

- سوال ۱: روش کلی غیر فعالسازی موقت و فعالسازی مجدد آنتی ویروس به چه صورتی می باشد؟ ۴
- سوال ۲: آیا می توان دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" بدون حذف مازول مربوطه بطور کامل غیر فعال نمود؟ ۸
- سوال ۳: چگونه می توان بصورت موقت دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" غیر فعال نمود و چگونه آنرا دوباره فعال کنیم؟ ۱۰
- سوال ۴: چگونه می توان مازول دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" بطور کامل و برای همیشه حذف کرد؟ ۱۳
- سوال ۵: آیا می توان فایل و یا مسیر خاصی را مشخص نمود تا آنتی ویروس آنرا اسکن نکند؟ ۱۵
- سوال ۶: چگونه می توانم از به روز بودن (Update) نرم افزار ضد ویروس خود اطمینان داشته باشم؟ ۱۷
- سوال ۷: نحوه به روز رسانی اولیه نرم افزار "NOD32" نسخه خانگی به چه ترتیبی می باشد؟ ۱۸
- سوال ۸: ضد ویروس "NOD32" را روی رایانه خود نصب کرده ام، با وجودیکه Username و Password مربوط به لایسنس را وارد می کنم اما نمی توانم آن را آپدیت کنم و با پیغام Invalid Username / Password مواجه میشوم. چگونه این مشکل را برطرف نمایم؟ ۲۲
- سوال ۹: چه تفاوتی میان نسخه های غیر معتبر (کرک) موجود در بازار و نسخه های تجاری نرم افزارهای شرکت "ESET" وجود دارد و به چه دلیل کاربران ملزم به خرید نرم افزارهای رجیستر شده می باشند؟ ۲۳
- سوال ۱۰: نرم افزار ضد ویروس و پروسی را با عنوان "MBR" شناسایی می نماید اما قادر به حذف و یا پاکسازی آن حتی در محیط "Safe Mode" نمی باشد، چه باید کرد؟ ۲۴
- سوال ۱۱: چگونه باید قابلیت "System Restore" ویندوز را غیر فعال نمود؟ ۲۶
- سوال ۱۲: نحوه اسکن کردن سیستم در محیط "Safe Mode" چگونه است و چه مزایایی دارد؟ ۲۷
- سوال ۱۳: نرم افزار ضد ویروس نصب شده روی رایانه فایلی را به عنوان ویروس شناسایی کرده و آنرا پاکسازی می نماید اما مجدداً ویروس ظاهر می گردد چه کاری باید انجام داد؟ ۳۰
- سوال ۱۴: پس از اسکن کردن سیستم و پاکسازی کامل درایو های سیستم با دابل کلیک باز نمی شوند. چگونه این مشکل را برطرف کنیم؟ ۳۱
- سوال ۱۵: FolderOptions و برخی از قسمت های ویندوز همانند Taskmanager پس از پاکسازی کامل همچنان غیر است. برای حل این مشکل چه باید کرد؟ ۳۱

- سوال ۱۶: فلش یا یکی از درایو ها را اسکن و پاکسازی کردیم ، اما کلیه اطلاعات آن حذف شد اما فضای اطلاعات حذف شده در آن درایو همچنان اشغال شده است. برای بازیابی فایل ها چه باید کرد ؟ ۳۱
- سوال ۱۷: وقتی درایو یا پوشه ای را اسکن می کنیم نرم افزار ضد ویروس آن را شناسایی نموده ولی فایل ویروسی را حذف (Delete) نمی کند چه کاری باید انجام دهیم؟ ۳۱
- سوال ۱۸: نحوه استفاده از اسکنر نرم افزارهای شرکت "ESET" جهت اسکن فایلها، پوشه ها و درایوهای رایانه چگونه است؟ ۳۲
- سوال ۱۹: نرم افزار "ESET Smart Security" مرتبا پنجره هایی با عناوین "Outbound Traffic" و "Inbound Traffic" نمایش داده می دهد، این پنجره ها چیست و چه باید کرد؟ ۳۵
- سوال ۲۰: چرا هنگام اسکن رایانه در پنجره مربوطه بعضی فایلها بصورت آبی رنگ و با پیغام "error opening" نمایش داده می شود؟ ۳۸
- سوال ۲۱: در هنگام کار با اینترنت آنتی ویروس پنجره ای با پیام "Connection terminated - quarantined" را نمایش داد، منظور از این پیام چیست؟ ۳۹
- سوال ۲۲: آنتی ویروس در هنگام یافتن فایل آلوده پیام "Cleaned by deleting - quarantined" را در پنجره خود نمایش می دهد این پیام به چه معنی می باشد؟ ۴۰
- سوال ۲۳: چگونه می توان بر روی تنظیمات آنتی ویروس کلمه رمزی قرار داد تا سایرین نتوانند تنظیمات آنتی ویروس را تغییر دهند و یا آن را خاموش کنند؟ ۴۰
- سوال ۲۴: کلمه رمزی برای آنتی ویروس ESET تنظیم کرده بودیم. اما حال آن را فراموش کرده ایم . چگونه می توان این رمز را غیر فعال کرد ؟ ۴۰
- سوال ۲۴: چرا آنتی ویروس برنامه هایی همانند Ultra را ویروس شناسائی می کند درحالی که این برنامه ابزاری برای مخفی کردن IP و گذر از فایروال هاست ؟ ۴۱
- سوال ۲۵: اعتبار لایسنس آنتی ویروس من به پایان رسیده است و خطای Username / Password نمایش داده می شود. برای تمدید لایسنس خود باید چه اقدامی انجام دهم و هزینه این تمدید چقدر است؟ ۴۲
- سوال ۲۶: نرم افزار حسابداری شرکت ما هلو (طرفه نگار) می باشد. اما در هنگام نصب و استفاده ، آنتی ویروس فایل Holo.exe را حذف کرده و اجازه نصب و استفاده از نرم افزار هلو را نمی دهد؟ ۴۲
- سوال ۲۷: خرید لایسنس های ESET از شرکت های غیرمعتبر چه پیامد هایی را به دنبال خواهد داشت ؟ ۴۳
- سوال ۲۸: مدتی است که پس از بالا آمدن ویندوز، سیستم محافظتی آنتی ویروس ESET غیر فعال است و نماد آن به رنگ قرمز است. لذا هر بار باید به صورت دستی با زدن گزینه Start all Antivirus and antispyware protection آنتی ویروس را فعال کنم ؟ ۴۴
- سوال ۲۹: سیستم من به آلوده به ویروس است و نصب آنتی ویروس روی سیستم با مشکلات مختلفی روبرو میشود. چه راهکاری را پیشنهاد میکنید ؟ ۴۴
- سوال ۳۰: ویندوز من آلوده است و آنتی ویروس روی آن نصب نمی شود. از طرفی هم برنامه های کاربردی مهمی روی آن نصب است و تعویض ویندوز مشکلات زیادی را به دنبال خواهد داشت ؟ ۴۴
- سوال ۳۱: نگارش آنتی ویروس ESET من قدیمی است حال نگارش جدید آنتی ویروس خود را تهیه کرده ام . چگونه آن را نصب کنم ؟ ۴۵

- سوال ۳۲: آنتی ویروس من به محض مشاهده یک فایل ویروسی آن را حذف می کند. چه تنظیماتی را اعمال کنم که برای حذف از من کسب اجازه شود؟ ۴۵
- سوال ۳۳: چگونه آنتی ویروس را تنظیم کنم که حتی با زدن فرمان **Clean files** در منوی کلیک راست هم پس از اجازه کاربر فایل های ویروسی را حذف کند؟ ۴۶
- سوال ۳۴: ویندوز سیستم را تعویض کرده ام و در هنگام نصب آنتی ویروس کد فعال سازی قبلی تأیید نمی شود و برای کد فعال سازی جدید هم پیغام "حق ثبت این سریال به پایان رسیده است" نمایش داده میشود؟ ۴۷
- سوال ۳۵: می خواهم آنتی ویروس را بر روی سیستمی نصب کنم اما پیغام "حق ثبت این سریال به پایان رسیده است" نمایش داده میشود علت چیست؟ ۴۸
- سوال ۳۶: آیا بین چهار روش فعال سازی و عملکرد آنتی ویروس رابطه ای وجود دارد و کدام روش فعال سازی از همه بهتر است؟ ... ۴۸

سوال ۱: روش کلی غیر فعالسازی موقت و فعالسازی مجدد آنتی ویروس به چه صورتی می باشد؟

به منظور غیر فعالسازی و فعالسازی مجدد گاردهای نرم افزار ضد ویروس مراحل زیر را دنبال نمایید:

توجه: این غیر فعالسازی تا راه اندازی مجدد (Restart) رایانه پا بر جا خواهد بود و در صورت راه اندازی مجدد گاردها بصورت خودکار فعال خواهند گردید.

**روش اول: غیر فعال سازی و فعال سازی مجدد آنتی ویروس در حالت Standard mod:

اگر آنتی ویروس شما در حالت استاندارد است (در پنجره اصلی آنتی ویروس در گوشه پایین سمت چپ عبارت Display : Standard mode درج شده است) برای خاموش کردن موقت آنتی ویروس کافیست بر روی آیکن آنتی ویروس در نوار وظیفه کلیک کرده (تصویر شماره ۱) و سپس از سمت چپ بخش Setup را انتخاب نموده و بعد از پنل سمت راست گزینه Temporarily disable Antivirus and antispyware protection را کلیک نمائید. سپس پیغامی ظاهر می شود که باید دکمه Yes آن را بزنید. با این کار آنتی ویروس موقتا غیر فعال میشود. برای فعال کردن مجددا آن در حالت Standard کافیست از همان بخش Setup گزینه Enable Antivirus and antispyware protection را کلیک نمائید تا آنتی ویروس مجددا به وضعیت فعال خود بازگردد.

**روش اول: غیر فعال سازی آنتی ویروس در حالت Advanced mod:

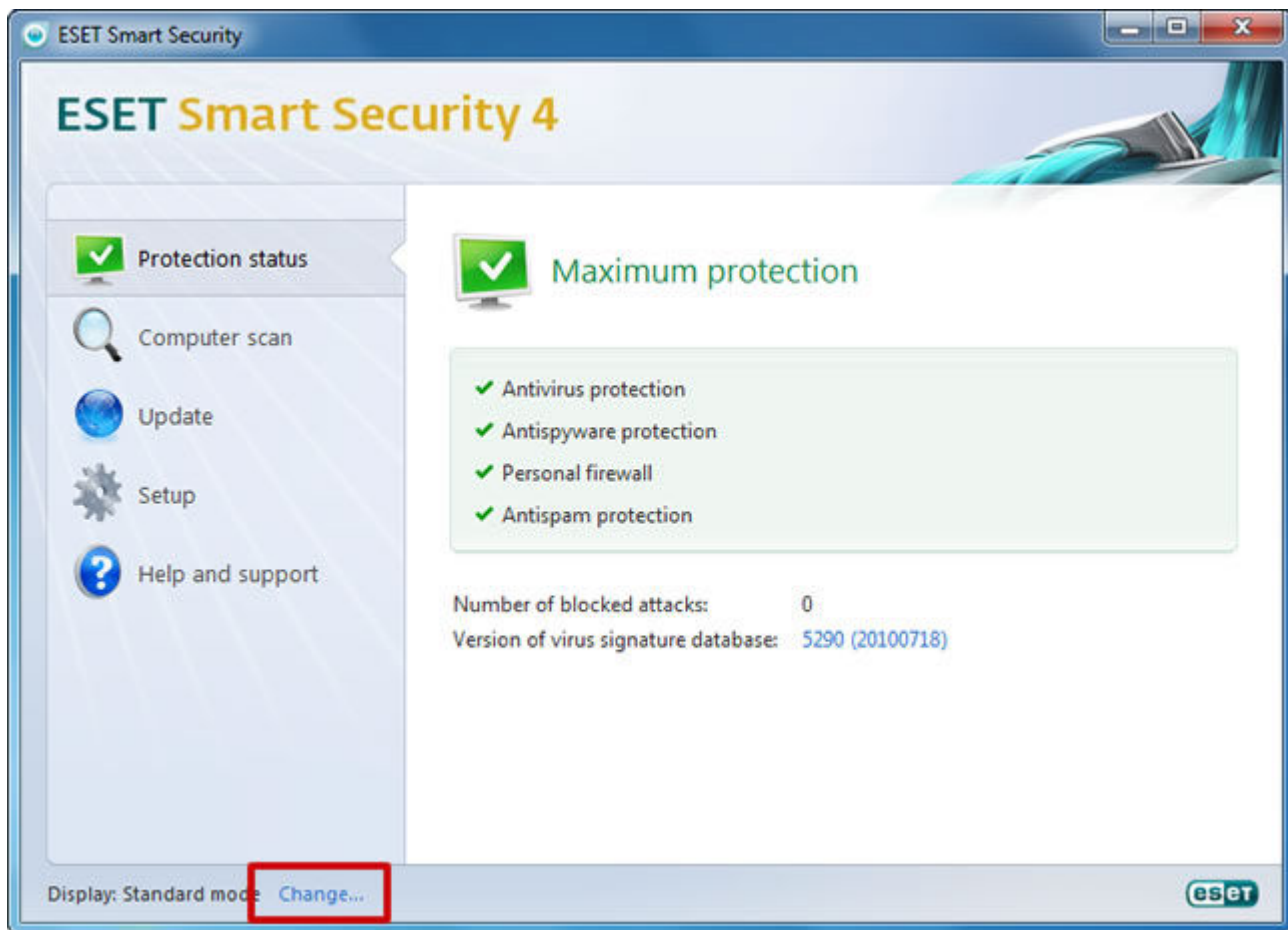
** تغییر به حالت "Advanced mode"

۱- ابتدا اطمینان حاصل نمایید که نرم افزار "ESET Smart Security" و یا "ESET NOD32" در حالت "Advanced mode" قرار گرفته باشد. بدین منظور نرم افزار ضد ویروس را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



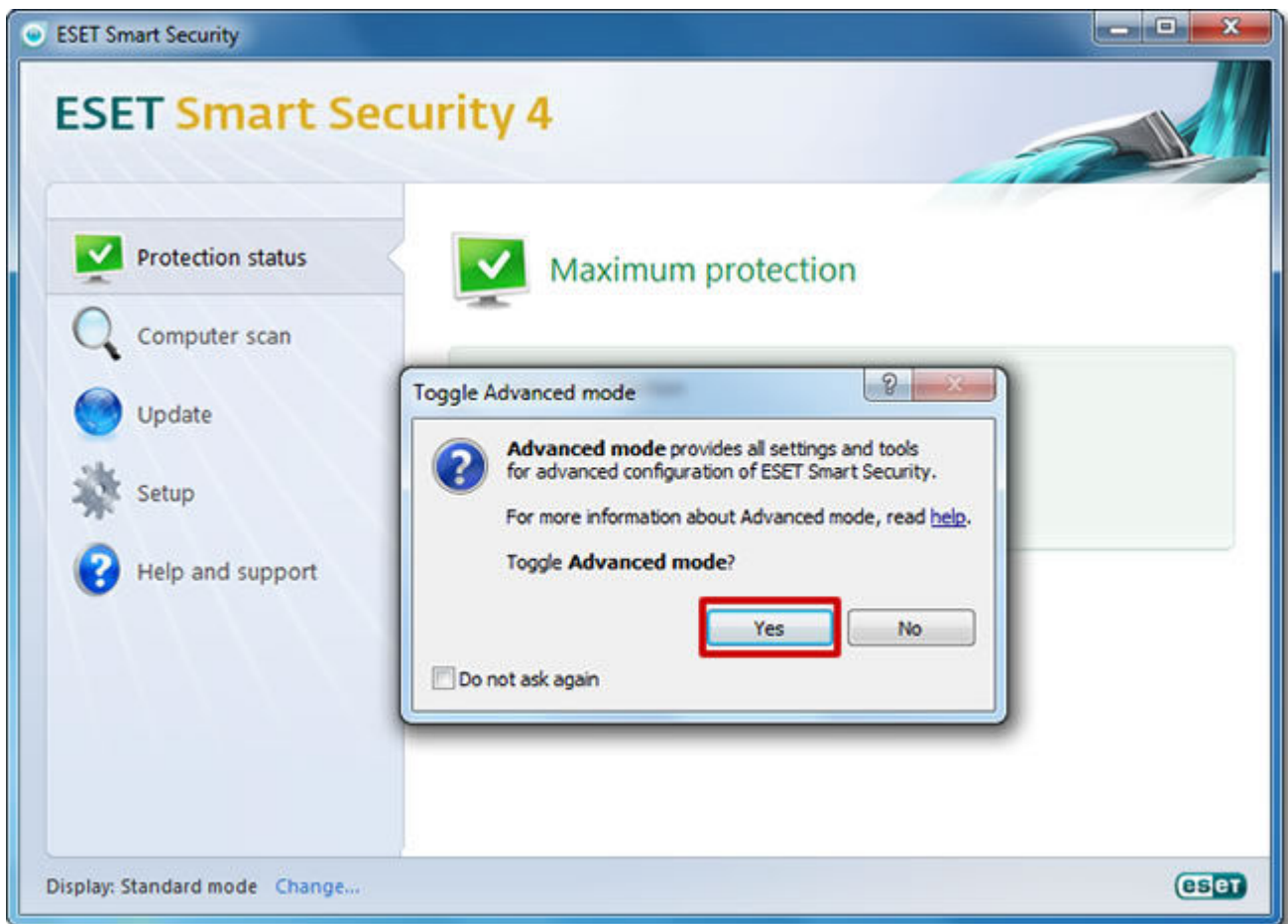
تصویر شماره ۱

۲- دقت کنید اگر در صفحه اصلی نرم افزار منتهی الیه سمت چپ و پایین در مقابل برچسب "Display" مقدار "Standard mode" درج شده بود گزینه "Change" را جهت تغییر حالت از "Standard mode" به "Advanced mode" (مطابق تصویر شماره ۲) کلیک نمایید.



(تصویر شماره ۲)

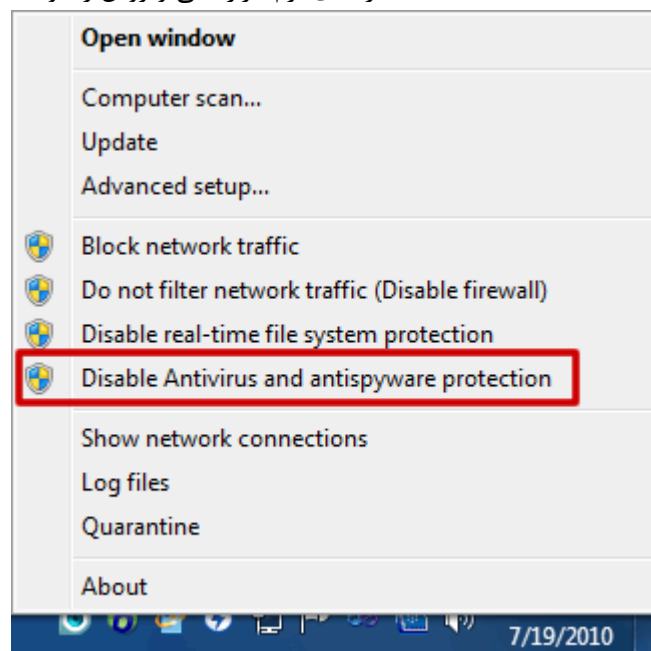
با انجام مرحله فوق پنجره تاییدی (مطابق تصویر شماره ۳) باز نمایش داده خواهد شد. در این حالت گزینه "Yes" را انتخاب کنید و سپس پنجره اصلی نرم افزار را ببندید .



(تصویر شماره ۳)

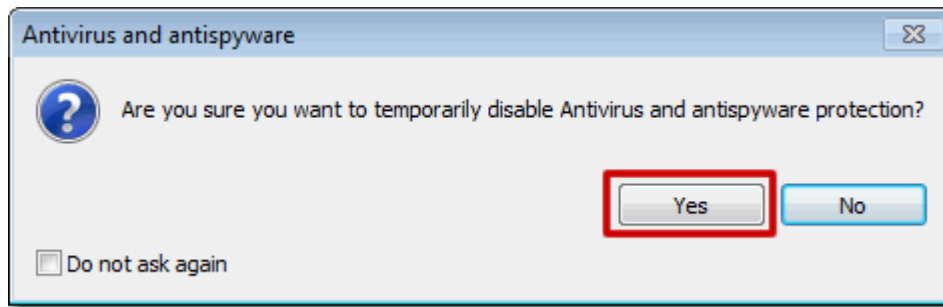
***** غیر فعالسازی موقت آنتی ویروس در حالت Advanced mode**

۱- روی آیکن نرم افزار در نوار وظیفه ویندوز کلیک راست نموده و در منوی باز شده (مطابق تصویر شماره ۴) می توانید با انتخاب گزینه "Disable Antivirus and antispyware protection" گاردهای نرم افزار آنتی ویروس را موقتا غیرفعال کنید.



(تصویر شماره ۴)

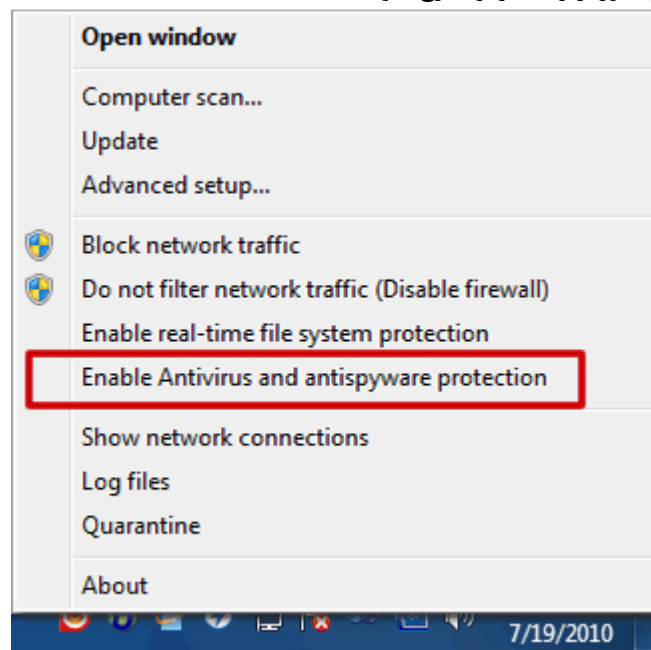
۲- در این مرحله (مطابق تصویر شماره ۵) در پنجره تایید باز شده گزینه را انتخاب کنید تا عملیات غیر فعالسازی خاتمه یابد. پس از انجام این مراحل آیکن نرم افزار در نوار وظیفه ویندوز به رنگ قرمز تغییر خواهد نمود.



