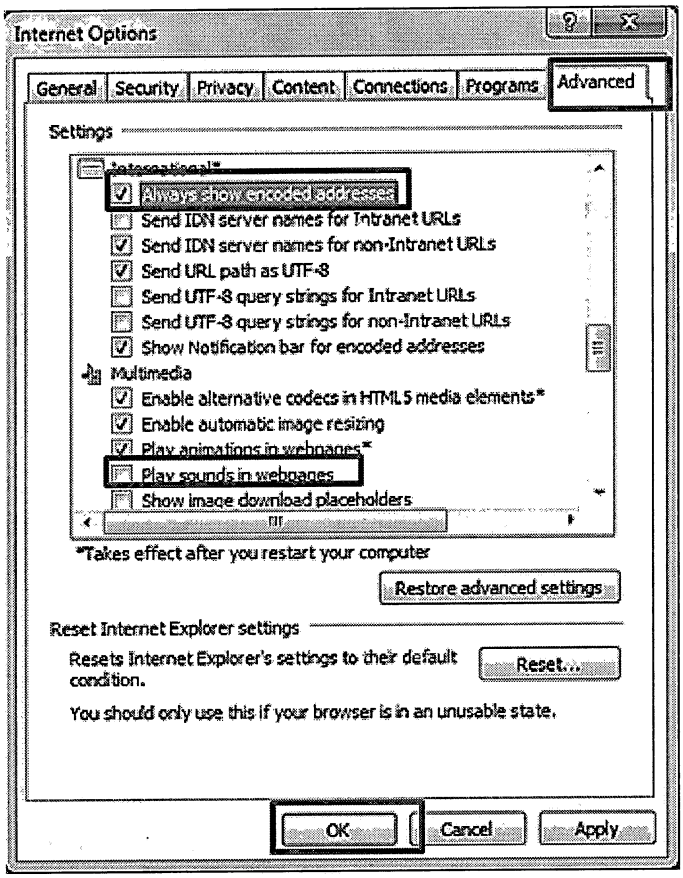
۵- حال در بخش Privacy مقدار High را انتخاب کنید:



۶- سپس در بخش Advanced گزینه Third-Party browser extensions را غیر فعال کنید:



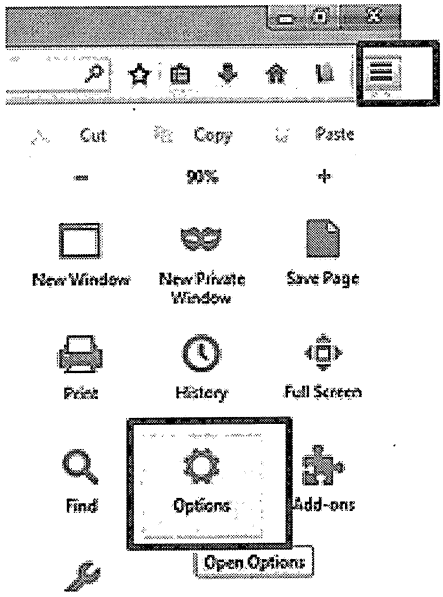
۷- در مرحله بعد گزینه Always show encoded address را انتخاب و فعال و گزینه Play sounds in webpages را غیرفعال نموده و کلید OK را انتخاب کنید


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Always show encoded addresses
Send IDN server names for Intranet URLs
Send IDN server names for non-Intranet URLs
Send URL path as UTF-8
Send UTF-8 query strings for Intranet URLs
Send UTF-8 query strings for non-Intranet URLs
Show Notification bar for encoded addresses
Multimedia
Enable alternative codecs in HTML5 media elements*
Enable automatic image resizing
Play animations in webpages*
Play sounds in webpages
Show image download placeholders
*Takes effect after you restart your computer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
OK
Cancel
Apply