(تصویر شماره ۵)

*** فعالسازی مجدد آنتی ویروس در حالت Advanced mode

۱- روی آیکن نرم افزار در نوار وظیفه ویندوز کلیک راست نموده و در منوی باز شده (مطابق تصویر شماره ۶) می توانید با انتخاب گزینه "Enable Antivirus and Antispyware protection" گاردهای نرم افزار ضد ویروس را مجدداً فعال کنید. پس از انجام این مراحل آیکن نرم افزار در نوار وظیفه ویندوز از رنگ قرمز خارج خواهد شد.



(تصویر شماره ۶)

سوال ۲: آیا می توان دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" بدون حذف ماژول مربوطه بطور کامل غیر فعال نمود؟

به منظور غیر فعالسازی و فعالسازی مجدد ماژول دیواره آتش (Firewall) نرم افزار "ESET Smart Security" مراحل زیر را دنبال نمایید:

توجه: این غیر فعالسازی بدلیل عدم حذف ماژول دیواره آتش در هر زمانی قابل فعالسازی مجدد توسط کاربر می باشد و بر خلاف غیر فعالسازی بصورت موقت، در صورت راه اندازی مجدد ماژول مذکور بصورت خودکار فعال نخواهد شد.

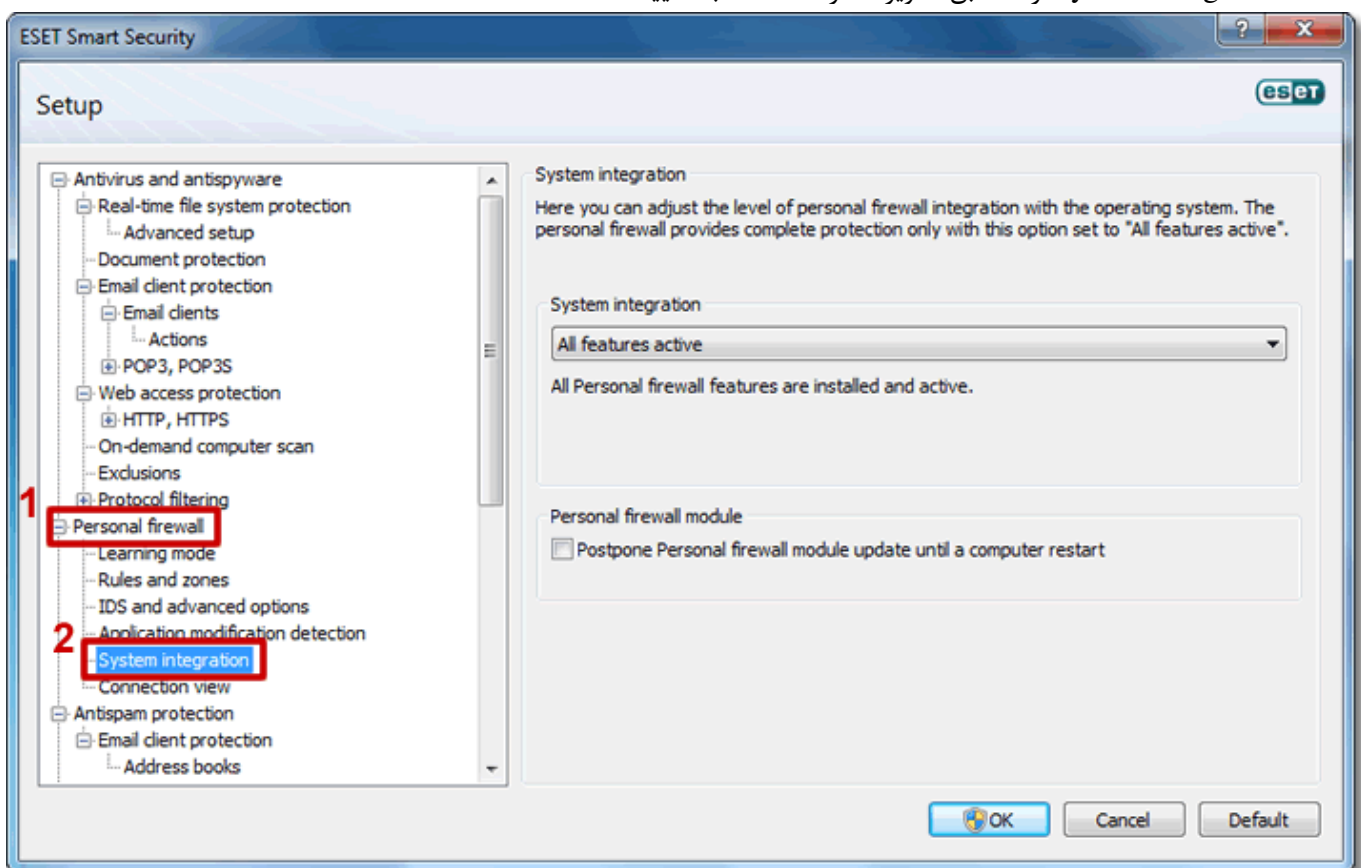
** غیر فعالسازی دیواره آتش

۱- نرم افزار "ESET Smart Security" را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



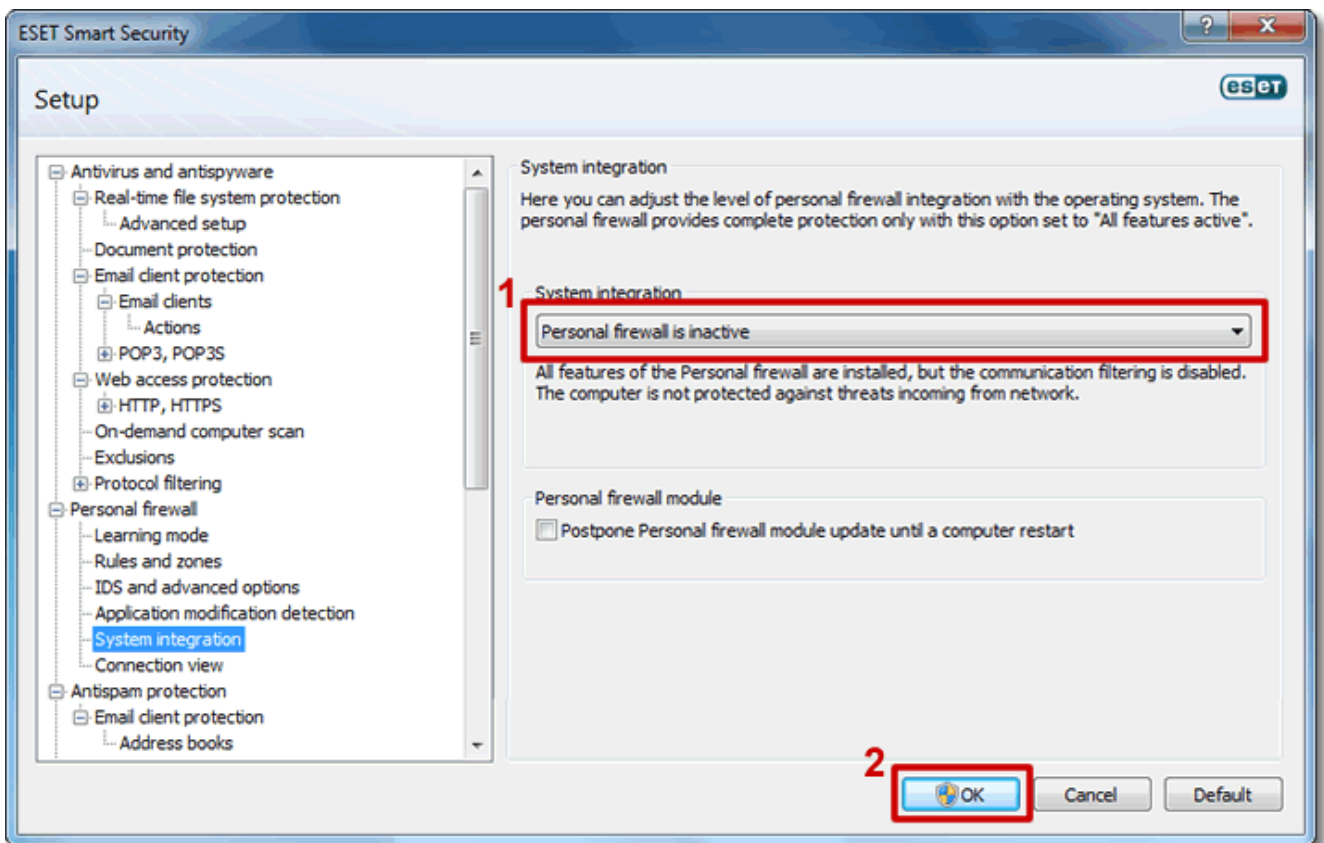
(تصویر شماره ۱)

۲- با فشردن دکمه "F5" از روی صفحه کلید وارد صفحه تنظیمات نرم افزار شوید. در پانل سمت از شاخه "Personal Firewall" زیر شاخه "System integration" را (مطابق تصویر شماره ۲) انتخاب نمایید.



(تصویر شماره ۲)

۳- در قسمت سمت راست پنجره "System integration" از فهرست باز شدنی موجود (مطابق تصویر شماره ۳) گزینه "Personal is inactive" را انتخاب کنید و در نهایت دکمه "OK" را کلیک نمایید و سپس سیستم را Restart نمایید.



(تصویر شماره ۳)

** فعالسازی مجدد دیواره آتش

برای فعال سازی مجدد دیوار آتش آنتی ویروس منوی فوق را بر روی گزینه All Futures Active قرار دهید و سیستم را Restart نمایید.

سوال ۳: چگونه می توان بصورت موقت دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" غیر فعال نمود و چگونه آنرا دوباره فعال کنیم؟

به منظور غیر فعالسازی و فعالسازی مجدد مازول دیواره آتش (Firewall) نرم افزار "ESET Smart Security" مراحل زیر را دنبال نمایید:

توجه: این غیر فعالسازی تا راه اندازی مجدد (Restart) رایانه پا بر جا خواهد بود و در صورت راه اندازی مجدد مازول دیواره آتش (Firewall) بصورت خودکار فعال خواهد گردید.

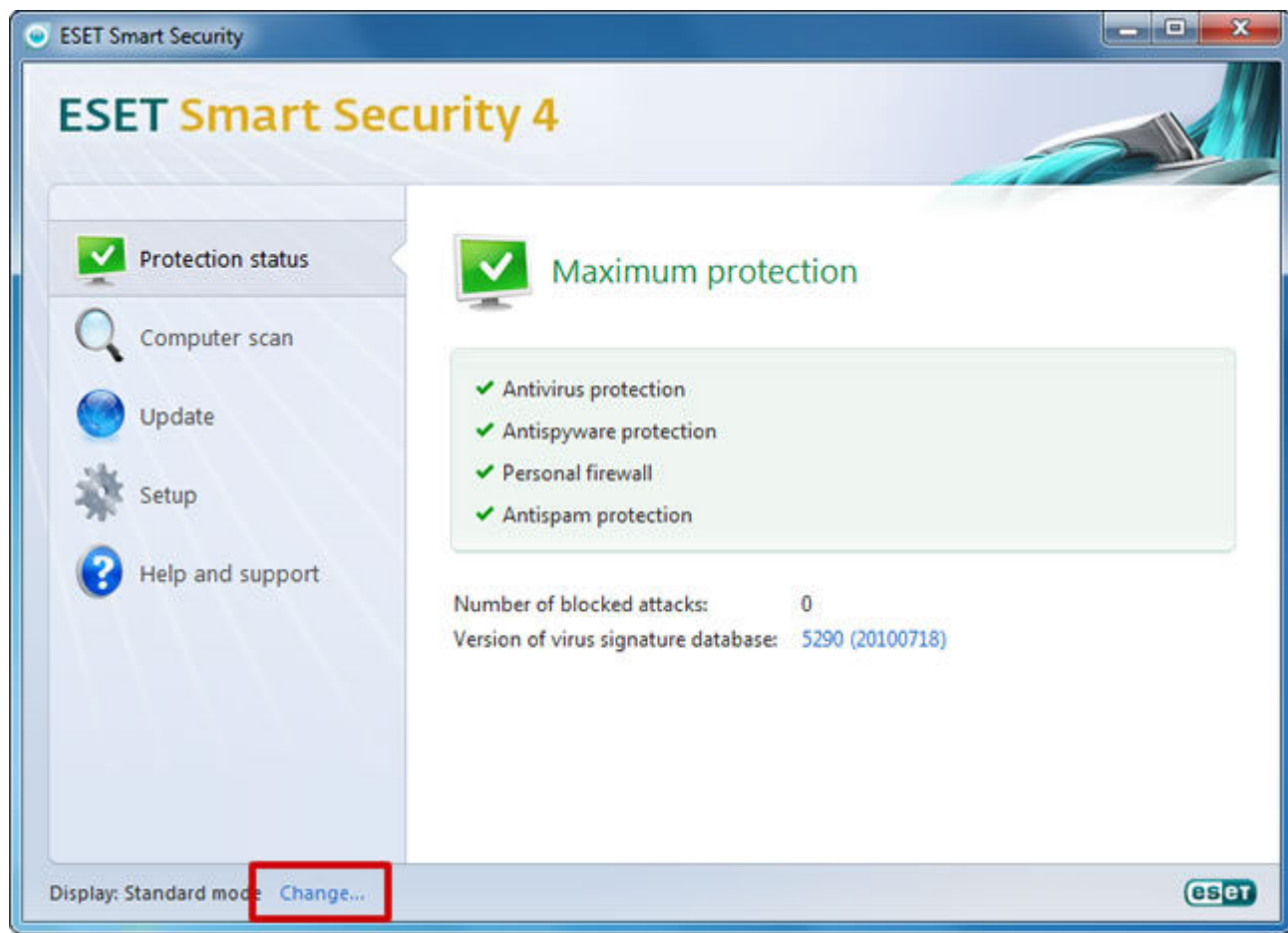
:: تغییر به حالت "Advanced mode"

۱- ابتدا اطمینان حاصل نمایید که نرم افزار "ESET Smart Security" در حالت "Advanced mode" قرار گرفته باشد. بدین منظور نرم افزار "ESET Smart Security" را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



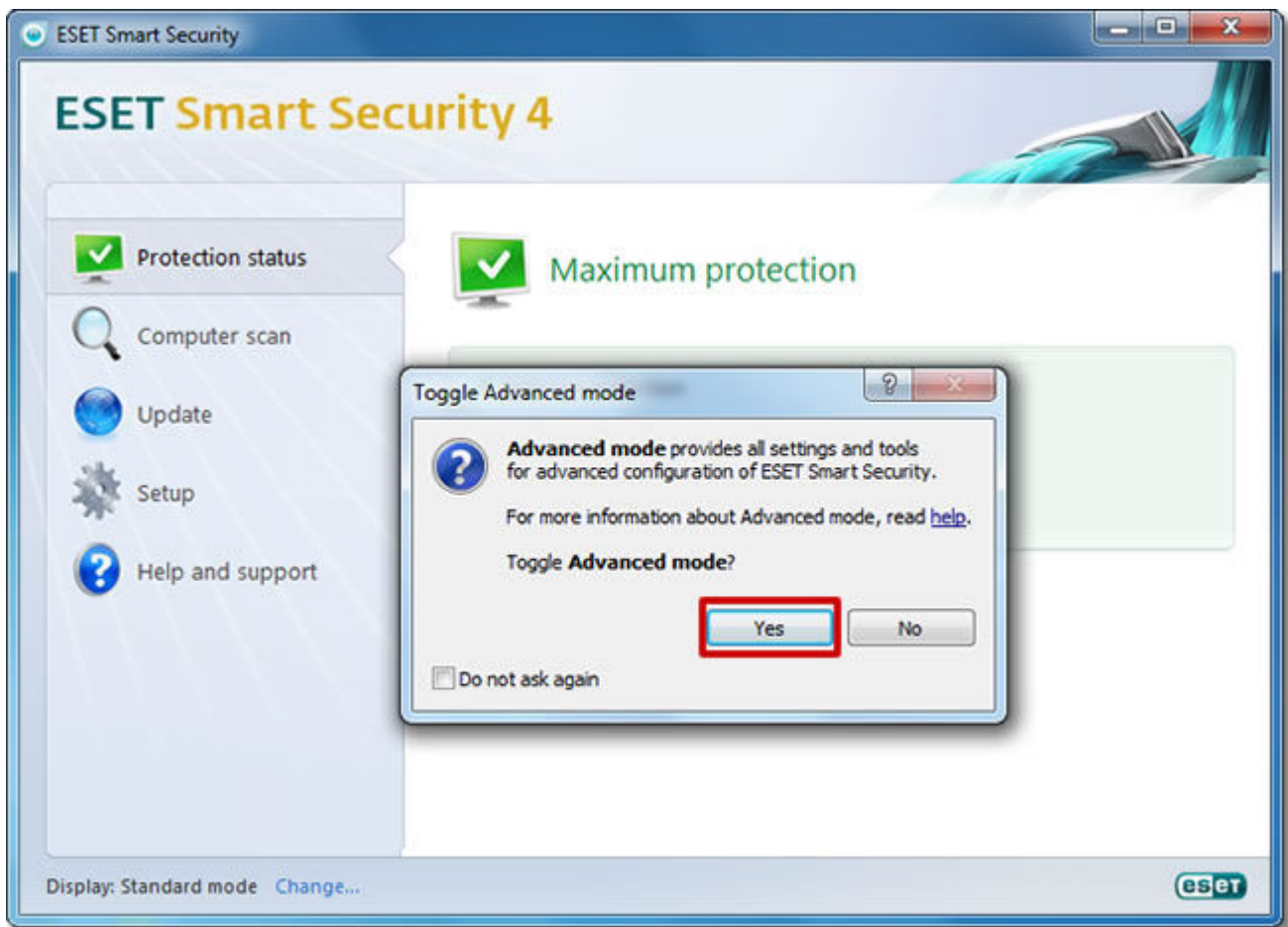
(تصویر شماره ۱)

۲- دقت کنید اگر در صفحه اصلی نرم افزار منتهی الیه سمت چپ و پایین در مقابل برچسب "Display" مقدار "Standard mode" درج شده بود گزینه "Change" را جهت تغییر حالت از "Standard mode" به "Advanced mode" (مطابق تصویر شماره ۲) کلیک نمایید.



(تصویر شماره ۲)

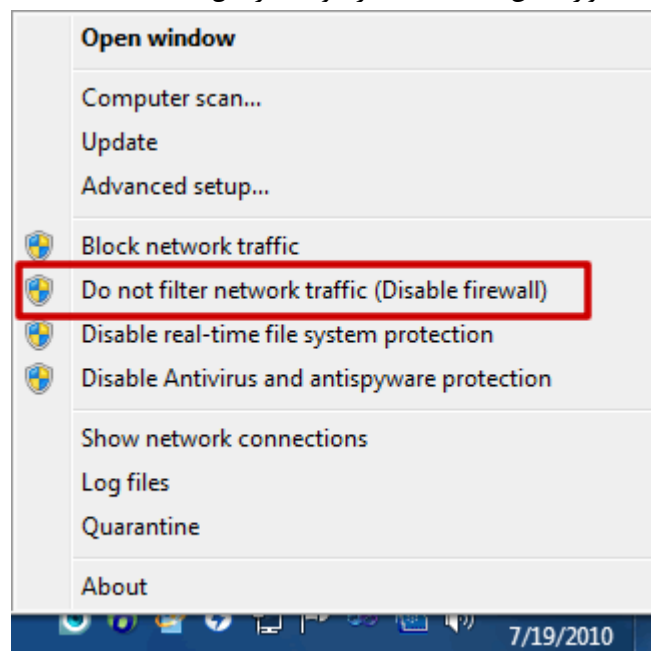
با انجام مرحله فوق پنجره تاییدی (مطابق تصویر شماره ۳) باز نمایش داده خواهد شد. در این حالت گزینه "Yes" را انتخاب کنید و سپس پنجره اصلی نرم افزار را ببندید .



(تصویر شماره ۳)

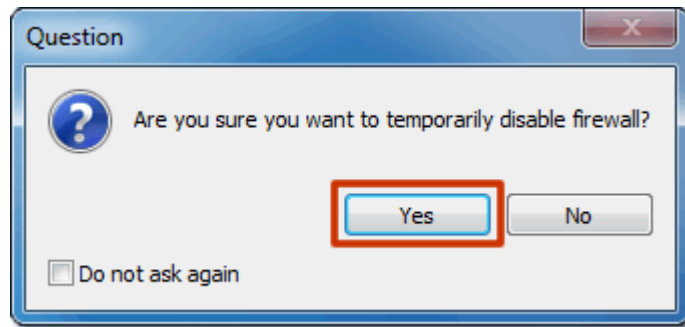
*** غیر فعالسازی موقت دیواره آتش

۱- روی آیکن نرم افزار در نوار وظیفه ویندوز کلیک راست نموده و در منوی باز شده (مطابق تصویر شماره ۴) می توانید با انتخاب گزینه "Do not filter network traffic" دیواره آتش (Firewall) را موقتا غیرفعال کنید.



(تصویر شماره ۴)

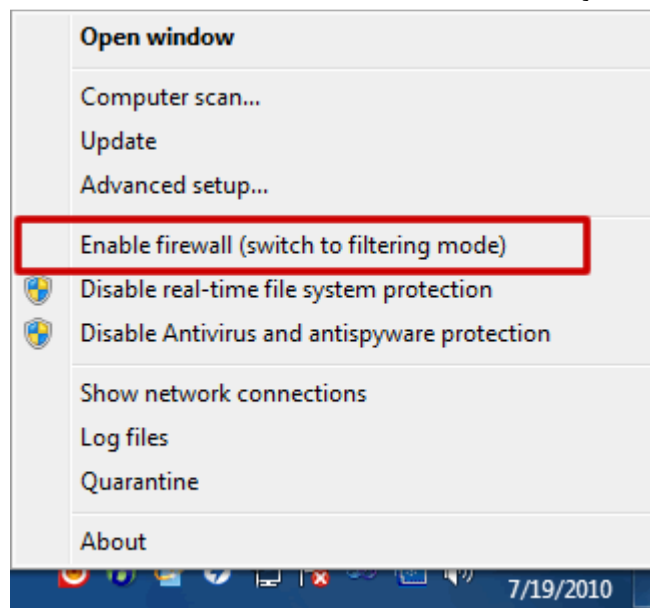
۲- در این مرحله (مطابق تصویر شماره ۵) در پنجره تایید باز شده گزینه را انتخاب کنید تا عملیات غیر فعالسازی خاتمه یابد. پس از انجام این مراحل آیکن نرم افزار در نوار وظیفه ویندوز به رنگ قرمز تغییر خواهد نمود.



(تصویر شماره ۵)

*** فعالسازی مجدد دیواره آتش

۱- روی آیکن نرم افزار در نوار وظیفه ویندوز کلیک راست نموده و در منوی باز شده (مطابق تصویر شماره ۶) می توانید با انتخاب گزینه "Enable firewall" دیواره آتش (Firewall) را مجدداً فعال کنید. پس از انجام این مراحل آیکن نرم افزار در نوار وظیفه ویندوز از رنگ قرمز به رنگ آبی فیروزه ای تغییر خواهد نمود.



(تصویر شماره ۶)

سوال ۴: چگونه می توان ماژول دیواره آتش (Firewall) را در نسخه های "ESET Smart Security" بطور کامل و برای همیشه حذف کرد؟

یکی از قابلیت‌های موجود در نرم افزار "ESET Smart Security" وجود ماژول دیواره آتش یا اصطلاحاً "Firewall" می باشد که کلیه داده های ارسالی و دریافتی نرم افزارهای مختلف و پورتهای مورد استفاده آنها را رصد نموده و در صورت هر گونه استفاده غیر مجاز از رایانه کاربر ارتباط موردنظر را بلوکه می نماید. در بعضی مواقع کاربران نرم افزار "ESET Smart Security" ممکن است بخواهند آنرا برای همیشه حذف نمایند .

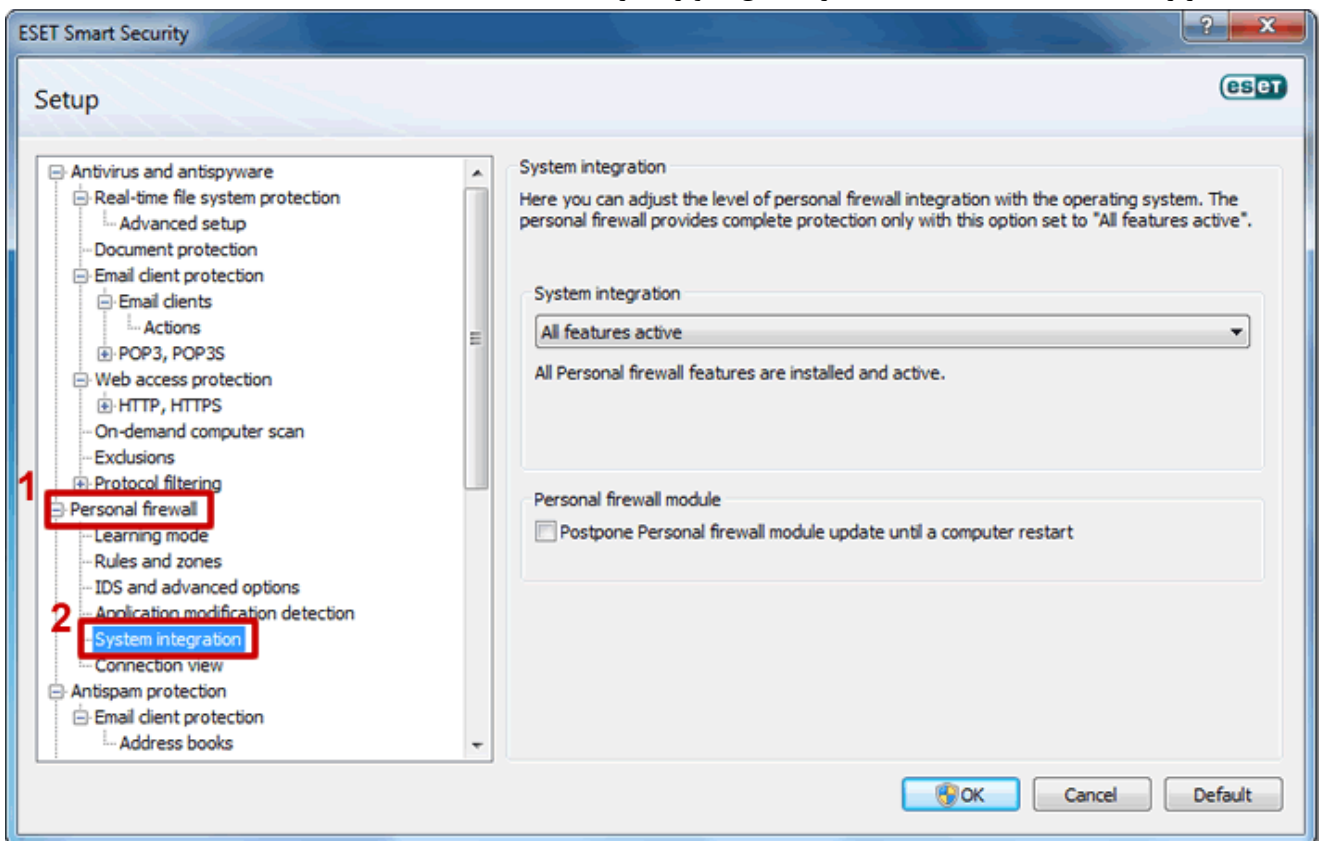
توجه :در صورت حذف این ماژول دیگر نمی توان آنرا دوباره بازگرداند مگر اینکه نرم افزار "ESET Smart Security" را مجدداً نصب کنید.

۱- نرم افزار "ESET Smart Security" را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



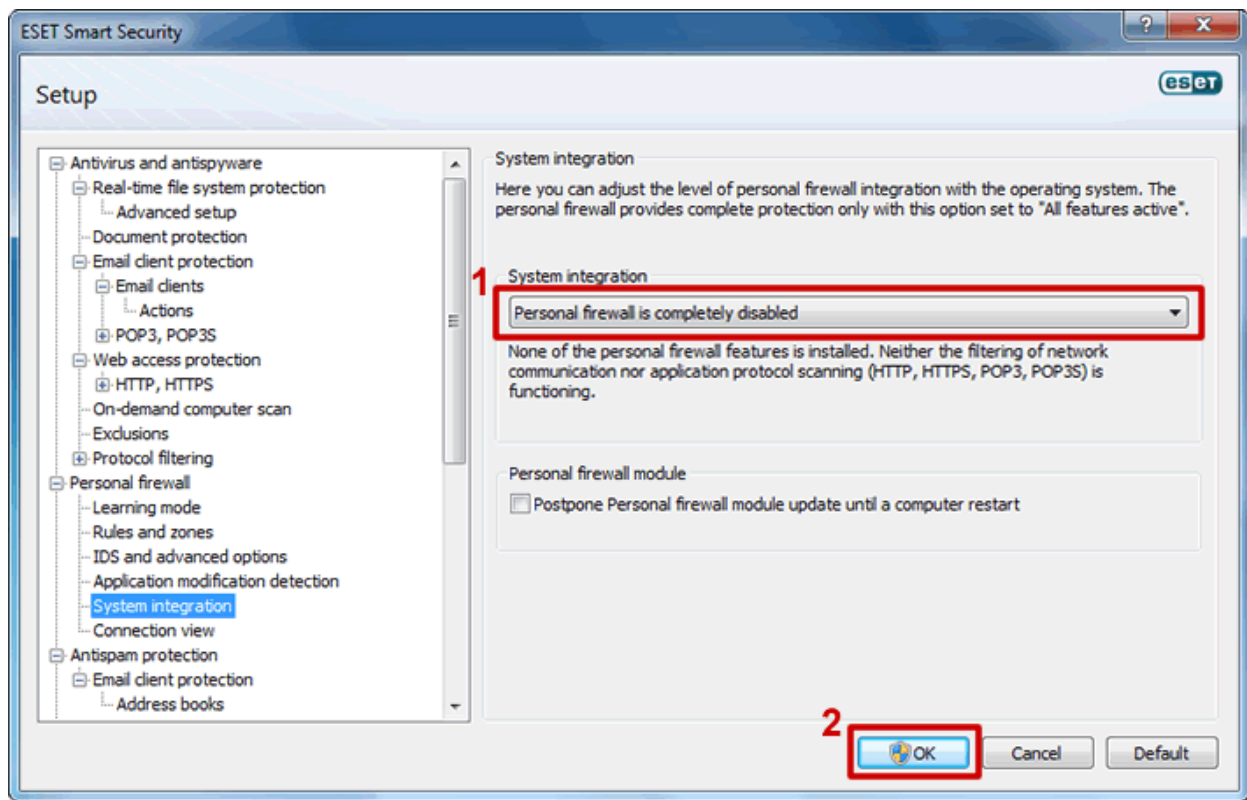
(تصویر شماره ۱)

۲- با فشردن دکمه "F5" از روی صفحه کلید وارد صفحه تنظیمات نرم افزار شوید. در پانل سمت چپ از شاخه "Personal Firewall" زیر شاخه "System integration" را (مطابق تصویر شماره ۲) انتخاب نمایید .



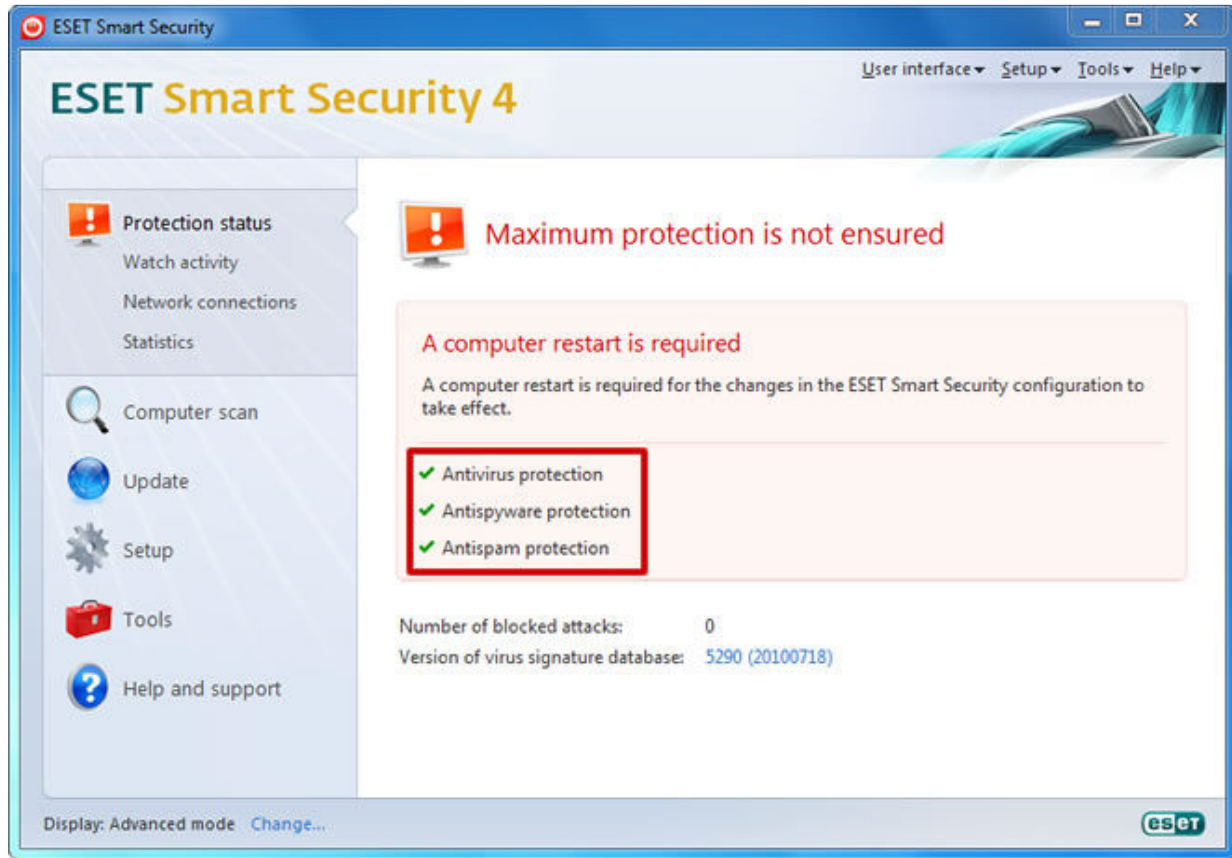
(تصویر شماره ۲)

۳- در قسمت سمت راست پنجره "System integration" از فهرست باز شدنی موجود (مطابق تصویر شماره ۳) گزینه "Personal Firewall is completely disabled" را انتخاب کنید و در نهایت دکمه "OK" را کلیک نمایید .



(تصویر شماره ۳)

۴- پس از انجام مراحل فوق پنجره "Setup" بسته شده و نرم افزار شما را به صفحه اصلی و منوی "Protection status" هدایت می نماید. در این صفحه (مطابق تصویر شماره ۴) در قسمت سمت راست ماژول "Personal Firewall" از فهرست ماژولها حذف شده است. در خاتمه به منظور اعمال تغییرات فوق می بایست یک بار رایانه خود را "Restart" نمایید.



(تصویر شماره ۴)

سوال ۵: آیا می توان فایل و یا مسیر خاصی را مشخص نمود تا آنتی ویروس آنرا اسکن نکند؟

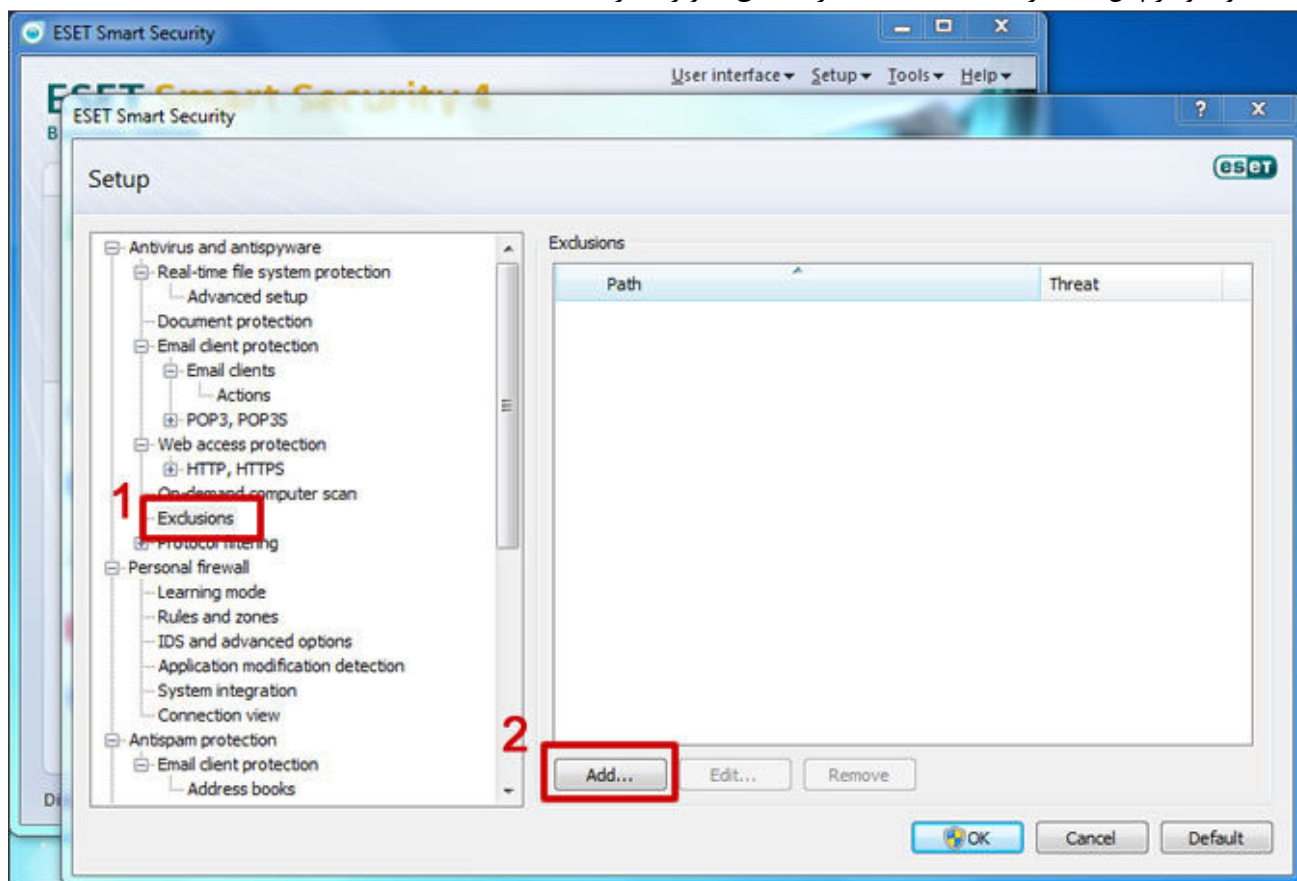
مشخص نمودن یک فایل و یا یک مسیر خاص به منظور عدم بررسی آن توسط نرم افزارهای ضد ویروس، یکی از بخشهای مهم هر نرم افزار ضد ویروس می باشد که اصطلاحاً به آن (Exclusions) گفته می شود. لازم به ذکر است معمولاً فایل‌های کرک نرم افزارها و یا فایل‌های اجرایی نرم افزارهای ایرانی بدلیل عدم استاندارد سازی مناسب ممکن است سبب شود نرم افزارهای ضد ویروس آنها را به عنوان بدافزار (Malware) شناسایی نموده و اقدام به حذف و یا بلوکه نمودن آن نمایند. نرم افزارهای شرکت "ESET" نیز دارای این قابلیت بوده و کاربران می توانند در صورت نیاز به روش زیر از آن استفاده کنند. این روش برای معرفی فایل نرم افزارهایی همانند حسابداری هلو نیز استفاده می شود.

۱- نرم افزار امنیتی شرکت "ESET" را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



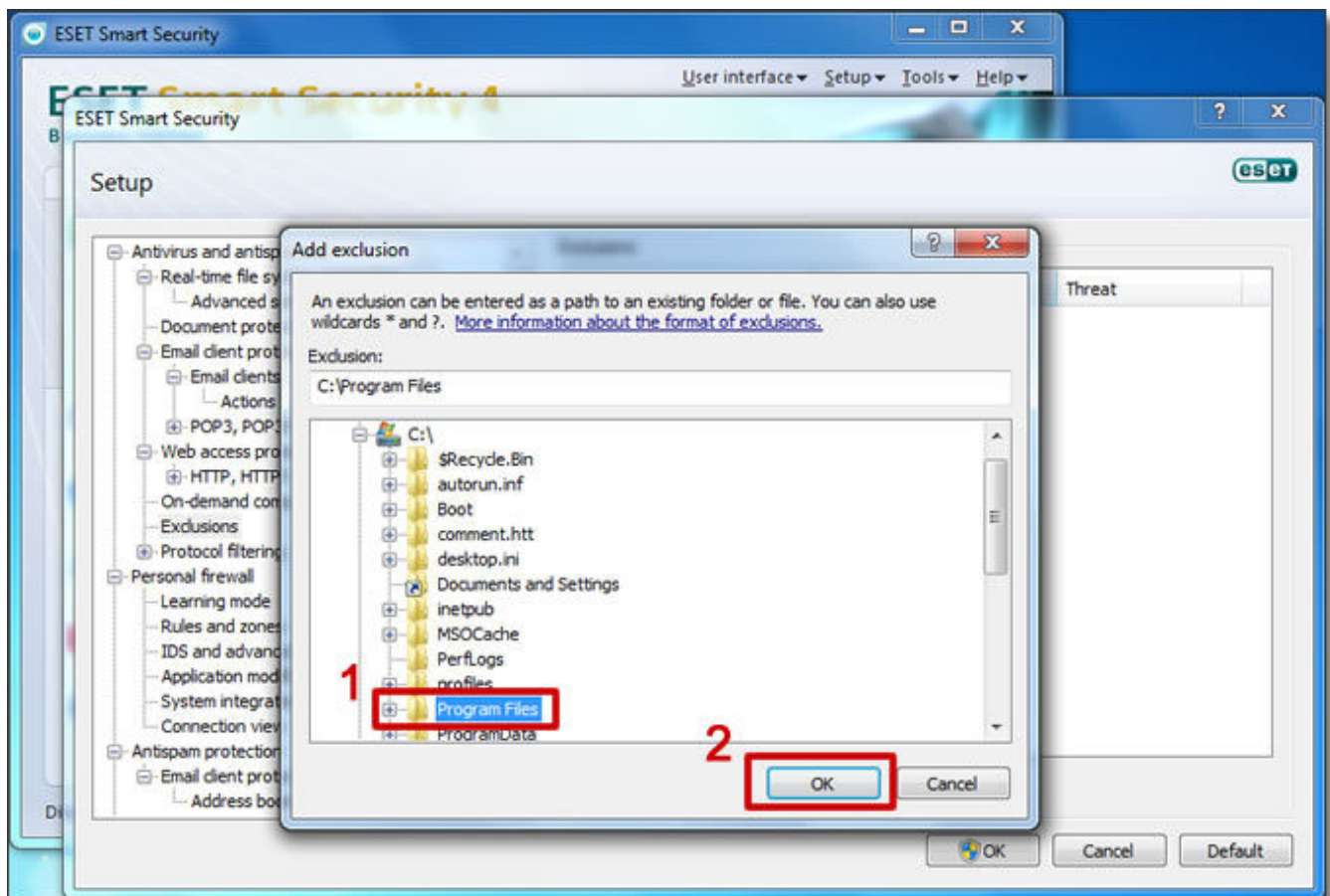
(تصویر شماره ۱)

۲- با فشردن دکمه "F5" از روی صفحه کلید وارد صفحه تنظیمات نرم افزار شوید. در پانل سمت چپ سر شاخه "Exclusions" را انتخاب نموده و در پانل سمت راست دکمه "Add" را (مطابق تصویر شماره ۲) کلیک نمایید.