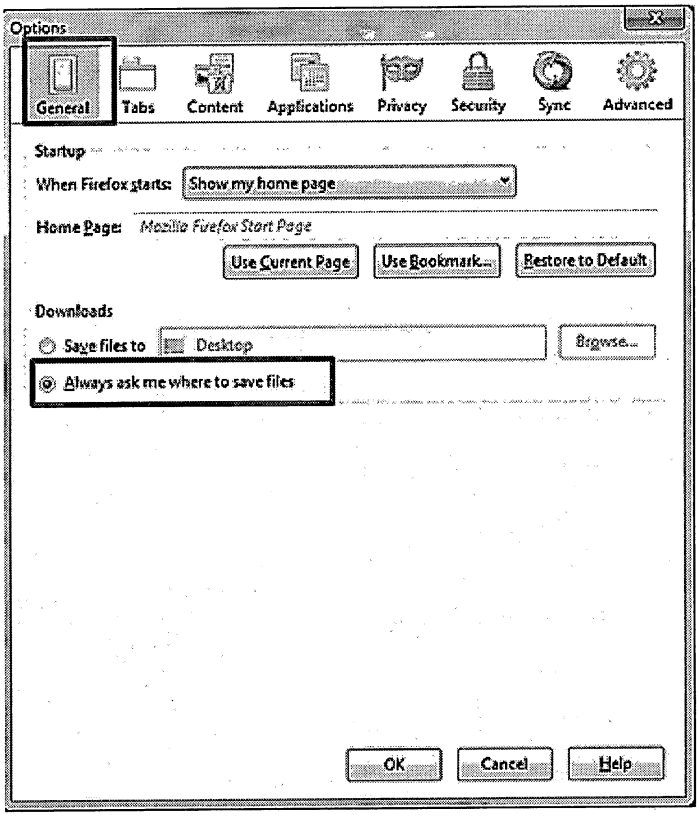
مرورگر Mozilla Firefox

۱- مرورگر Firefox را بازکنید.

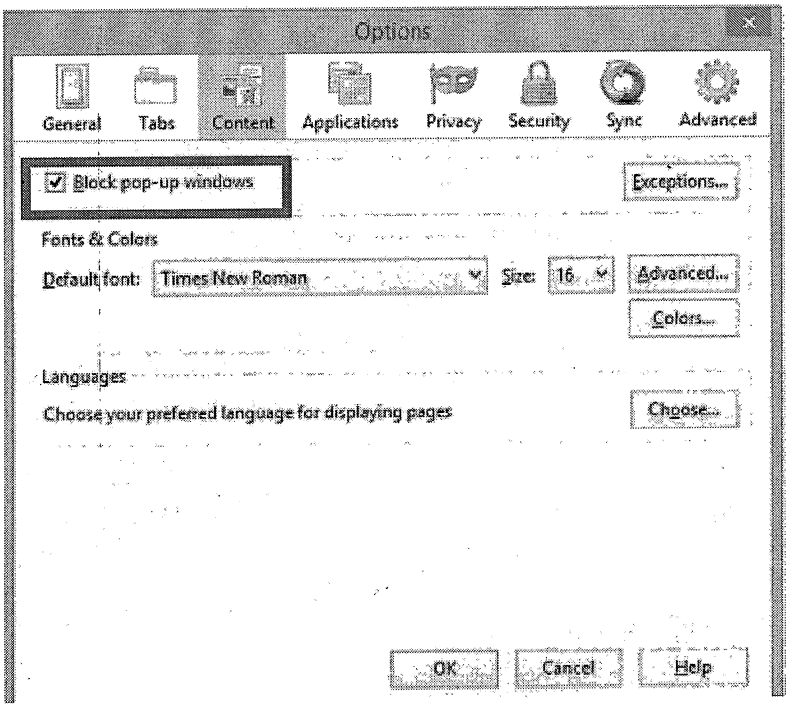
۲- از منوی Tools گزینه Options را انتخاب کرده و یا مطابق شکل زیر، آیکون Options را انتخاب کنید:



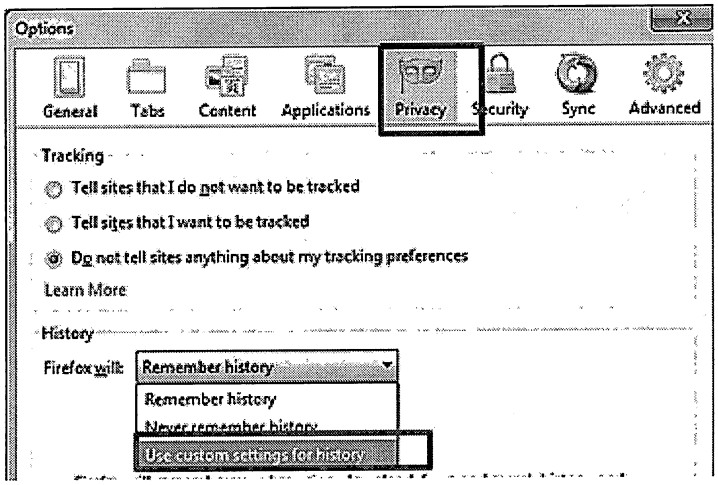
۳- در بخش General گزینه Always ask me where to save file را انتخاب کنید تا همواره در زمان ذخیره اطلاعات، در مورد مکان ذخیره‌سازی پرسش شود:



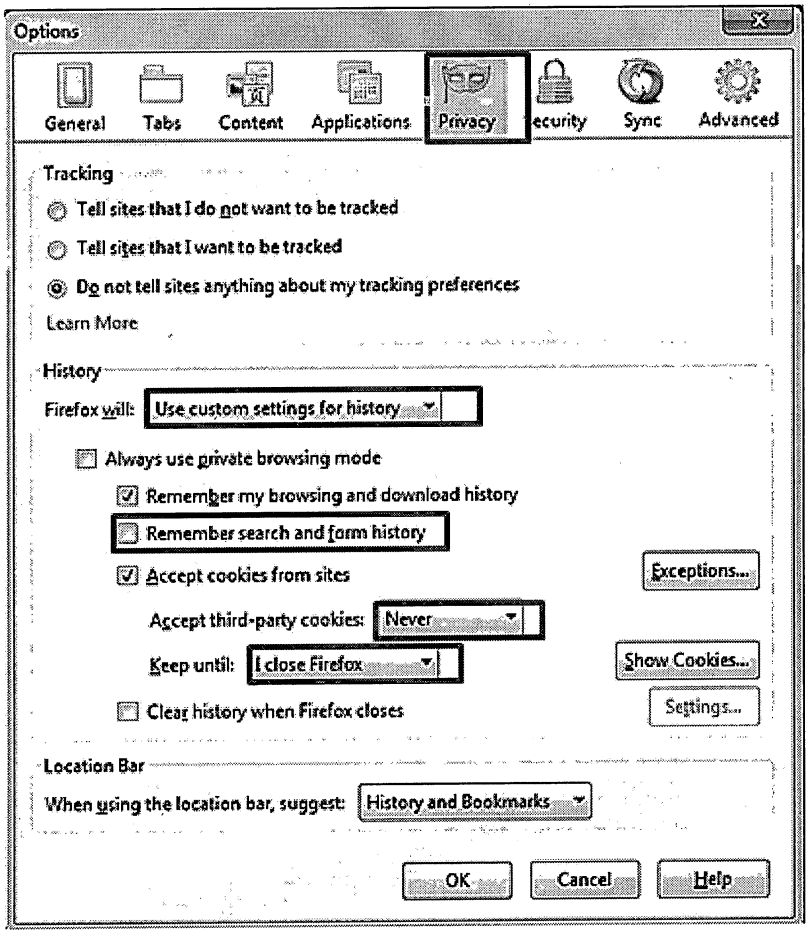
۴- در بخش content گزینه Block popup window را انتخاب نمائید:



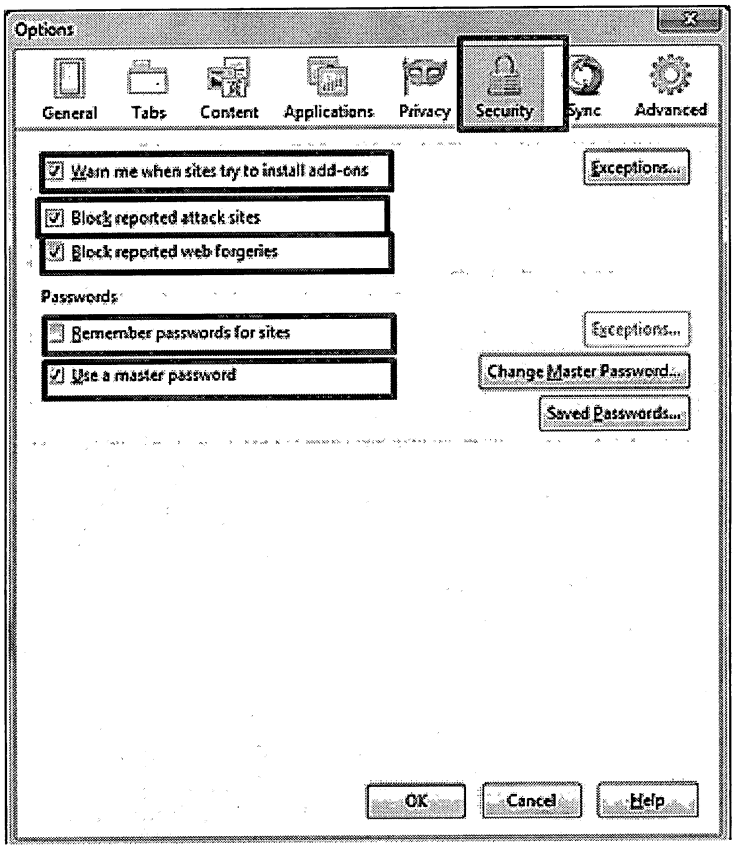
۵- در بخش Privacy گزینه Use custom settings for history را انتخاب کنید:



و سپس گزینه Remember search and form history را غیرفعال نموده، برای Accept third-party cookies گزینه Never و برای Keep until گزینه I close FireFox را انتخاب کنید:



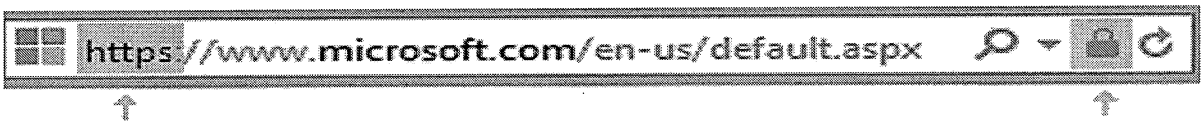
۶- در بخش Security تنظیمات زیر بایستی لحاظ شده باشند:



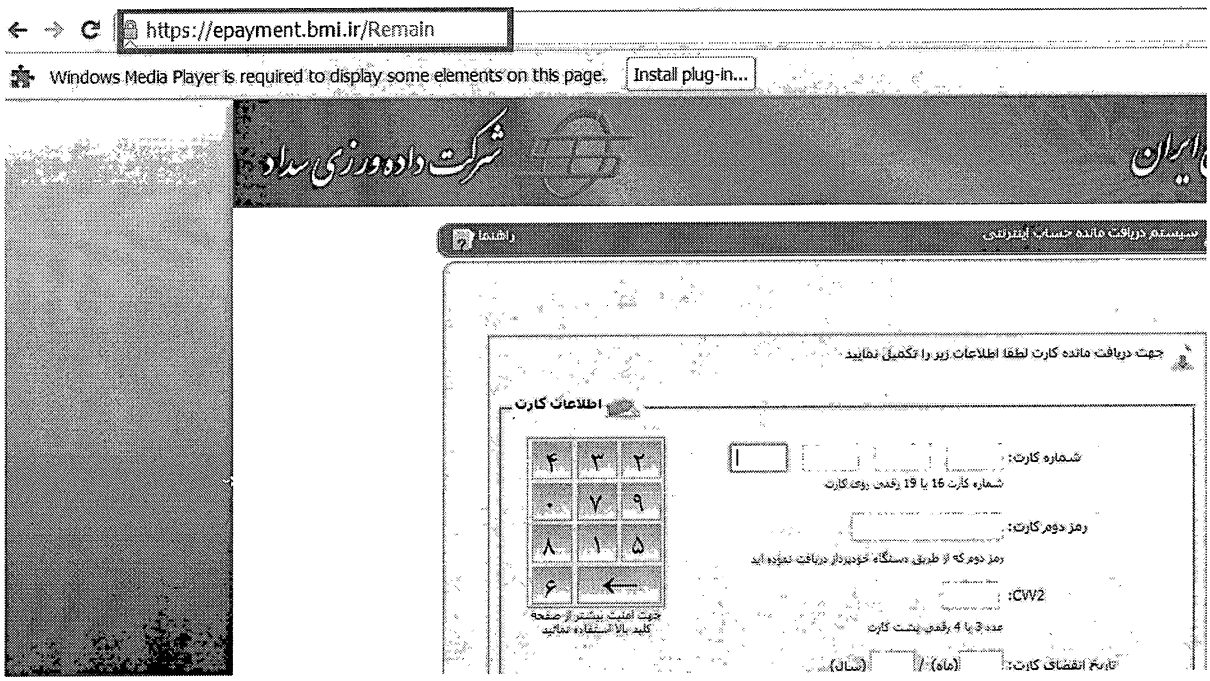
۷- در نسخه‌های قدیمی Firefox تنظیمات امنیتی دیگری نظیر غیرفعال‌سازی Java و تنظیمات مربوط به JavaScript نیز لازم است اعمال شوند. اگرچه استفاده از نسخه‌های قدیمی توصیه نمی‌شود ولی در صورت استفاده بایستی این تنظیمات توسط مسئول شبکه اعمال شوند.