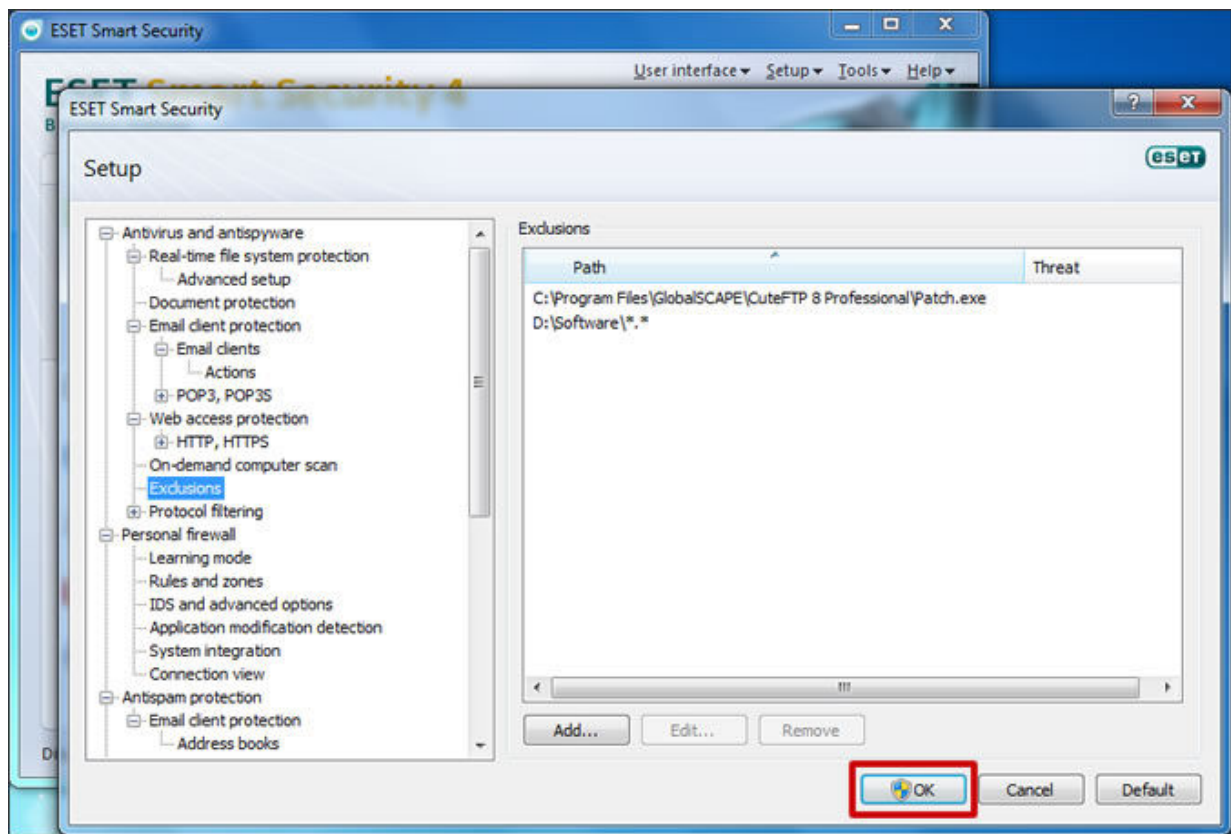
(تصویر شماره ۲)

۳- پس از مراحل فوق پنجره انتخاب (مطابق تصویر شماره ۳) باز شده و کاربر می تواند فایل، پوشه، و درایو موردنظر خود را انتخاب کرده و با کلیک گزینه "OK" آنرا به فهرست "Exclusions" اضافه نماید. لازم به ذکر است کاربر می تواند از کاراکترهای "?" و "*" به منظور عملیات فیلترینگ فایلها نیز استفاده کند.



(تصویر شماره ۳)

۴- مرحله شماره ۲ را به ازاء هر یک از فایلها، پوشه ها و درایوهای موردنظر خود تکرار کرده و در نهایت پس از مشاهده فهرست تکمیل شده (مطابق تصویر شماره ۴) گزینه "OK" را کلیک کنید و نرم افزار امنیتی خود را ببندید. لازم به ذکر است با استفاده از گزینه های "Remove" و "Edit..." می توانید موارد انتخاب شده را حذف و یا ویرایش نمایید.



(تصویر شماره ۴)

سوال ۶: چگونه می توانم از به روز بودن (Update) نرم افزار ضد ویروس خود اطمینان داشته باشم؟

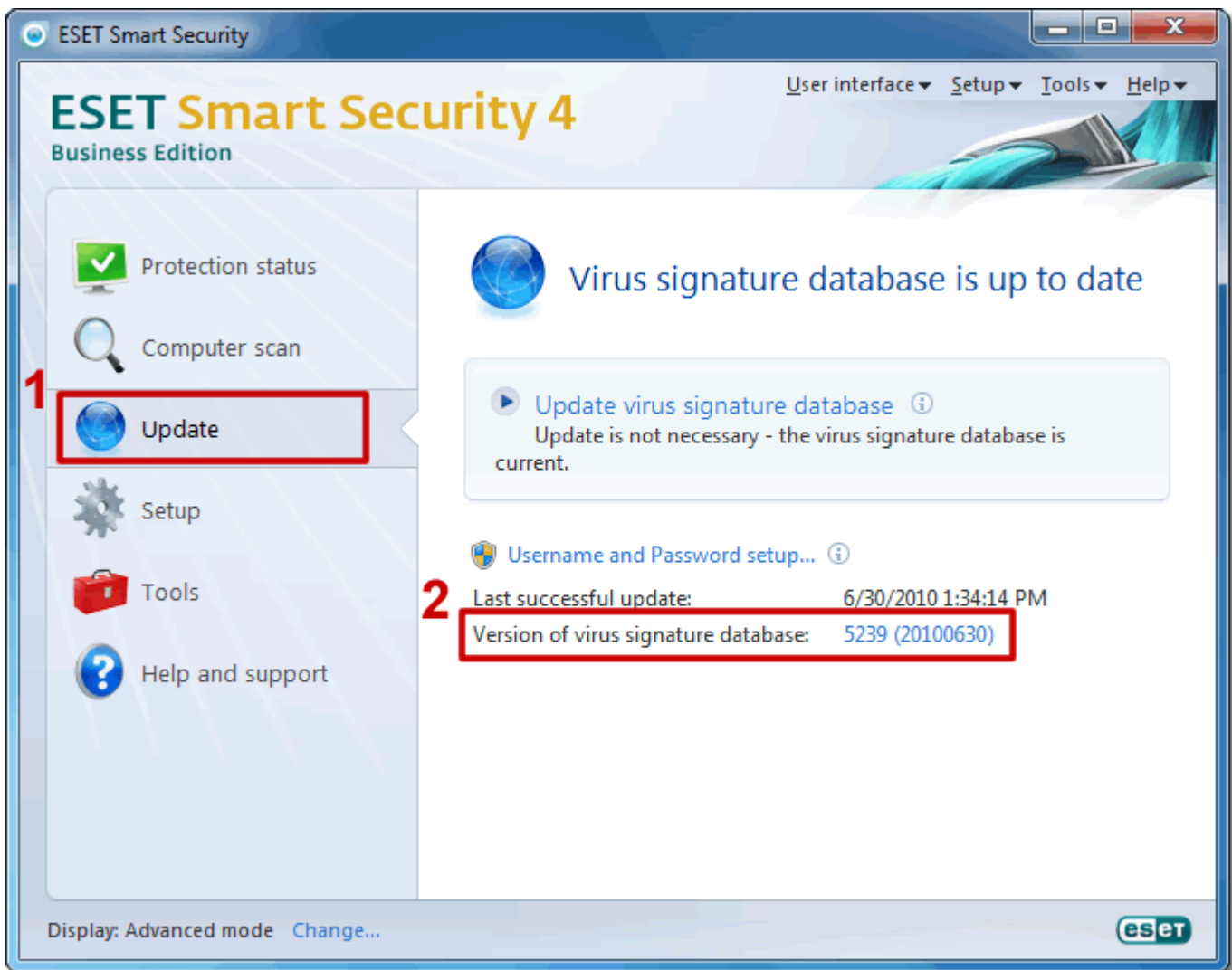
جهت بررسی و اطمینان از به روز بودن (Update) نرم افزارهای شرکت "ESET" مراحل زیر را دنبال نمایید:

۱- شماره بانک اطلاعاتی (Virus Signature Database) مربوط به نرم افزار ضد ویروس خود را یافته و آن را یادداشت نمایید. این شماره به دو روش قابل مشاهده است، در روش اول می بایست نشانگر ماوس را روی آیکن نرم افزار در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) نگه دارید، پس از چند ثانیه پنجره بالنی کوچکی باز میگردد که شماره مذکور در خط دوم آن قابل رویت می باشد .



(تصویر شماره ۱)

همانطور که در تصویر فوق دیده می شود این شماره چهار رقمی قبل از پرانتز درج گردیده و عدد داخل پرانتز نشانگر تاریخ بروزرسانی می باشد. در روش دوم می توانید صفحه اصلی نرم افزار را با دو مرتبه کلیک بر روی آیکن فوق باز نموده و از فهرست سمت چپ گزینه "Update" را انتخاب کرده و در قسمت سمت راست (مطابق تصویر شماره ۲) شماره مذکور را مشاهده نمایید.



(تصویر شماره ۲)

۲- حال به سایت رسمی شرکت کامیران مراجعه نموده و از قسمت سمت چپ در بخش بروزرسانی آنتی ویروس تاریخ و نگارش آخرین بروزرسانی را مشاهده نموده و با آنتی ویروس خود مقایسه کنید. اگر مشابه بودند یعنی آنتی ویروس شما آپدیت و بروز می باشد.

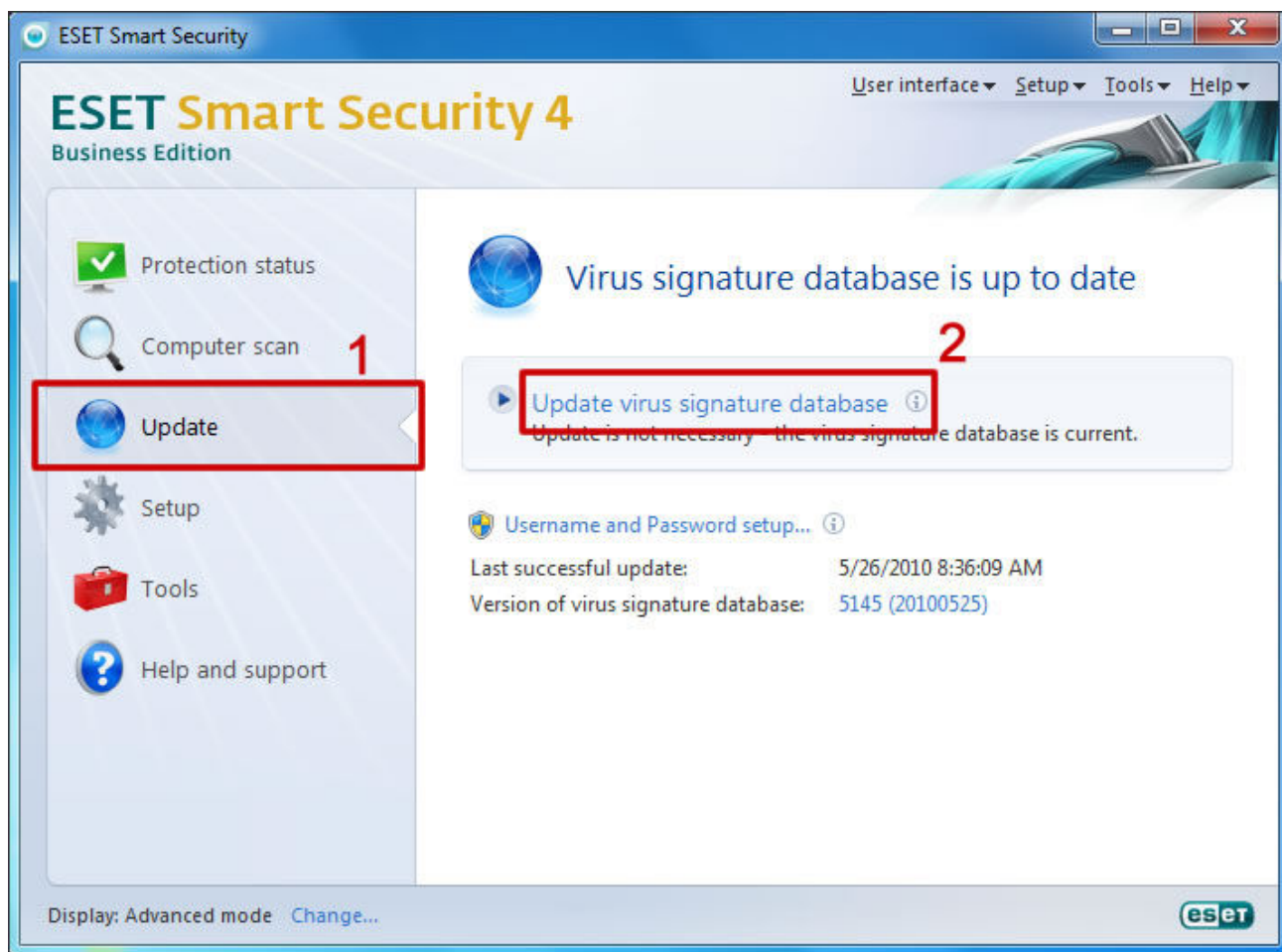
سوال ۷: نحوه به روز رسانی اولیه نرم افزار "NOD32" نسخه خانگی به چه ترتیبی می باشد؟

پس از نصب نرم افزارهای خانگی شرکت "ESET" لازم است رایانه خود را به اینترنت متصل نمایید تا عمل به روز رسانی بصورت خودکار انجام پذیرد. همچنین شما می توانید به منظور اطمینان از به روز رسانی مراحل زیر را بصورت دستی کنترل نمایید:
 ۱- نرم افزار "NOD32" را با کلیک بر روی آیکن آن در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) روی صفحه باز کنید.



(تصویر شماره ۱)

۲- در قسمت سمت چپ از پنجره اصلی نرم افزار گزینه "Update" را انتخاب نموده و از قسمت سمت راست روی گزینه کلیک نمایید.
 (مطابق تصویر شماره ۲)

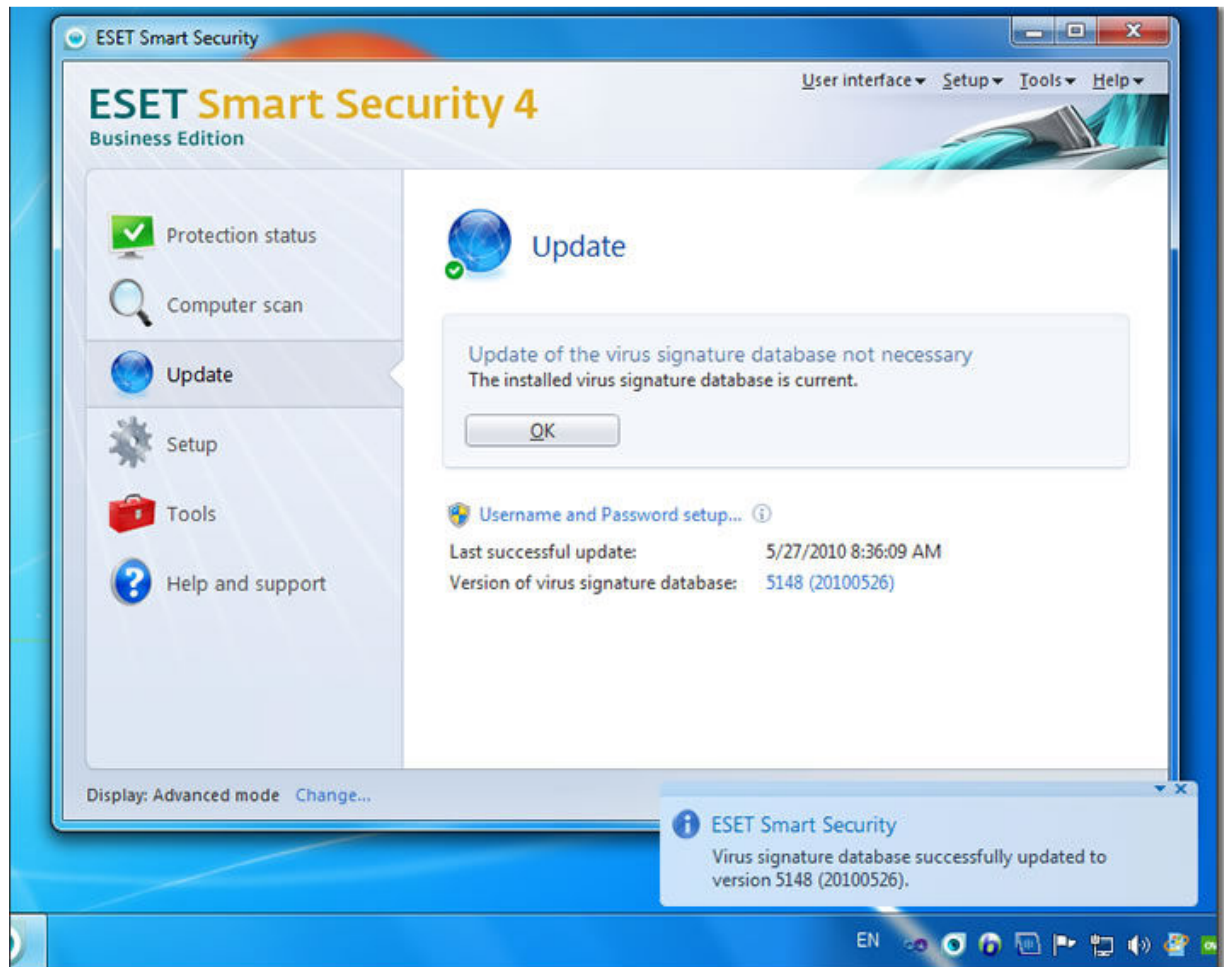


(تصویر شماره ۲)

۳- پس از این کار عملیات به روز رسانی شروع شده (مطابق تصویر شماره ۳) و در نهایت در صورت موفقیت پیامی در گوشه سمت چپ صفحه نمایش مبنی بر اتمام عملیات با درج شماره و تاریخ به روز رسانی (مطابق تصویر شماره ۴) نمایش داده خواهد شد.



(تصویر شماره ۳)



(تصویر شماره ۴)

سوال ۸: ضد ویروس "NOD32" را روی رایانه خود نصب کرده ام، با وجودیکه Username و Password مربوط به لایسنس را وارد می کنم اما نمی توانم آن را آپدیت کنم و با پیغام Invalid Username / Password مواجه میشوم. چگونه این مشکل را برطرف نمایم؟

مراحل زیر را به ترتیب انجام دهید:

۱- تاریخ رایانه خود را بررسی کنید تا مطمئن گردید تاریخ (روز، ماه و سال) و ساعت به درستی تنظیم شده است.

۲- "Username" و "Password" لایسنس را به درستی و با دقت از شناسنامه لایسنس خود تایپ نمایید. دقت کنید که سه حرف اول Username باید با حروف بزرگ وارد شود و Password کاملا با حروف کوچک وارد می شود. در موارد بسیار زیادی بدلیل عدم رعایت در تایپ حروف کوچک و بزرگ ساعتها وقت کاربر تلف گردیده است. در صورت مشاهده خطا می بایست شناسه کاربری (Username) و کلمه عبور (Password) خود را بررسی نموده تا از معتبر بودن آن اطمینان حاصل نمایید.

همچنین با مراجعه به وب سایت رسمی شرکت کامیران از بخش تست لایسنس می توانید وضعیت اعتبار لایسنس و صحت Username & Password خود را چک نمایید.

۳- اگر هنوز مشکل برطرف نشده است بهتراست تنظیمات سرور بروزرسانی را چک کنید. در آنتی ویروس دکمه F5 را بزنید و سپس از سمت راست بخش Update را انتخاب نمایید. از پنل سمت راست دقت نمایید که بخش update server بر روی سرورهای بروزرسانی esetupdates تنظیم باشد و بر روی مسیر های داخلی ویندوز تنظیم نباشد. اگر esetupdates در لیست سرور ها قرار ندارد باید سیستم پدافند داخلی آنتی ویروس (Self Defence) را خاموش کرده ، سیستم را Restart کنید و سپس برنامه تنظیم بروزرسانی آنلاین را از مراحل نصب مجددا نصب کنید (برنامه دوم از مراحل نصب آنتی ویروس) و سپس مجددا Self Defence را روشن کنید. برای فعال یا غیر فعال کردن self defence از بخش تنظیمات آنتی ویروس اولین بخش یعنی Antivirus and antispyware را کلیک کرده و از بخش سمت راست از گزینه Enable Self-defence استفاده نمایید.

۴- اگر با انجام موارد فوق مشکل شما حل نشده است در اولین فرصت با واحد پشتیبانی آنلاین و یا تلفنی شرکت مهندسی کامیران تماس حاصل نموده تا متخصصین پشتیبانی با استفاده از سیستم پشتیبانی فنی از راه دور (Remote Help) مشکل سیستم شما را بررسی نمایند.

سوال ۹: چه تفاوتی میان نسخه های غیر معتبر (کرک) موجود در بازار و نسخه های تجاری نرم افزارهای شرکت "ESET"

وجود دارد و به چه دلیل کاربران ملزم به خرید نرم افزارهای رجیستر شده می باشند؟

نرم افزارهای ضد ویروس بعلاوت انجام نقش حفاظت رایانه ها از اهمیت زیادی برخوردار می باشند هرگونه ضعف و نقصان در کارکرد آنها صدمات جبران ناپذیری به اطلاعات موجود در هارد دیسک کامپیوتر وارد می آورد. نسخه های کرک شده با مسائل و مشکلات مختلفی روبرو می باشند که در زیر به ذکر تعدادی از آنها اشاره می گردد:

۱- نسخه های کرک شده معمولا از دستکاری نسخه های آزمایشی نرم افزارهای ضد ویروس تهیه می گردند حال آنکه نسخه های آزمایشی خود دارای کاستی های متعددی می باشند، از جمله هوش مصنوعی در آنها به مقدار قابل ملاحظه ای تضعیف گردیده است و دیگر آنکه هنگام برخورد با فایل آلوده با آنکه فایل قابل پاکسازی ویروسی (Clean) می باشد اما گزینه حذف فایل (Delete) فعال می باشد و فایل موردنظر از روی رایانه کاربر حذف خواهد گردید. این موضوع بعضا سبب از کار افتادن سیستم عامل نیز می گردد.

۲- نسخه های کرک در هنگام روزآمد شدن فقط مخزن ویروس را روزآمد می نمایند و از روزآمد نمودن ماژولها و بخشهای کلیدی نرم افزار که الگوریتم مبارزه با ویروسها را تغییر میدهد عاجز می باشند.

۳- هر لحظه ممکن است مخزن ویروس و پایگاه داده نرم افزار ضد ویروس کرک شده قطع گردد و تهیه نسخه جدید معمولا با وقفه روبرو خواهد بود. این وقفه ریسک و احتمال آلودگی رایانه کاربر و یا شبکه را افزایش خواهد داد و صدمات ناشی از آن گاه غیر قابل جبران خواهد بود.

۴- مسیر روزآمد کردن مخزن ویروس در نسخه های آزمایشی با مسیر آن در نسخه های تجاری متفاوت بوده و با تاخیر بیشتری روبرو است لذا به همان اندازه ریسک کاربران افزایش می یابد.

۵- کاربرانی که از آنتی ویروس های کرک شده استفاده می کنند از خدمات پشتیبانی شرکت کامیران و همچنین نرم افزارهای رایگان همراه آنتی ویروس اصلی (همانند گارد فلش کامیران و ابزار های مرتبط) بی بهره اند و هیچ شرکت یا ارگانی پاسخ گوی مشکلات آنها نخواهد بود.

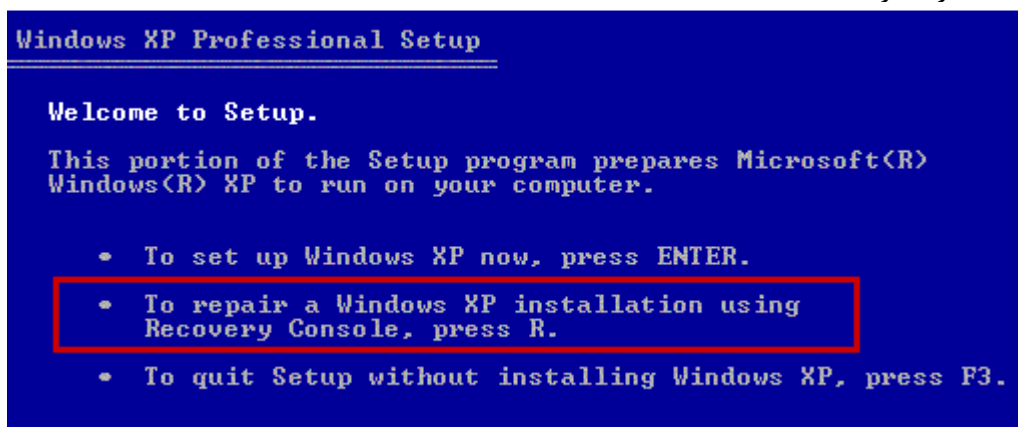
سوال ۱۰: نرم افزار ضد ویروس و ویروسی را با عنوان "MBR" شناسایی می نماید اما قادر به حذف و یا پاکسازی آن حتی در محیط "Safe Mode" نمی باشد، چه باید کرد؟

در مواردی ممکن است ویروسها اقدام به دستکاری و یا آلوده نمودن بخش "Master Boot Record" دیسک سخت رایانه ها نمایند. این بخش حاوی آدرس فایل‌های موجود و ذخیره شده در دیسک سخت می باشد و در صورتی که توسط نرم افزارهای ضد ویروس و یا به هر دلیلی حذف گردد در حقیقت آدرس فایل‌های مذکور از بین رفته و به عبارت ساده اطلاعات موجود روی دیسک سخت از بین می رود. لذا در اینگونه موارد بهتر است با استفاده از امکانات خود سیستم عامل اقدام به بازسازی بخش مذکور به صورت زیر نمود:

:: سیستم عامل "Windows XP"

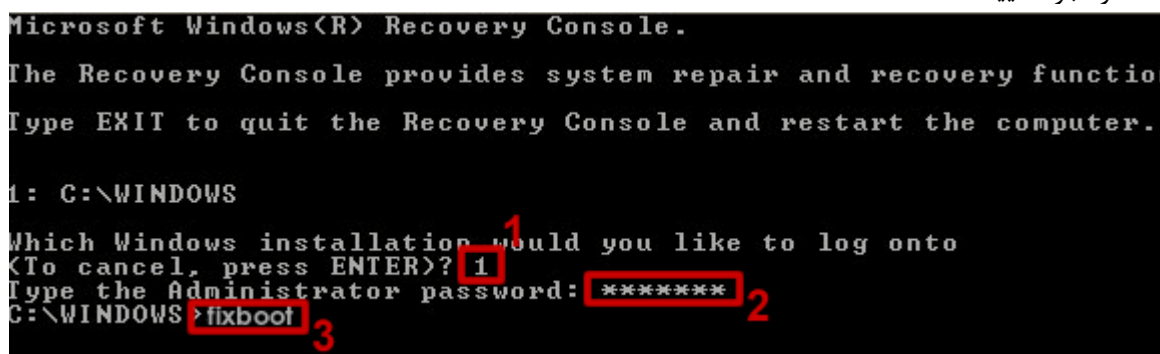
۱- لوح فشرده سیستم عامل را درون دیسک خوان قرار داده و سیستم عامل را بوسیله آن "Boot" نمایید.

۲- پس از انجام مرحله فوق منتظر نمایش صفحه خوش آمد گویی (مطابق تصویر شماره ۱) بمانید. سپس مطابق توضیح نمایش داده شده دکمه "R" صفحه کلید را فشار دهید.



(تصویر شماره ۱)

۳- اکنون (مطابق تصویر شماره ۲) در پنجره کنسول بازسازی سیستم عامل ابتدا شماره سیستم عامل موردنظر خود را انتخاب کرده و در ادامه کلمه عبور سطح مدیریت سیستم عامل (Administrator) را وارد کنید در نهایت دستور "fixboot" را تایپ و با زدن دکمه "Enter" آنرا اجرا نمایید.

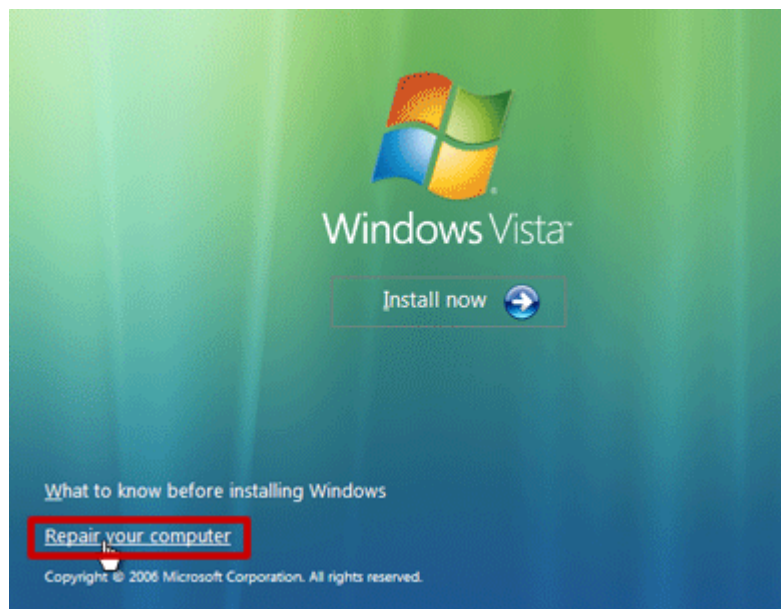


(تصویر شماره ۲)

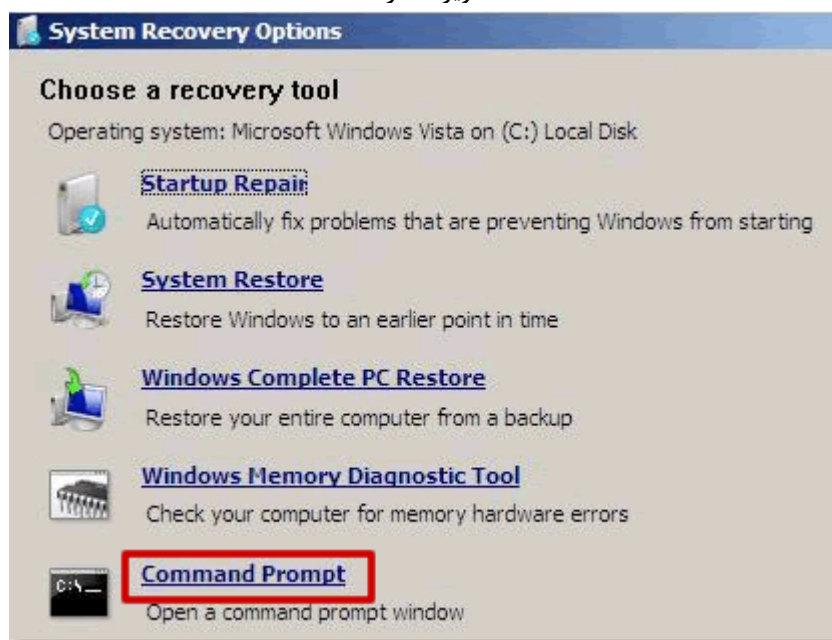
:: سیستم عامل "Windows Vista / 7"

۱- لوح فشرده سیستم عامل را درون دیسک خوان قرار داده و سیستم عامل را بوسیله آن "Boot" نمایید.

۲- پس از انجام این مرحله و انتخاب زبان، زمان و سایر پارامترها صفحه آغازین نصب سیستم عامل (مطابق تصویر شماره ۳) نمایش داده خواهد شد. در این حالت گزینه "Repair your computer" را انتخاب نموده و منتظر نمایش پنجره "System Recovery Options" باشید. در این پنجره (مطابق تصویر شماره ۴) روی گزینه "Command Prompt" کلیک نمایید.



(تصویر شماره ۳)



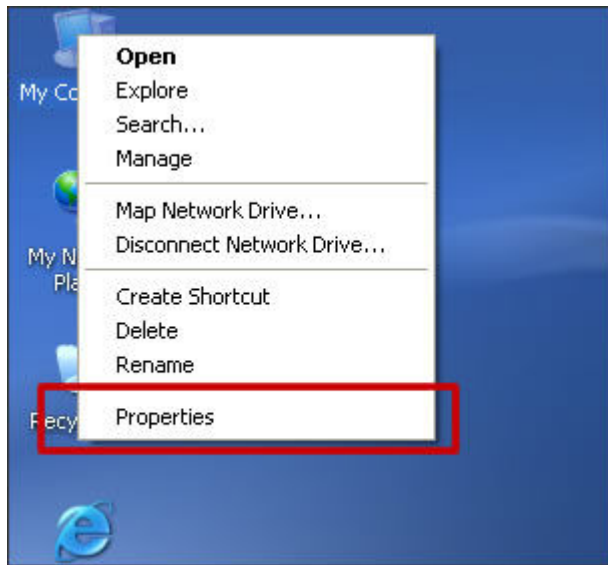
(تصویر شماره ۴)

۳- در نهایت در پنجره "Command Prompt" دستور "bootrec.exe" را تایپ و با زدن دکمه "Enter" آنرا اجرا نمایید.

سوال ۱۱: چگونه باید قابلیت "System Restore" ویندوز را غیر فعال نمود؟

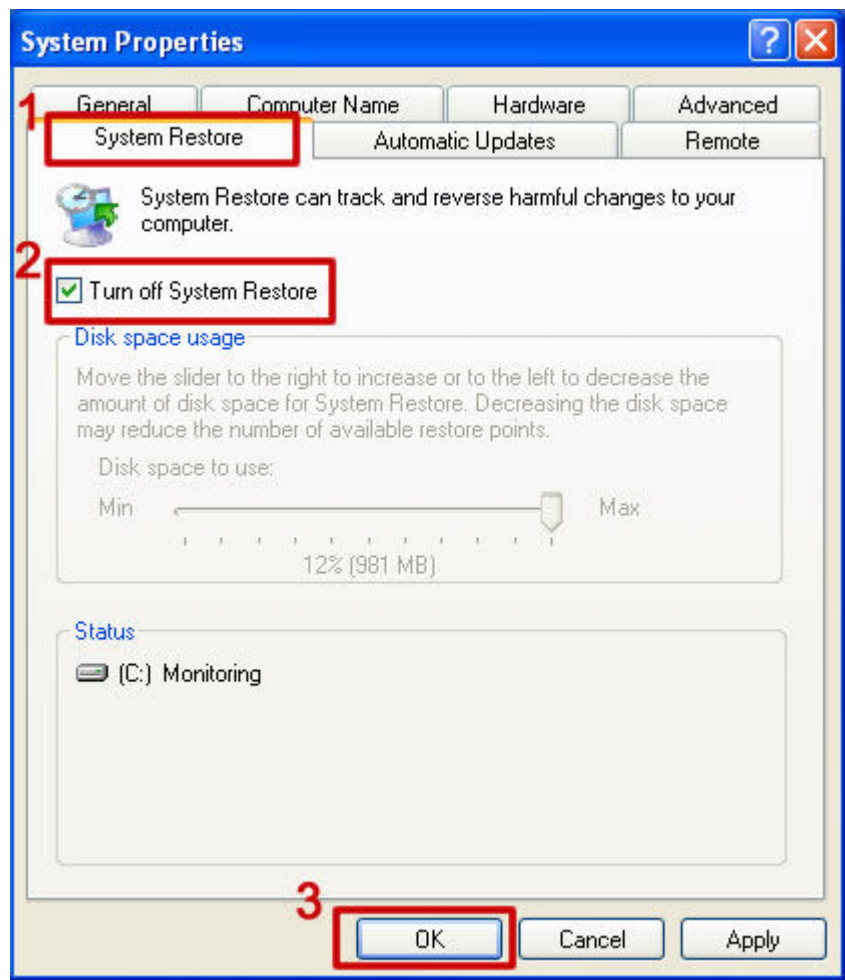
بسیاری ویروسها با استفاده قابلیت "System Restore" می توانند پس از پاکسازی رایانه توسط نرم افزارهای امنیتی، مجددا خود را فعال کنند لذا لازم است این قابلیت را غیر فعال نمود. برای این منظور مراحل زیر را دنبال نمایید:

۱- روی آیکن "My Computer" کلیک راست کرده و گزینه "Properties" را (مطابق تصویر شماره ۱) انتخاب کنید .



(تصویر شماره ۱)

۲- سپس در پنجره باز شده به سر برگ "System Restore" مراجعه کرده و (مطابق تصویر شماره ۲) گزینه "Turn off System Restore" را بزنید و در نهایت دکمه "OK" را کلیک نمایید.



(تصویر شماره ۲)

سوال ۱۲: نحوه اسکن کردن سیستم در محیط "Safe Mode" چگونه است و چه مزایایی دارد؟

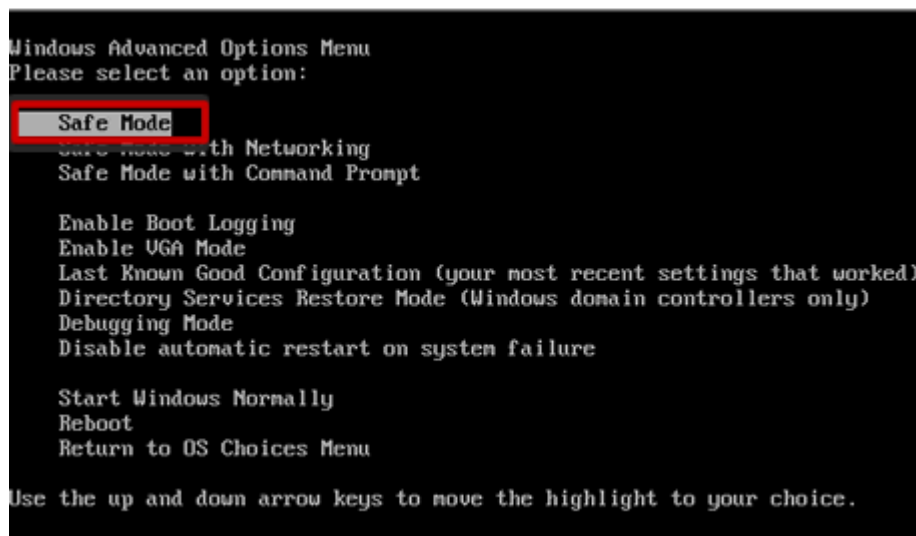
محیط "Safe Mode" محیطی است که در آن سیستم عامل با کمترین سرویسهای ممکن اجرا شده و کمترین منابع سیستمی را در اختیار می گیرد. این حالت بهترین بستر ممکن جهت اسکن و پاکسازی رایانه کاربر از فایل‌های آلوده موجود در آن می باشد. توصیه می گردد کاربرانی که به تازگی اقدام به نصب نرم افزارهای امنیتی شرکت "ESET" کرده اند با استفاده از این روش رایانه خود را اسکن نموده تا از وجود فایل‌های آلوده قبلی اطمینان حاصل کنند. همچنین بعضا ممکن است کاربران با فایل‌های آلوده ای مواجه گردند که نرم افزارهای امنیتی مذکور در حالت معمول ویندوز قادر به پاکسازی آنها نباشد و لازم است تا با استفاده از این روش اینگونه آلودگی ها نیز مرتفع گردند.

هشدار بسیار مهم: اسکن از طریق Safe Mode با استفاده از برنامه اسکنر تحت داس ESET انجام می شود. این برنامه برای کاربران عادی، فاقد امکان قرنطینه می باشد و همچنین شاخه های تعریف شده در بخش Exclusions (استثنا های اسکن) را نیز پاکسازی می نماید. لذا اگر در سیستم خود فایل هایی دارید که در بخش Exclusions تعریف کرده اید، باید آنها را بر روی سی دی یا فلش کپی کنید زیرا پس از اسکن از طریق Safe mode آنها پاکسازی خواهند شد و قابل بازبازی از قرنطینه هم نیستند. کاربران حرفه ای می توانند برای اینکه قابلیت قرنطینه و Exclusions در حالت اسکن Safe Mode فعال شود از سوئیچ ها و پارامتر های خط فرمان استفاده نمایند. توضیحات کامل این فرامین در بخش "۳-۵ خط فرمان" راهنمای PDF آنتی ویروس درج شده است.

برای اجرای اسکن از محیط Safe Mode موارد زیر را به ترتیب دنبال نمایید:

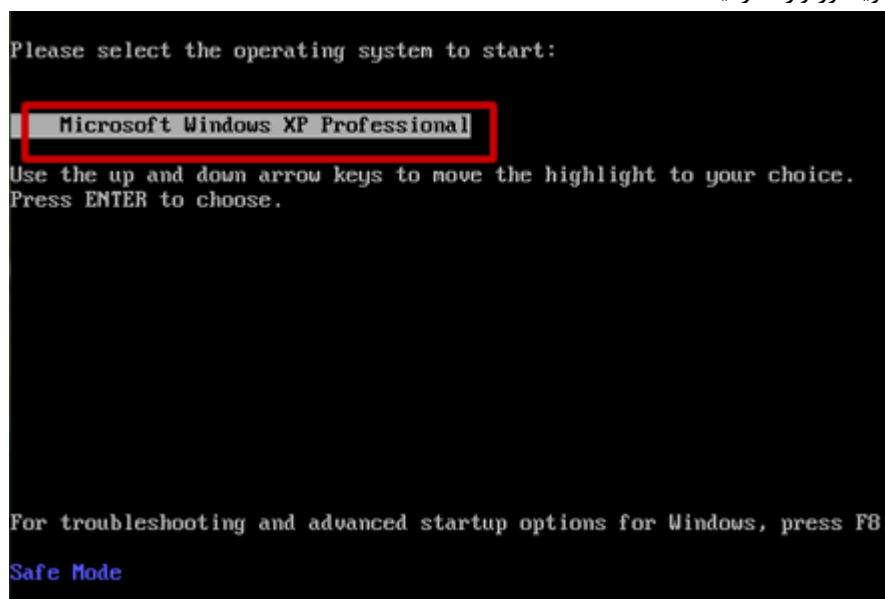
۱ - قابلیت "System Restore" در سیستم عامل را غیر فعال نمایید. (نحوه این کار در مطالب قبل درج شده است)

۲- رایانه خود را "Restart" نموده و در هنگام راه اندازی مجدد دکمه "F8" صفحه کلید را چندین مرتبه فشار دهید تا وارد محیط "Windows Advanced Options menu" گردید سپس (مطابق تصویر شماره ۱) با استفاده از دکمه های جهتی صفحه کلید روی گزینه "Safe Mode" رفته و کلید "Enter" را بزنید.



(تصویر شماره ۱)

۳- پس از این مرحله وارد صفحه دیگری خواهید شد و لازم سیستم عامل خود را انتخاب نموده (مطابق تصویر شماره ۲) و دکمه "Enter" را بزنید در نهایت رایانه شروع به راه اندازی در محیط "Safe Mode" می گردد و پیامهایی را نمایش میدهد (مطابق تصویر شماره ۳) منتظر بمانید تا به صفحه ویندوز وارد گردید.



(تصویر شماره ۲)

```

multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\l_intl.nls
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\FONTS\ugaoen.fon
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\AppPatch\drvmain.sdb
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\ACPI.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\MMILIB.SYS
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\pci.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\isapnp.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\intelide.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\PCIIDEX.SYS
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\MountMgr.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\ftdisk.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\drivers\dnload.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\drivers\dnio.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\PartMgr.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\VolSnap.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\atapi.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\disk.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\CLASSPNP.SYS
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\fltMgr.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\system32\DRIVERS\sr.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\Fastfat.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\KSecDD.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\NDIS.sys
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\System32\Drivers\Mup.sys

```

(تصویر شماره ۳)

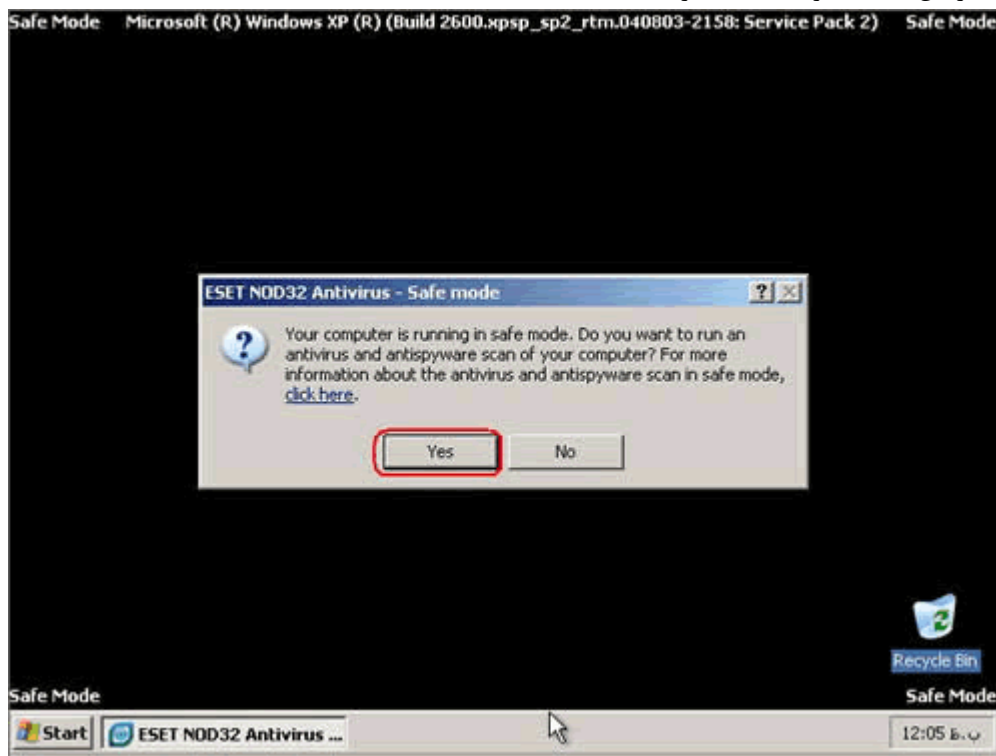
۴- قبل از ورود به صفحه اصلی ویندوز سوالی از شما پرسیده می شود که در حالت گزینه "OK" را انتخاب نموده تا وارد محیط ویندوز گردید.