بند ۵- ۸: وارد کردن اطلاعات حساس در صفحات وب

به‌منظور وارد کردن اطلاعات حساس مانند اطلاعات کارت‌های اعتباری لازم است حتما به آدرس وب‌سایتی که قصد وارد کردن اطلاعات در آن را دارید، دقت نمایید باید آدرس چنین وب‌سایت‌هایی با https شروع شود و علامت یک قفل در کنار آدرس آن‌ها قرار داشته باشد:



گاهی اوقات مهاجمان با تغییرات کوچکی در آدرس URL منجر به فریب کاربران می‌شوند. شکل زیر نشان-دهنده آدرس مربوط به بانک ملی می‌باشد که علاوه بر اینکه با علامت قفل و https آغاز شده است آدرس آن نیز صحیح می‌باشد.



بند ۵-۹: بستن پنجره‌های بالارونده

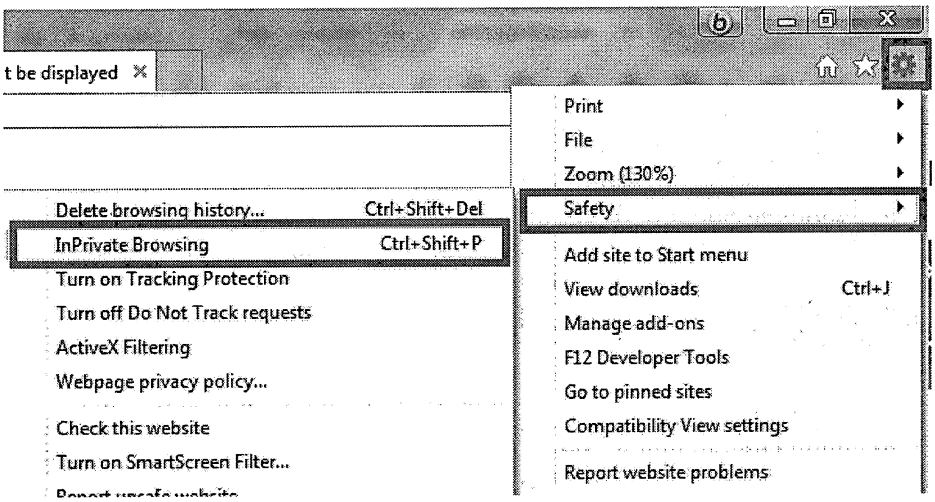
پنجره‌های بالارونده معمولا با ورود به سایت‌ها مشاهده می‌شوند، شکل‌های زیر نمونه‌ای از این پنجره‌ها را نشان می‌دهند:

برای بستن این پنجره‌ها از CTRL+F4 استفاده کنید.