۵- اکنون می بایست نرم افزار امنیتی را اجرا کرده و اقدام به اسکن رایانه نمایید. بدین منظور وارد منوی "Start" ویندوز شده و با توجه به نوع نرم افزار امنیتی خود با استفاده یکی از مسیرهای زیر آنرا اجرا نمایید.

All Program -> ESET -> ESET NOD32 Antivirus -> ESET NOD32 Antivirus

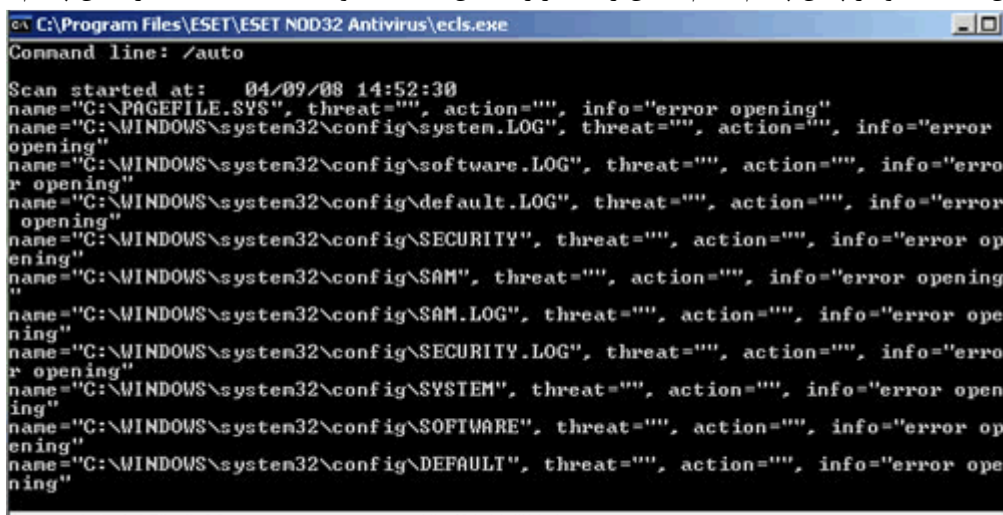
All Program -> ESET -> ESET Smart Security -> ESET Smart Security

۶ - پس از اجرا نمودن نرم افزار با توجه به مسیر اجرایی اجرا شده قبل از شروع به اسکن (مطابق تصویر شماره ۴) تاییدیه ای از کاربر پرسیده می شود که در این قسمت گزینه "Yes" را انتخاب نمایید.



(تصویر شماره ۴)

۷- پس در نهایت عمل اسکن (مطابق تصویر شماره ۵) شروع می گردد. این عملیات بسته به حجم اطلاعات موجود در رایانه ممکن است چندین ساعت بطول بیانجامد و در پایان پیغام اتمام اسکن را به کاربر نمایش میدهد. خواهشمند است تا ظاهر شدن پیغام منتظر بمانید.



```
C:\Program Files\ESET\ESET NOD32 Antivirus\ecds.exe
Command line: /auto
Scan started at: 04/09/08 14:52:30
name="C:\PAGEFILE.SYS", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\system.LOG", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\software.LOG", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\default.LOG", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SECURITY", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SAM", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SAM.LOG", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SECURITY.LOG", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SYSTEM", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\SOFTWARE", threat="", action="", info="error opening"
name="C:\WINDOWS\system32\config\DEFAULT", threat="", action="", info="error opening"
```

(تصویر شماره ۵)

سوال ۱۳: نرم افزار ضد ویروس نصب شده روی رایانه فایلی را به عنوان ویروس شناسایی کرده و آنرا پاکسازی می نماید اما مجدداً ویروس ظاهر می گردد چه کاری باید انجام داد؟

در سیستم عاملهای ویندوز قابلیت با عنوان "System Restore" بصورت پیش فرض به منظور پشتیبان گیری از فایل‌های سیستم عامل فعال می باشد. بسیاری از ویروسها با تکیه بر این قابلیت می توانند خود را قبل از حذف توسط نرم افزارهای ضد ویروس درون این فایل پشتیبان ذخیره نموده و پس از راه اندازی مجدد رایانه دوباره به محل قبلی خود باز گردند. به همین دلیل است که پس از شناسایی و پاکسازی مجدداً توسط نرم افزار ضد ویروس شناسایی می گردد. جهت برطرف نمودن این مشکل مراحل زیر را دنبال نمایید:

۱- قابلیت "System Restore" در سیستم عامل را غیر فعال نمایید.

۲- رایانه موردنظر را در محیط "Safe mode" با استفاده از آنتی ویروس اسکن نمائید. توضیح نحوه اسکن در محیط Safe Mode در مطالب قبلی مندرج است.

۳- پس از اطمینان از حذف کامل ویروس، در صورت نیاز می توانید مجدداً قابلیت "System Restore" را فعال نمایید.

۴- در صورت برطرف نشدن مشکل با واحد پشتیبانی شرکت مهندسی کامیران تماس حاصل نمائید.

سوال ۱۴: پس از اسکن کردن سیستم و پاکسازی کامل درایو های سیستم با دابل کلیک باز نمی شوند. چگونه این مشکل را

برطرف کنیم؟

این مشکل با اعمال عملیات واکسیناسیون توسط گارد فلش فارسی کامیران حل خواهد شد. برای این کار گار فلش کامیران را گشوده و از بخش واکسیناسیون، گزینه واکسیناسیون فلش ها و درایو ها را انتخاب نموده و سیستم را Restart نمایید.

سوال ۱۵: FolderOptions و برخی از قسمت های ویندوز همانند Taskmanager پس از پاکسازی کامل همچنان غیر

است. برای حل این مشکل چه باید کرد؟

برای حل این مشکل باید برنامه Registry Fix از مجموعه گارد فلش را اجرا کنید. به مسیر زیر بروید و برنامه مذکور را اجرا کنید. سپس سیستم را Restart کنید و نتیجه را مشاهده نمایید:

Start → All Programs → KAMIRAN Co. → KAMIRAN Flash Guard → Registry Fix

سوال ۱۶: فلش یا یکی از درایو ها را اسکن و پاکسازی کردیم، اما کلیه اطلاعات آن حذف شد اما فضای اطلاعات حذف شده

در آن درایو همچنان اشغال شده است. برای بازیابی فایل ها چه باید کرد؟

برخی از ویروس ها خود را به شکل اطلاعات کاربر در می آورند و اطلاعات اصلی را از نظر پنهان کرده و به صورت سیستمی تبدیل می کنند. در این حالت در هنگام ویروس یابی به نظر میرسد که اطلاعات اصلی در حال حذف است. اما اطلاعات اصلی با همان حجم همچنان در آن درایو قرار دارد. برای بازیابی اطلاعات مخفی شده به مسیر زیر بروید و برنامه مذکور را اجرا کنید. سپس نتیجه را مشاهده نمایید:

Start → All Programs → KAMIRAN Co. → KAMIRAN Flash Guard → Recover Hidden Data

پس از اجرای این برنامه درایوی که اطلاعات آن مخفی شده است را به صورت (مثال: C:) معرفی کنید و منتظر بمانید که عملیات در صفحه مشکی رنگ ظاهر شده به انتها برسد.

سوال ۱۷: وقتی درایو یا پوشه ای را اسکن می کنم نرم افزار ضد ویروس آن را شناسایی نموده ولی فایل ویروسی را حذف

(Delete) نمی کند چه کاری باید انجام دهم؟

نرم افزارهای امنیتی شرکت "ESET" در حین اسکن و مواجهه با فایل های آلوده ممکن است پیام فوق را برای کاربر به نمایش در آورند. این پیغام دلایل مختلفی می تواند داشته باشد که در زیر به آنها اشاره می کنیم:

۱- فایل آلوده جزء یکی از فایل های در حال اجرا سیستم عامل بوده و یا اینکه در حال حاضر در اختیار نرم افزار دیگری می باشد که این امر سبب می گردد اسکن نرم افزار نتواند اقدام به پاکسازی آن نماید. در این حالت بهتر است رایانه موردنظر را در حالت "Safe Mode" که اکثر سرویس های سیستم عامل به حالت غیر فعال می باشند اسکن نمود.

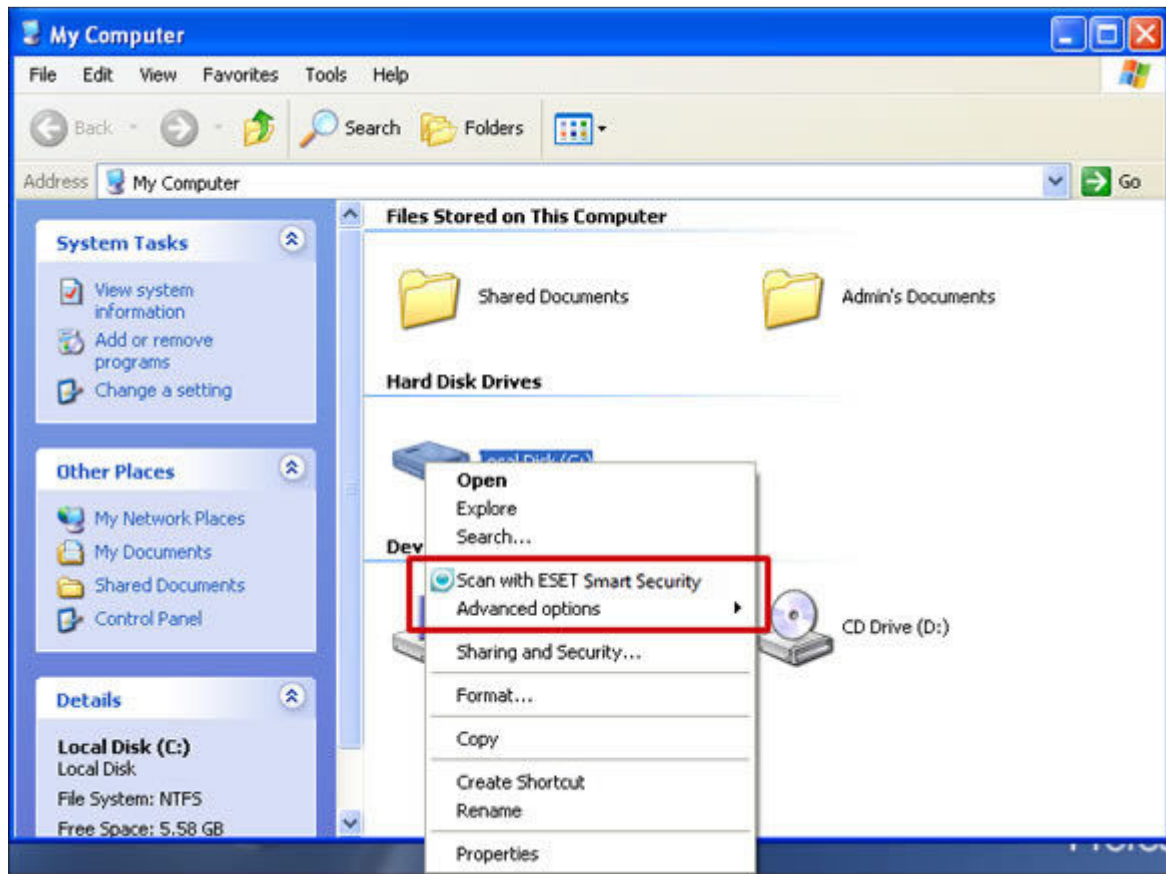
۲- ممکن است نحوه اسکن را به درستی انجام نداده و یا از حالت "Scan without cleaning" استفاده کرده باشید. لذا لازم است با تنظیمات و ویژگی های مربوط به اسکن نرم افزارهای امنیتی شرکت "ESET" آشنا شده آنها را مورد استفاده قرار دهید. (توضیحات بیشتر در سوال بعدی)

سوال ۱۸: نحوه استفاده از اسکنر نرم افزارهای شرکت "ESET" جهت اسکن فایلها، پوشه ها و درایوهای رایانه چگونه است؟

با استفاده از نرم افزارهای امنیتی شرکت "ESET" به دو طریق می توان اقدام به اسکن فایلها، پوشه ها و درایوهای رایانه نمود:

***** اسکن از طریق منوی کلیک راست (Context Menu)**

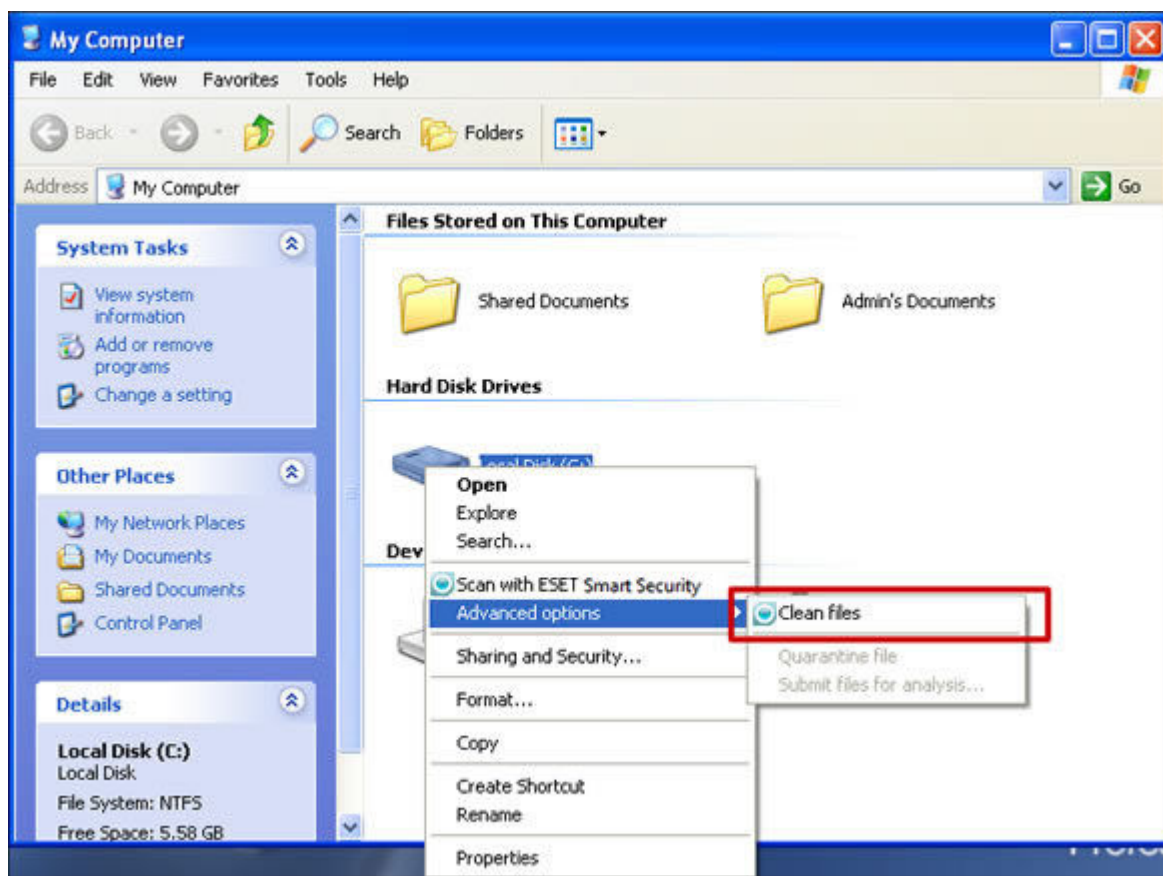
در این حالت می توانید در هر زمان بر روی فایل، پوشه و یا درایو موردنظر خود کلیک راست کنید و در پنجره باز شده (مطابق تصویر شماره ۴) با انتخاب یکی از دو گزینه زیر عمل اسکن را آغاز نمایید:



(تصویر شماره ۴)

۱- گزینه "Scan with ESET... را انتخاب نمایید. در این حالت عمل اسکن با حالت "Scan without cleaning" انجام می پذیرد بدین ترتیب اگر اسکنر نرم افزار ضد ویروس موفق به شناسایی فایل آلوده ای گردد آنرا پاکسازی نخواهد کرد .

۲- از زیر شاخه "Advanced options" گزینه "Clean files" را (مطابق تصویر شماره ۵) انتخاب کنید، در این حالت اسکنر در صورت شناسایی فایل آلوده اقدام به پاکسازی آن خواهد نمود.



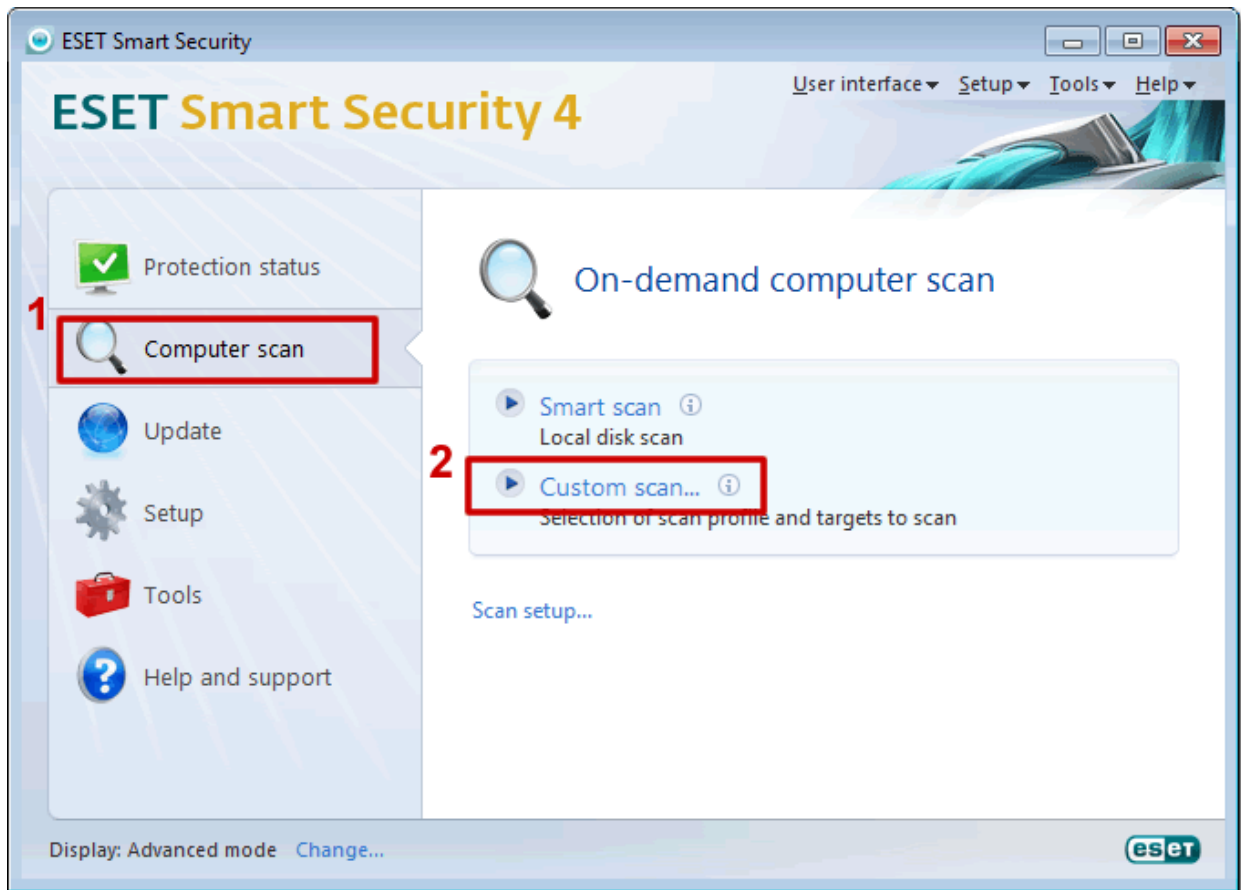
(تصویر شماره ۵)

***** اسکن از طریق محیط اصلی نرم افزار**

در این حالت ابتدا با دو بار کلیک بر روی آیکن نرم افزار در نوار وظیفه ویندوز (مطابق تصویر شماره ۱) وارد صفحه اصلی نرم افزار ضد ویروس گردید. سپس از منوی سمت چپ گزینه "Computer scan" را انتخاب کرده و در پنجره سمت راست گزینه "Custom scan" (مطابق تصویر شماره ۲) کلیک نمایید.

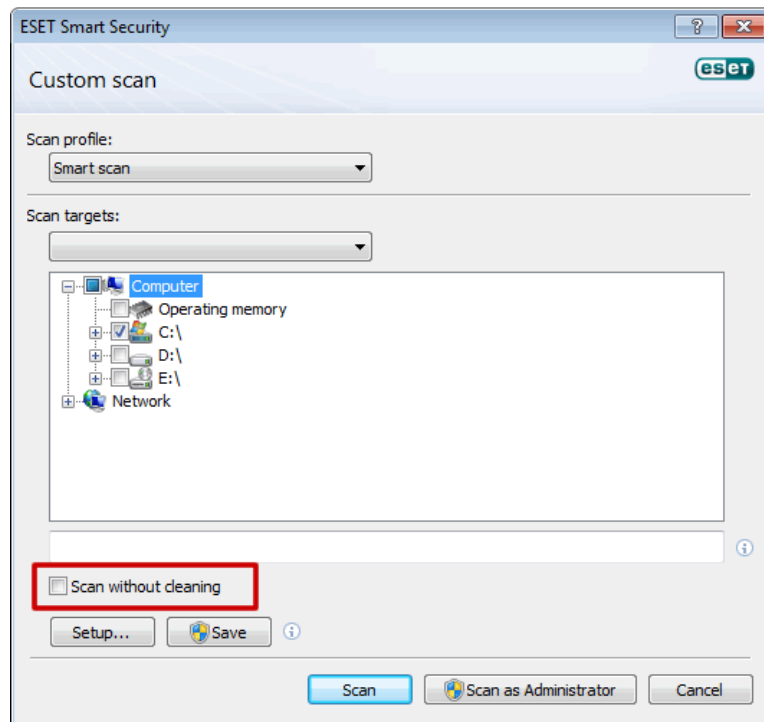


(تصویر شماره ۱)



(تصویر شماره ۲)

بعد از مراحل فوق پنجره اسکنر (مطابق تصویر شماره ۳) باز خواهد شد، در این پنجره مسیر موردنظر را تعیین نموده و دکمه "Scan" را کلیک کنید. لازم به ذکر است شرکت "ESET" در نسخه های جدید نرم افزارهای امنیتی خود امکانی را با عنوان "Scan without cleaning" در قسمت اسکنر خود گنجانیده است. در صورتی که این گزینه در هنگام اسکن انتخاب شده باشد اگر نرم افزار ضد ویروس موفق به شناسایی فایل آلوده ای گردد آنرا پاکسازی نخواهد نمود و فقط کاربر را از وجود آن مطلع میسازد .



(تصویر شماره ۳)

سوال ۱۹: نرم افزار "ESET Smart Security" مرتبا پنجره هایی با عناوین "Inbound" و "Outbound Traffic"

"Traffic" نمایش داده می دهد، این پنجره ها چیست و چه باید کرد؟

پس از نصب محصول "Smart Security" شرکت "ESET" در واقع یک ماژول "Personal Firewall" به عنوان قسمتی از نرم افزار اصلی بر روی رایانه کاربر نصب می شود. کار دیواره آتش (Firewall) کنترل ترافیک ورودی "Inbound" و ترافیک خروجی "Outbound" می باشد. لازم به ذکر است دیواره آتش دارای دو حالت مهم زیر می باشد:

۱- "Automatic mode"

در این حالت کلیه ترافیک ورودی و خروجی رایانه کاربر بصورت خودکار توسط نرم افزار کنترل شده و هیچگونه تاییدیه و پنجره ای برای کاربر نمایش داده نخواهد شد.

۲- "Interactive mode"

در این حالت که معمولا مورد پسند کاربران حرفه ای تر می باشد کلیه ترافیک ورودی و خروجی رایانه کنترل شده و با تمام جزئیات برای کاربر نمایش داده می شود و کاربر می تواند با استناد به داده های مذکور مجوز برقراری و یا عدم برقراری ترافیک را صادر نماید.

برای اطلاع از نحوه تغییر حالت فایروال فیلم آموزشی "کار با دیوار آتش SmartSecurity" را نگاه کنید. (این فیلم آموزشی در مجموعه فیلم های آموزشی آنتی ویروس، در بخش فیلم های تخصصی آنتی ویروس قرار دارد.)

با توجه به حالات مذکور در صورتی که کاربران تنظیمات دیواره آتش نرم افزار خود را بر روی حالت "Interactive mode" قرار دهند پنجره های "Inbound traffic" و "Outbound traffic" با رنگهای (سبز، قرمز و نارنجی) برای آنها نمایش داده خواهد شد (مطابق تصویر شماره ۱) که در زیر به جزئیات آن اشاره شده است:



(تصویر شماره ۱)

*** گزینه "Allow"

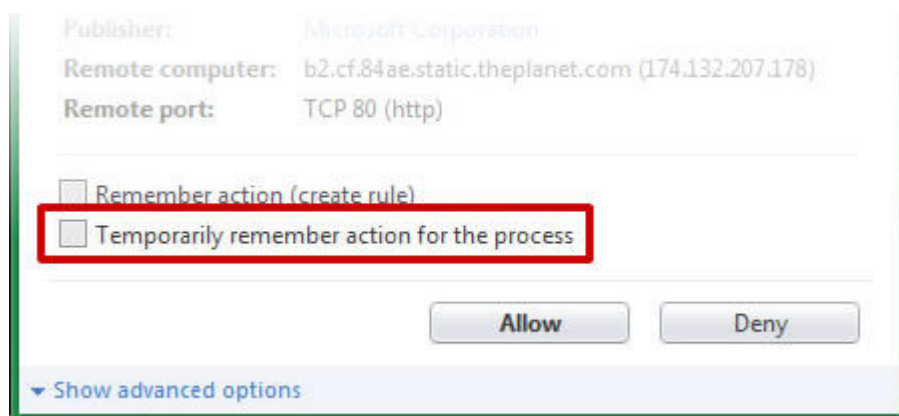
این گزینه به معنای تایید و صدور مجوز جهت برقراری ترافیک مربوطه می باشد. در این حالت کاربر با مشاهده جزئیات ترافیک (با کلیک بر روی گزینه "Show advanced options") موردنظر می تواند به یکی از روشهای زیر تأییدیه خود را به نرم افزار اعلام نماید:

۱- انتخاب گزینه "Remember Action" در صورتی که این گزینه انتخاب شده باشد (مطابق تصویر شماره ۲) و سپس کاربر گزینه "Allow" را کلیک نماید، تأییدیه و مجوز ترافیک مذکور بصورت یک دستورالعمل در نرم افزار ذخیره شده و در صورت برقراری مجدد آن در هر زمانی دیگر پنجره مذکور برای وی نمایش داده نخواهد شد.



(تصویر شماره ۲)

۲- انتخاب گزینه "Temporarily remember..." در صورتی که این گزینه انتخاب شده باشد (مطابق تصویر شماره ۳) و سپس کاربر گزینه "Allow" را کلیک نماید، به ترافیک مذکور موقتاً مجوز داده شده و تا زمانی که رایانه کاربر راه اندازی مجدد (Restart) نگردد برقرار می باشد و پنجره موردنظر این ترافیک تا آن زمان برای کاربر نمایش داده نخواهد شد.



(تصویر شماره ۳)

• در صورتی که کاربر قبل از کلیک گزینه "Allow"، هیچ یک از گزینه های "Remember Action" و "Temporarily remember..." را انتخاب نکرده باشد، به ترافیک موردنظر موقتاً مجوز داده شده و اگر نیاز به برقراری مجدد ترافیک باشد دوباره این پنجره برای کاربر نمایش داده خواهد شد.

*** گزینه "Deny"

این گزینه به معنای عدم تایید و عدم صدور مجوز جهت برقراری ترافیک مربوطه می باشد. در این حالت کاربر با مشاهده جزئیات ترافیک (با کلیک بر روی گزینه "Show advanced options") موردنظر می تواند به یکی از روشهای زیر عدم تایید خود را به نرم افزار اعلام نماید:

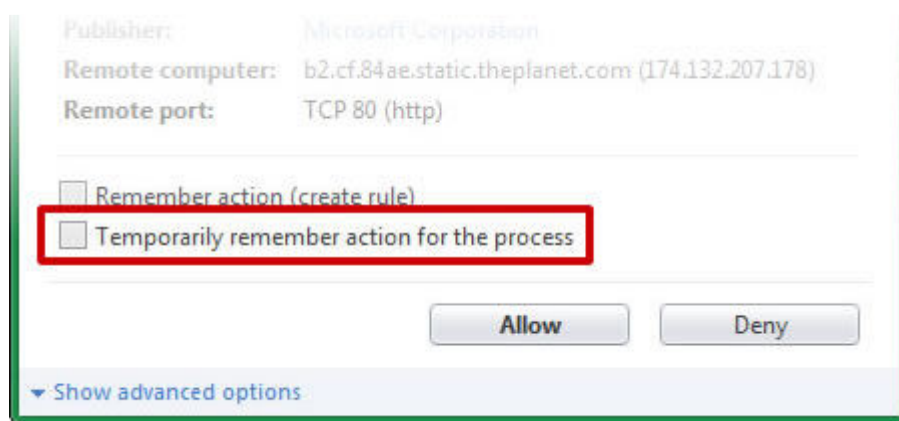
۱- انتخاب گزینه "Remember Action" در صورتی که این گزینه انتخاب شده باشد (مطابق تصویر شماره ۴) و سپس کاربر گزینه

"Deny" را کلیک نمایید، عدم تاییده ترافیک مذکور بصورت یک دستورالعمل در نرم افزار ذخیره شده و در صورت برقراری مجدد آن در هر زمانی دیگر پنجره مذکور برای وی نمایش داده نخواهد شد.



(تصویر شماره ۴)

۲- انتخاب گزینه: "Temporarily remember..." در صورتی که این گزینه انتخاب شده باشد (مطابق تصویر شماره ۵) و سپس کاربر گزینه "Deny" را کلیک نماید، به ترافیک مذکور موقتا قطع شده و تا زمانی که رایانه کاربر راه اندازی مجدد (Restart) نگردد برقرار می باشد و پنجره موردنظر این ترافیک تا آن زمان برای کاربر نمایش داده خواهد شد.



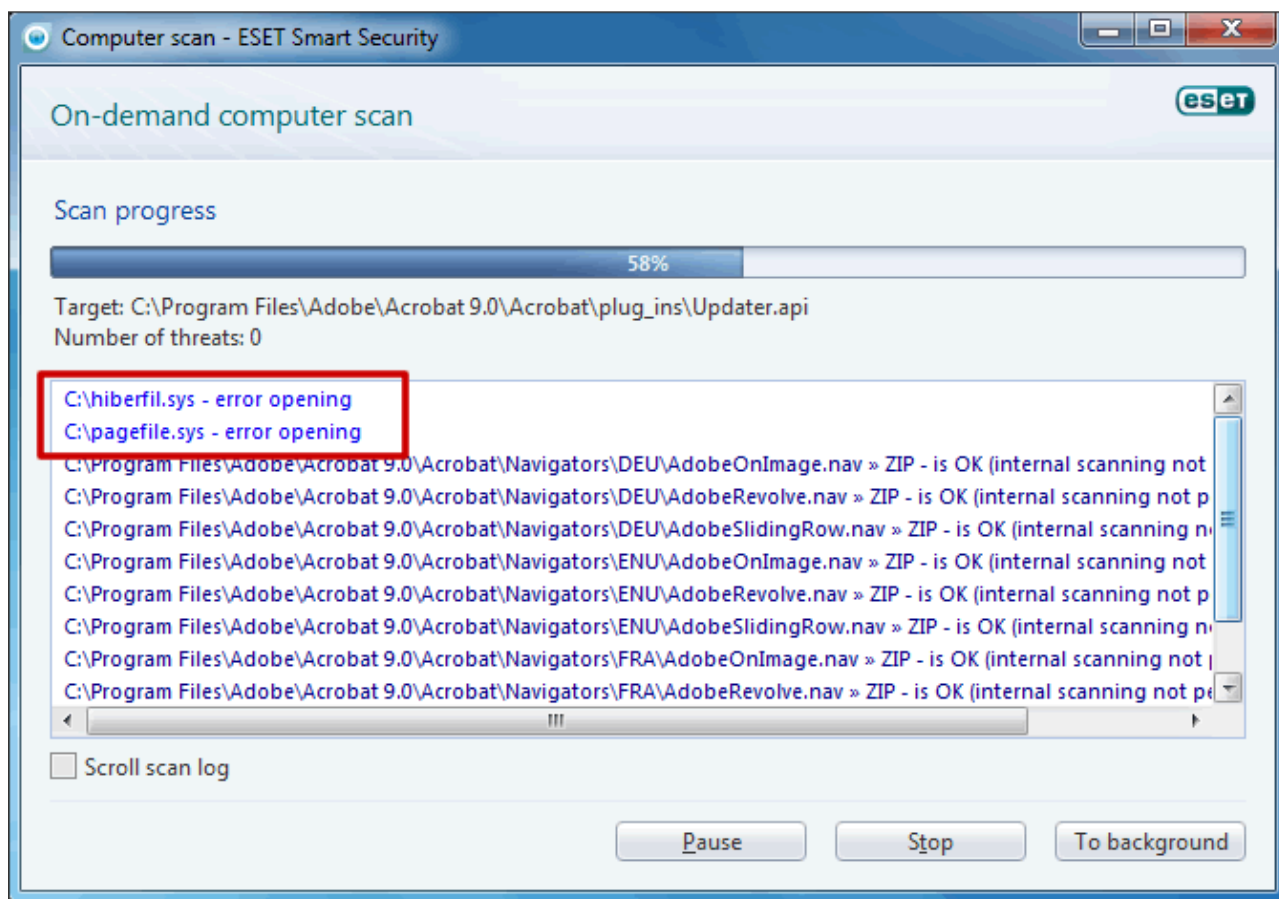
(تصویر شماره ۵)

• در صورتی که کاربر قبل از کلیک گزینه "Deny"، هیچ یک از گزینه های "Remember Action" و "Temporarily remember" را انتخاب نکرده باشد، ترافیک موردنظر موقتا قطع شده و اگر نیاز به برقراری مجدد ترافیک باشد دوباره این پنجره برای کاربر نمایش داده خواهد شد.

سوال ۲۰: چرا هنگام اسکن رایانه در پنجره مربوطه بعضی فایلها بصورت آبی رنگ و با پیغام "error opening" نمایش داده می شود؟

دلایل این پیغام می تواند یکی از موارد زیر می باشد:

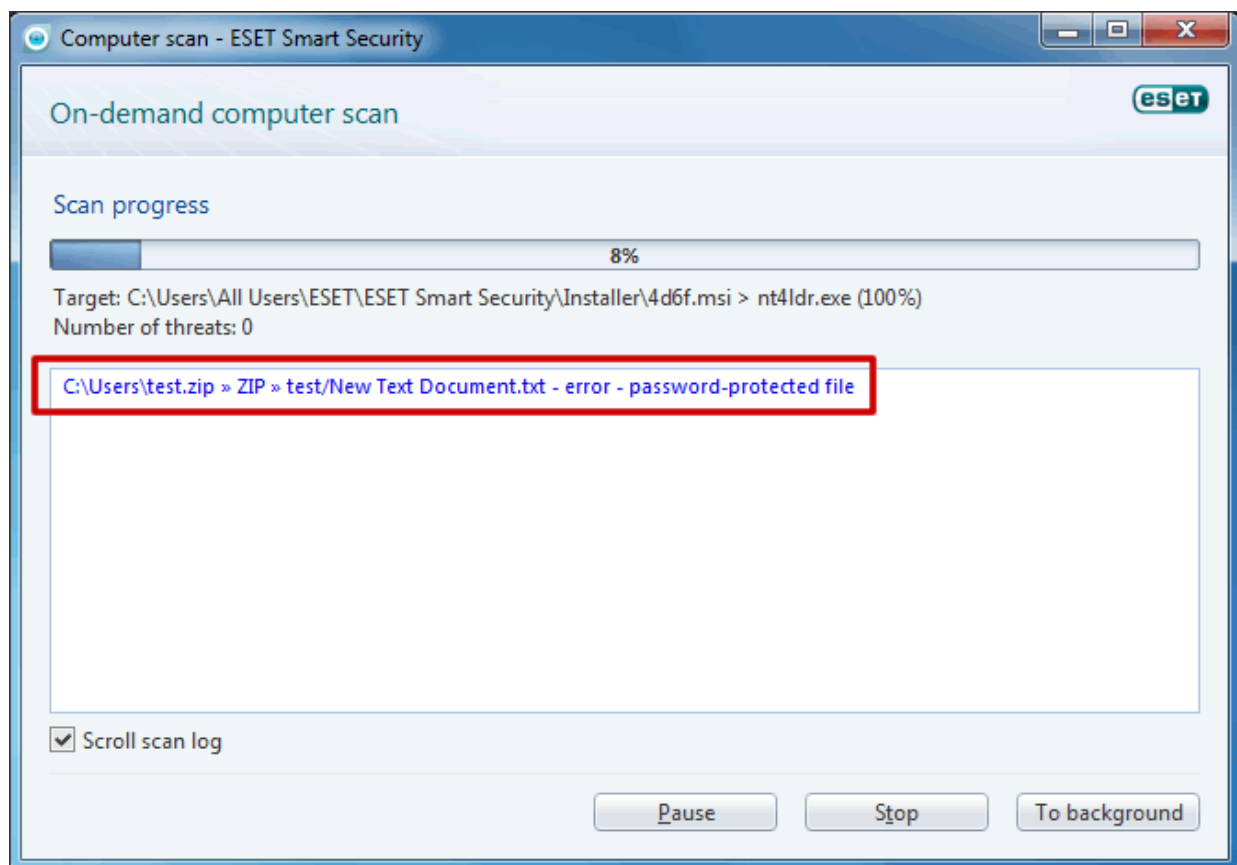
۱- نرم افزارهای امنیتی شرکت "ESET" در هنگام اسکن کلیه فایلها و سرویسهای جاری رایانه را مورد ارزیابی قرار میدهد. چنانچه فایلی جزء یکی از فایلهای سیستمی بوده و توسط سیستم عامل در حال استفاده می باشد لذا اسکنر نمی تواند به آن دسترسی داشته باشد و پیغام مذکور (مطابق تصویر شماره ۱) نمایش داده می شود. لازم به ذکر است یک فایل نمی تواند بصورت همزمان در اختیار دو برنامه قرار گیرد.



(تصویر شماره ۱)

۲- نرم افزارهای ضد ویروس قادر به باز کردن فایلهای فشرده "ZIP, RAR, ..." که دارای رمز عبور می باشند نیستند و به همین دلیل نمی توانند آنها را باز کرده و محتویات آنها را کنترل نمایند به همین دلیل اسکنر نرم افزار هنگام برخورد با این فایلها پیغام مذکور (مطابق تصویر شماره ۲) را نمایش می دهد.

نکته: این نوع فایل ها که با رنگ آبی در گزارشات اسکن مشخص می شوند بی خطر بوده و آسیبی را برای سیستم به همراه نخواهند داشت. برای مثال فایل های hiberfil.sys و pagefile.sys که توسط سرویس های داخلی ویندوز مورد استفاده قرار می گیرند از این دسته فایل ها می باشند.



(تصویر شماره ۲)

سوال ۲۱: در هنگام کار با اینترنت آنتی ویروس پنجره ای با پیام **"Connection terminated - quarantined"** را نمایش داد، منظور از این پیام چیست؟

نرم افزارهای امنیتی شرکت "ESET" دارای گارد مخصوصی به نام "Web access protection" است که در وظیفه آن کنترل کلیه ارتباطات شبکه ای و اینترنتی رایانه می باشد. هنگامی که کاربر حین استفاده از اینترنت مورد حمله سایتی آلوده قرار بگیرد و یا اقدام به دانلود فایلی آلوده از اینترنت نماید این بخش از نرم افزار بصورت خودکار ارتباط رایانه را با آن سایت (مطابق تصویر شماره ۱) قطع نموده و در صورتی که داده نیز در حال بارگیری بود آنرا را قرنطینه می نماید .



(تصویر شماره ۱)

سوال ۲۲: آنتی ویروس در هنگام یافتن فایل آلوده پیام "Cleaned by deleting - quarantined" را در پنجره خود

نمایش می دهد این پیام به چه معنی می باشد؟

نرم افزارهای امنیتی شرکت "ESET" به صورت پیش فرض طوری تنظیم گردیده اند که هنگام مواجهه با فایل آلوده ابتدا سعی در پاکسازی فایل آلوده دارند و در صورتی که فایل موردنظر قابلیت پاکسازی را نداشته باشد اقدام به حذف آن از روی رایانه می نمایند. لذا این پیام (مطابق تصویر شماره ۱) نماینگر این موضوع است که فایل آلوده یافت شده از روی رایانه کاربر حذف گردیده و یک نسخه پشتیبان از آن را در قرنطینه خود نگه داشته است.



(تصویر شماره ۱)

سوال ۲۳: چگونه می توان بر روی تنظیمات آنتی ویروس کلمه رمزی قرار داد تا سایرین نتوانند تنظیمات آنتی ویروس را

تغییر دهند و یا آن را خاموش کنند؟

برای قراردادن کلمه رمز بر روی تنظیمات آنتی ویروس باید در صفحه اصلی آنتی ویروس دکمه F5 را بزنید تا پنجره تنظیمات آنتی ویروس باز شود. سپس از گزینه های موجود در پنل سمت چپ بخش Access Setup را کلیک کرده و از پنل سمت راست دکمه Set Password را کلیک کنید. حال کلمه رمز مورد نظر خود را دو بار در فیلد های موجود وارد کنید و دکمه OK را بزنید. عبارت **Settings are password protected** به رنگ قرمز در صفحه ظاهر میشود که نشان از حفاظت تنظیمات توسط کلمه رمز را دارد. حال برای هر یک از عملیات تنظیمات آنتی ویروس باید رمز تعیین شده وارد گردد.

سوال ۲۴: کلمه رمزی برای آنتی ویروس ESET تنظیم کرده بودیم. اما حال آن را فراموش کرده ایم. چگونه می توان این

رمز را غیر فعال کرد؟

یکی از امکاناتی که ESET در اختیار کاربر قرار می دهد امکان تنظیم یک پسورد برای تنظیمات آنتی ویروس است. به طوری که جهت تغییر تنظیمات آن حتماً بایستی رمز عبور از پیش تعیین شده را وارد کرد. اما ممکن است به هر دلیلی این رمز عبور را فراموش یا گم کرده باشید. در این حالت حتی امکان پاک کردن آنتی ویروس نیز وجود ندارد.

اگر این رمز را فراموش کرده اید برای حذف آن ابتدا بایستی ویندوز را در حالت Safe Mode بالا بیاورید (برای این کار پس از روشن شدن سیستم به طور متوالی کلید F8 را بزنید و پس از پدیدار شدن منوی Windows Advanced Options، در میان گزینه های موجود Safe Mode را انتخاب کنید).

پس از ورود به محیط ویندوز در این حالت، از منوی Start بر روی Run کلیک نمایید و عبارت regedit را وارد کرده و Enter بزنید. در صورت استفاده از ویندوز ویستا یا ۷، پس از کلیک بر روی منوی Start بلافاصله عبارت regedit را وارد نمایید و Enter بزنید تا وارد محیط ویرایشگر رجیستری ویندوز شوید.