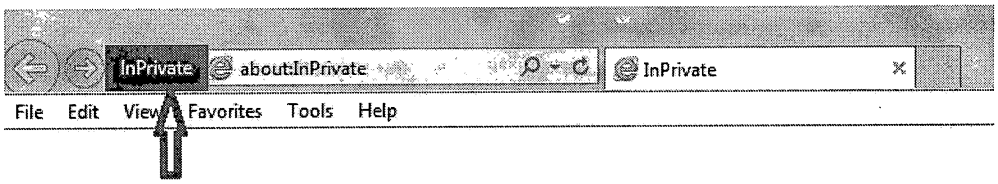
بند ۵-۱۲: استفاده از private tab

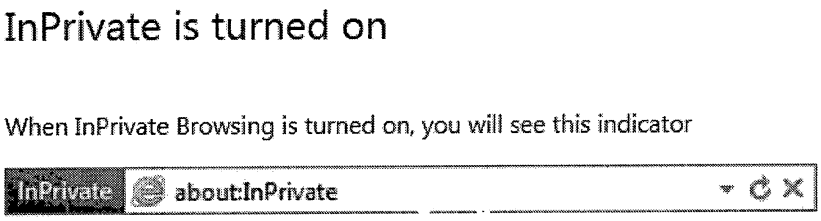
این ویژگی در IE11 قرار داده شده است که به وسیله‌ی آن می‌توان صفحات وب را بدون اینکه ردی از فعالیت-های شما بر روی وب‌سایت‌ها قرار بگیرد ملاقات کنید. این ویژگی کمک خواهد کرد تا تاریخچه‌ی مرور، فایل-های موقت اینترنت، داده‌های نوشته شده در فرم‌ها، کوکی‌ها، نام کاربری و کلمات عبور باقی نمانند. برای استفاده از این ویژگی مراحل زیر را انجام دهید:

۱- از قسمت safety، InPrivate Browsing را همانطور که در زیر نشان داده شده است انتخاب کنید:



۲- به این ترتیب تب InPrivate باید بصورت شکل زیر در کنار آدرس‌بار قرار گیرد:

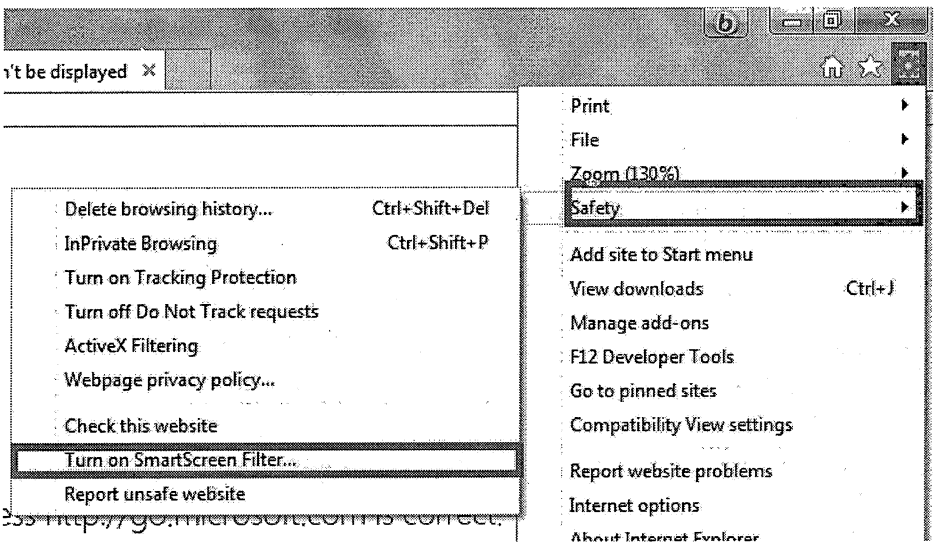




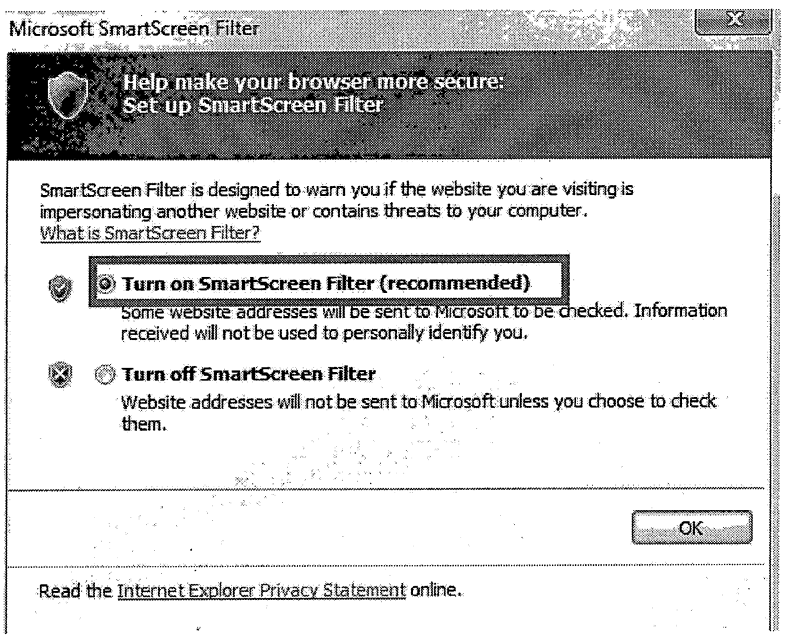
بند ۵-۱۳ : فعالسازی ویژگی SmartScreen Filter

ویژگی SmartSceern Filter که در IE وجود دارد در شناسایی وب‌سایت‌های فیشینگ به شما کمک خواهد کرد. همچنین از دانلود و نصب بدافزارها جلوگیری می‌کند. برای فعالسازی این ویژگی لازم است مراحل زیر طی شوند:

۱- از Safety، Turn on SmartScreen Filter را انتخاب کنید:

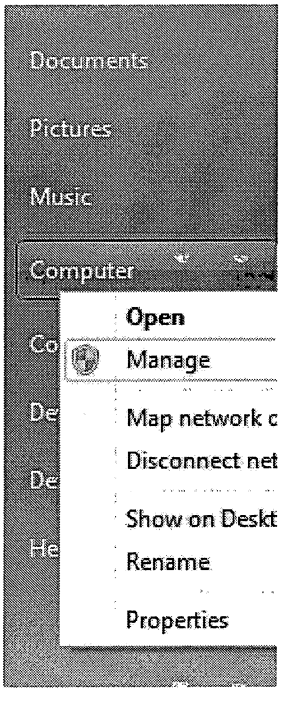


۲- در صفحه‌ی ظاهر شده گزینه‌ی Turn on SmartScreen را بصورت زیر انتخاب کنید:

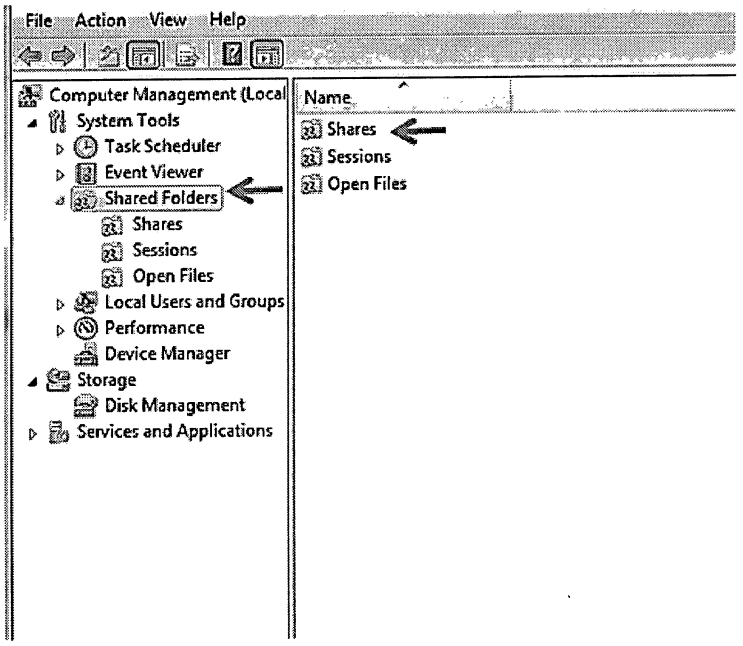


بند ۹-۱: غیرفعال کردن امکان به اشتراک‌گذاری در سیستم

۱- از منوی start بر روی Computer کلیک راست کرده و manage را انتخاب نمایید.



۲- از منوی سمت چپ Shared Folders را انتخاب کرده و shares را باز کنید.



۳- در قسمت Shares، با کلیک راست بر روی درایوها Stop sharing را انتخاب کنید.