اکنون در رجیستری به مسیر زیر بروید:

HKEY_LOCAL_MACHINE → SOFTWARE → ESET → ESETSecurity → CurrentVersion → Info

حال بر روی کلید PackageID راست کلیک کرده و Delete را انتخاب کنید. سپس بر روی دکمه Yes کلیک کنید. حال کافی است ویندوز را در حالت معمولی بالا آورده و نتیجه را مشاهده کنید.

سوال ۲۴: چرا آنتی ویروس برنامه هایی همانند Ultra را ویروس شناسائی می کند در حالی که این برنامه ابزاری برای مخفی کردن IP و گذر از فایروال هاست ؟

نرم افزار اشاره شده و نرم افزار های مشابه توسط آنتی ویروس های ESET به عنوان ویروس شناسائی نمی شوند بلکه اگر در گزارشات آنتی ویروس به آنها دقت کنید عبارت Unwanted Application را در انتهای آنها می بینید. این بدین معناست که این برنامه ویروس نیست اما برنامه ای است که بدون اجازه کاربر اقدام به ارسال اطلاعات و گذر از تنظیمات فایروال می کند که البته نرم افزار مذکور هم دقیقا همین کار را انجام میدهد و وظیفه آن گذر از محدودیت ها و فایروال ها بدون کسب اجازه از کاربر است. برای همین آنتی ویروس آن را به عنوان برنامه های ناخواسته شناسائی می کند.

راه کار پیشنهادی برای این برنامه ها اضافه کردن مسیر آنها در بخش Exclusions است که شرح کامل آن در سوال شماره ۵ و یا فیلم آموزشی تعریف استثنا های اسکن برای آنتی ویروس توضیح داده شده است. زیرا با این کار دیگر آنتی ویروس آن را اسکن نخواهد کرد. (البته اگر به آن برنامه اطمینان کامل دارید)

برای این کار ابتدا باید آنتی ویروس را خاموش کنید (توضیح در سوال شماره ۱) سپس اگر برنامه مورد نظر توسط آنتی ویروس حذف شده است ، آن را از قرنطینه بازیابی کرده (توضیحات در فیلم آموزشی بازیابی فایل های حذف شده از قرنطینه) و سپس با استفاده از توضیحات مندرج در سوال ۵ و یا فیلم آموزشی نحوه تعریف استثناهای اسکن برای آنتی ویروس ، برنامه مورد نظر را به عنوان استثناء معرفی نمایید.

در انتها پس از تعیین برنامه مربوطه به عنوان Exclusions می توانید آنتی ویروس را مجددا فعال نموده و به راحتی برنامه خود را اجرا کنید.

** راه کار دوم (توصیه نمی شود) :

راه کار دیگر برای عدم حذف این گونه برنامه ها خاموش کردن سیستم تشخیص برنامه های ناخواسته می باشد که این گزینه توصیه نمی شود. زیرا حتی اگر این سیستم هم غیر فعال باید با اسکن دستی هارد دیسک برنامه مذکور حذف خواهد شد.

تشخیص برنامه های ناخواسته گزینه ای است اختیاری که کاربر در هنگام نصب آنتی ویروس با انتخاب گزینه Enable detection of potentially unwanted applications آن را فعال می کند و بعد از اتمام نصب می توان آن را بدین صورت غیر فعال کرد. در محیط آنتی ویروس دکمه F5 را زده و سپس از پنل سمت چپ بخش Real-time file system protection را فعال نموده و از پنل سمت راست دکمه SETUP را کیک کنید. در پنجره ظاهر شده از سمت چپ بخش Options را کلیک کرده و گزینه potentially unwanted applications را غیر فعال کنید و سپس پنجره را OK کنید. با این کار در هنگام اجرای برنامه های ناخواسته آنتی ویروس آنها را حذف نخواهد کرد .

سوال ۲۵: اعتبار لایسنس آنتی ویروس من به پایان رسیده است و خطای Username / Password نمایش داده می شود.

برای تمدید لایسنس خود باید چه اقدامی انجام دهم و هزینه این تمدید چقدر است؟

تمدید لایسنس آنتی ویروس برای کاربران قدیمی شرکت کامیران معادل قیمت روز آنتی ویروس با کسر ۲۰ درصد تخفیف می باشد. برای تمدید لایسنس خود می توانید به صورت آنلاین به بخش تمدید لایسنس سایت کامیران مراجعه نموده و یا از فروشگاه آنلاین شرکت کامیران استفاده کنید. همچنین اگر به نمایندگان شرکت دسترسی دارید می توانید با آنها تماس گرفته و به صورت تلفنی یا حضوری لایسنس خود را تمدید نمائید.

اگر امکان تمدید اینترنتی و دسترسی به نمایندگان را نیز ندارید می توانید به صورت تلفنی با واحد پشتیبانی و فروش شرکت کامیران تماس حاصل نموده و لایسنس خود را به صورت تلفنی تمدید نمائید.

سوال ۲۶: نرم افزار حسابداری شرکت ما هلو (طرفه نگار) می باشد. اما در هنگام نصب و استفاده ، آنتی ویروس فایل

Holoo.exe را حذف کرده و اجازه نصب و استفاده از نرم افزار هلو را نمی دهد؟

برخی از نگارش های نرم افزار های حسابداری هلو (محصولی از شرکت طرفه نگار) به دلیل استفاده از پک کننده های موسوم به Themida توسط اکثر آنتی ویروس ها به عنوان یک برنامه پک شده Themida شناخته میشود. آنتی ویروس های ESET نیز این برنامه را به عنوان یک برنامه ناخواسته تشخیص داده و اگر کاربر تنظیمات تشخیص برنامه های ناخواسته را فعال کرده باشد فایل برنامه هلو به عنوان یک برنامه ناخواسته شناسایی شده و پاکسازی می گردد.

دقت کنید که برنامه های ناخواسته (Unwanted Applications) ویروس نیستند و تنها برنامه ای هستند که بدون اجازه کاربر فعالیت هایی را انجام می دهند و صرفا همه آنها خطرناک نیستند.

برای حل این مشکل شرکت کامیران به عنوان نماینده ESET با شرکت طرفه نگار رایزنی نموده اما تا کنون به دلیل عدم همکاری طرفه نگار در اضافه کردن امضای دیجیتال ، نتیجه ای در بر نداشته است زیرا فایل های EXE تولیدی شرکت طرفه نگار همانند اکثر شرکت های ایرانی تولید کننده نرم افزار فاقد اعتبار و امضای دیجیتال بوده و بدین خاطر از سوی شرکت های امنیتی جهان به رسمیت شناخته نمی شود. به هر حال تا زمان تولید این مجموعه هنوز مشکل از سوی طرفه نگار برطرف نشده است . اما شرکت کامیران راهکارهایی برای حل این مشکل معرفی نموده است که از این قرار است :

در هنگام نصب نرم افزار هلو : قبل از شروع فعالیت و نصب برنامه هلو بهتر است سیستم گارد حفاظتی آنتی ویروس را موقتا غیر فعال نمائید . توضیح این کار در سؤال شماره ۱ توضیح داده شده است. پس از نصب کامل هلو می توانید مجددا آنتی ویروس را فعال کنید.

پس از نصب نرم افزار هلو : پس از نصب نرم افزار هلو نیز برای اینکه فایل برنامه توسط آنتی ویروس حذف نشود باید آن را به عنوان استثنای اسکن در بخش Exclusions آنتی ویروس اضافه کنید. آموزش کامل این کار در فیلم آموزشی تحت عنوان "تعریف استثنا های اسکن برای آنتی ویروس" در مجموعه فیلم های آموزشی آنتی ویروس در اختیار شما قرار گرفته است.

برنامه هلو نصب بوده اما توسط آنتی ویروس حذف شده است : لازم به تذکر است که حذف فایل Holoo.exe توسط آنتی ویروس هیچ گونه اختلالی در اطلاعات حسابداری شما به وجود نمی آورد. برای بازیابی فایل Holoo.exe ابتدا آنتی ویروس را غیر فعال کرده (توضیحات مندرج در سؤال ۱) سپس طبق فیلم آموزشی بازیابی فایل های حذف شده از قرنطینه فایل Holoo.exe را بازیابی کنید. (این فیلم آموزشی در مجموعه فیلم های آموزشی آنتی ویروس ، در بخش فیلم های تخصصی آنتی ویروس قرار دارد.) سپس با استفاده از فیلم آموزشی "تعریف استثنا های اسکن برای آنتی ویروس" فایل Holoo.exe را به عنوان استثنا در بخش Exclusions آنتی ویروس اضافه کنید. و در نهایت آنتی ویروس را مجددا فعال کنید.

سوال ۲۷: خرید لایسنس های ESET از شرکت های غیرمعتبر چه پیامد هایی را به دنبال خواهد داشت ؟

برخی از شرکت های موجود در ایران لایسنس های خانگی ESET را از سایر نمایندگان تهیه کرده و هر لایسنس را به چندین کاربر می فروشند که این کار عواقب زیر را به دنبال خواهد داشت :

*** از آنجا که لایسنس های ESET دارای محدودیت کاربر می باشند ، هنگامی که یک لایسنس تک سیستمی روی چند سیستم فعال میشود پس از مدتی توسط شرکت ESET مسدود و Expire می گردد. در این حالت کلیه خریداران آن لایسنس قادر به بروزرسانی آنتی ویروس خود نخواهند بود و دچار مشکل جدی می گردند. در این حالت هم معمولاً شرکت های فروشنده مسئولیتی را قبول نکرده و این مشکل را به عدم حفظ اطلاعات لایسنس توسط کاربر نسبت می دهند. این داستان در نهایت به متضرر شدن کاربر می انجامد و کاربر مجبور است لایسنس دیگری را خریداری کند.

*** این گونه شرکت ها معمولاً گارانتی محکم و رسمی در قبال لایسنس ها ارائه نمی کنند لذا کاربر پس از مسدود شدن لایسنس خود نمی تواند ادعائی در مورد گارانتی لایسنس ها داشته باشد.

*** این گونه شرکت ها فاقد پشتیبانی آنلاین و یا تلفتی هستند و کاربران در هنگام بروز مشکلات ، مرجعی برای مشاوره و راهنمایی ندارند.

*** شرکت های غیر معتبر فاقد لابراتوار ویروس های رایانه ای می باشند و در زمینه تشخیص ویروس های جدید و ناشناخته نمی توانند کمکی به خریداران نمایند.

توصیه های شرکت کامیران برای خریداران محصولات امینیتی ESET :

*** سعی کنید از شرکت هایی خرید کنید که ترجیحاً در استان های کشور نمایندگان فعال دارند و این امر نشان از اعتبار و قدمت آنهاست. معمولاً در وب سایت شرکت ها لیست برخی از مشترکین آنها درج شده است که توجه به این بخش نیز اعتبار آن شرکت را نشان می دهد.

*** حتی المقدور سعی کنید از سایت های اینترنتی که فاقد دفتر مرکزی ، واحد پشتیبانی تلفنی و آنلاین هستند خرید نکنید.

*** در هنگام خرید گارانتی لایسنس خود را به مدت خریداری شده از شرکت فروشنده دریافت نمائید تا در صورت مشکلات احتمالی آپدیت با استناد به آن از شرکت ادعای خسارت کنید.

*** از دریافت گارانتی های لفظی پرهیز کنید. شرکت های معتبر ، گارانتی استرداد وجه را در فاکتور فروش خود قید می کنند. شرکت کامیران حتی در مورد نسخه های تک کاربره خانگی نیز گارانتی استرداد وجه یک ساله لایسنس را به صورت رسمی و قید شده در فاکتور فروش تحویل خریدار می نماید.

*** از خرید لایسنس هایی که از قبل شروع شده است و از مدت یک ساله آنها گذشته است خودداری نمائید . لایسنس های خریداری شده باید از روز فعال سازی به مدت یک سال اعتبار داشته باشند.

سوال ۲۸: مدتی است که پس از بالا آمدن ویندوز، سیستم محافظتی آنتی ویروس ESET غیر فعال است و نماد آن به رنگ قرمز است. لذا هر بار باید به صورت دستی با زدن گزینه Start all Antivirus and antispyware ptotection آنتی ویروس را فعال کنم؟

برای فعال شدن خودکار سیستم محافظتی آنتی ویروس و گارد های آن باید گزینه فعال شدن خودکار سیستم RealTime آنتی ویروس فعال باشد. برای اطمینان از فعال بودن آن، آنتی ویروس را باز کرده، دکمه F5 را بزنید تا پنجره تنظیمات آنتی ویروس نمایش داده شود. سپس از پنل سمت چپ بخش Real-time file system protection را کلیک کرده و از پنل سمت راست گزینه Start Real-time system protection را فعال نمائید. غیر فعال بودن این گزینه باعث می شود سیستم محافظتی آنتی ویروس در هنگام لود شدن ویندوز غیر فعال باشد. اگر با فعال کردن این گزینه مشکل حل نشد با بخش پشتیبانی شرکت کامیران تماس حاصل نمائید.

سوال ۲۹: سیستم من به آلوده به ویروس است و نصب آنتی ویروس روی سیستم با مشکلات مختلفی روبرو میشود. چه راهکاری را پیشنهاد میکنید؟

در مورد سیستم هایی که به ویروس آلوده است ساده ترین کار این است که ویندوز جدیدی نصب نمائید و پس از بالا آمدن ویندوز و نصب درایور های مادربورد، کارت صدا، گرافیک و ... بدون باز کردن درایو های هارددیسک ابتدا آنتی ویروس را نصب نمائید. سپس آنتی ویروس خود را بروزرسانی کرده و بعد طبق فیلم آموزشی اسکن، پاکسازی و واکسیناسیون سیستم کلید درایو های خود را پاکسازی و واکسینه نمائید. در نهایت سیستم را Restart کنید. حال می توانید درایو های هارد دیسک خود را باز کنید. دقت نمائید که اگر بعد از نصب ویندوز و قبل از پاکسازی کامل یکی از درایو های سیستم را باز کنید ممکن است ویروس هایی از نوع Autorun مجددا ویندوز شما را آلوده کرده و روند نصب آنتی ویروس را دچار اختلال نمایند. اگر روند فوق را طبق دستور انجام دهید نیازی به فرمت کامل کلید درایو ها نیز نخواهد بود و تنها فرمت کردن درایو ویندوز در هنگام نصب ویندوز جدید کفایت می کند.

سوال ۳۰: ویندوز من آلوده است و آنتی ویروس روی آن نصب نمی شود. از طرفی هم برنامه های کاربردی مهمی روی آن نصب است و تعویض ویندوز مشکلات زیادی را به دنبال خواهد داشت؟

در مورد آن دسته از کاربرانی که برنامه های کاربردی مختلفی روی سیستم نصب کرده اند و تعویض ویندوز برای آنها مشکل است باید بگوییم راه حل مشکل به دو صورت است. اول اینکه هارددیسک سیستم را به صورت مستقیم و یا با تبدیل های موجود به سیستم دیگری که یک آنتی ویروس اورجینال ESET آپدیت شده روی آن نصب است متصل کرده و آن را ویروسیایی کنید و سپس هارد دیسک را مجدداً به سیستم خود متصل کرده و آنتی ویروس را نصب نمائید. راه کار دوم استفاده از دیسک های نجات آنتی ویروس با قابلیت Bootable است که از آن به عنوان ESET SysRescue یاد می شود. این سی دی ها توسط آنتی ویروس های اورجینال ESET قابل تهیه هستند و قابلیت اسکن سیستم از محیط خارج از ویندوز را دارند. برای اطلاع بیشتر از نحوه کار این دیسک های با پشتیبانی شرکت تماس گرفته و یا به یکی از نمایندگان شرکت مراجعه نمائید. همچنین مقالات مختلفی در مورد طرز ساخت این سی دی در سایت رسمی شرکت کامیران در اختیار شما قرار دارد. همچنین می توانید برای استفاده از خدمات ویروس یابی تخصصی شرکت کامیران به یکی از نمایندگان تائید شده ارائه خدمات شرکت کامیران مراجعه نمائید و از خدمات ویروس یابی تخصصی با استفاده از دیسک های نجات بهره مند شوید.

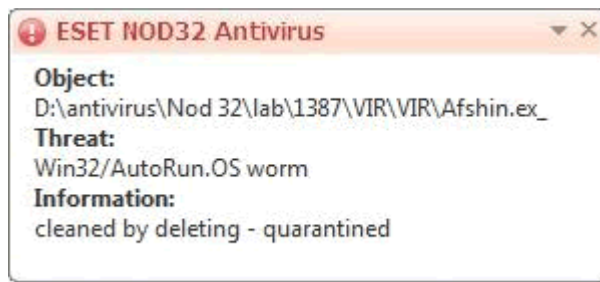
هشدار: دقت نمائید که قبل از انجام هر یک از روش های فوق باید از اطلاعات مهم خود نسخه پشتیبان تهیه نمائید زیرا ممکن است عملیات ویروس یابی به اطلاعات شما صدمه وارد کرده و به دلیل چسبیدن ویروس ها به فایل های اجرایی ویندوز ممکن است ویندوز شما دچار اختلال گردد که در این حالت تنها راه حل تعویض ویندوز می باشد.

سوال ۳۱: نگارش آنتی ویروس ESET من قدیمی است حال نگارش جدید آنتی ویروس خود را تهیه کرده ام . چگونه آن را نصب کنم ؟

برای نصب نگارش جدید می توانید ابتدا نگارش قبلی را Uninstall نموده و سپس نگارش جدید را مجدداً نصب نمایید. (پس از Uninstall کردن نگارش قبلی حتماً باید سیستم Reformat شود) اگر بخواهید اطلاعات آنتی ویروس قبلی از قبیل Username و Password حذف نشود می توانید به روش ارتقاء عمل کنید. برای این کار نیازی به حذف آنتی ویروس قبلی نیست. لذا مثل حالت عادی اگر سی دی آنتی ویروس جدید را دارید مراحل ۱ تا چهار نصب را انجام دهید . (اگر در مرحله ۲ با خطا مواجه شدید سیستم را یک بار Restart کرده و مرحله ۲ تا ۴ را ادامه دهید) اما اگر آنتی ویروس را از سایت دانلود کرده اید دو مرحله بیشتر نخواهید داشت. مرحله ۱: نصب آنتی ویروس و مرحله ۲: نصب گارد فلش کامیران . که این دو مرحله را نیز پشت سر هم نصب نمایید. پس از نصب کامل آنتی ویروس، آیکن آن به رنگ زرد (نارنجی) در می آید که نشان از ارتقای آنتی ویروس به نگارش جدید دارد. حال کفایت برای فعال شدن کامل آنتی ویروس جدید سیستم را Restart نمایید.

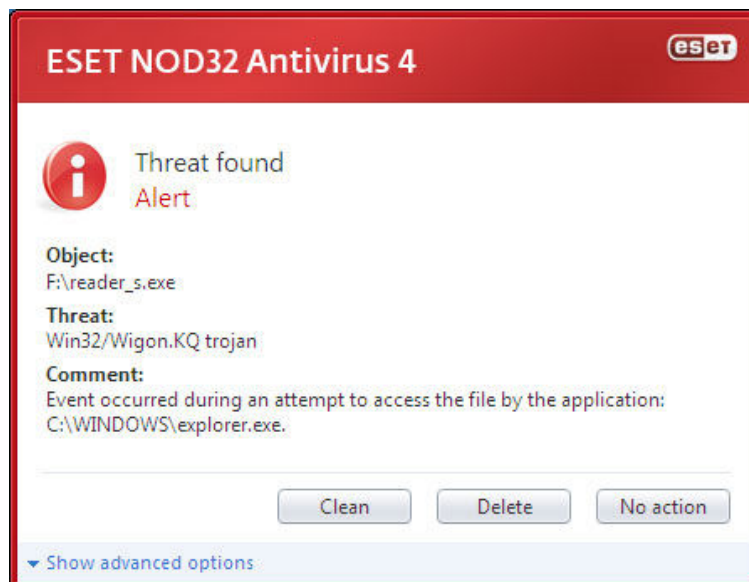
سوال ۳۲: آنتی ویروس من به محض مشاهده یک فایل ویروسی آن را حذف می کند. چه تنظیماتی را اعمال کنم که برای حذف از من کسب اجازه شود ؟

آنتی ویروس های اورجینال ارائه شده توسط شرکت کامیران دارای سامانه پاکسازی خودکار در سیستم Real-time می باشد. در این حالت برای مثال وقتی شما شاخه ای که فایل ویروسی در آن قرار دارد را باز می کنید فایل ویروسی درون آن به صورت خودکار شناسائی شده و پاکسازی میشود و پیغامی به شکل زیر ظاهر می شود.



در این حالت فایل ویروسی یافت شده ، پاکسازی می شود و یک کپی از آن در بخش قرنطینه ذخیره می شود. حال اگر بخواهید آنتی ویروس را به حالتی تنظیم کنید که برای حذف ویروس ها از شما کسب اجازه شود به این طریق عمل کنید **(این کار برای کاربران عادی توصیه نمی شود و تنها برای کاربران حرفه ای کاربرد دارد) :**

آنتی ویروس خود را گشوده و دکمه F5 را بزنید تا پنجره تنظیمات آن ظاهر شود. از پنل سمت چپ بخش Real-time file system protection را کلیک کنید. سپس از پنل راست دکمه Setup را بزنید. بعد از پنجره ظاهر شده از بخش چپ گزینه Cleaning را کلیک کرده و در قسمت راست زبانه میله افقی را به سمت عبارت NoCleaning بکشید و پنجره را Ok کنید. حال اگر به فایل ویروسی برخورد کنید پنجره ای به شکل زیر ظاهر میشود :



در این پنجره با زدن دکمه Clean در صورت امکان فایل آلوده بدون حذف کامل، پاکسازی می شود. اگر امکان پاکسازی فایل نباشد و کل ساختار فایل ویروس باشد فایل به صورت کامل حذف می شود. زدن دکمه Delete هم فایل ویروس را با عملیات حذف از سیستم پاکسازی می کند. فرمان No Action نیز فعلا عملکردی را در مورد ویروس اعمال نمی کند اما دسترسی و اجرای فایل ویروسی همچنان قفل شده خواهد ماند و در صورت کلیک بر روی ویروس، پنجره فوق مجددا ظاهر خواهد شد.

سوال ۳۳: چگونه آنتی ویروس را تنظیم کنم که حتی با زدن فرمان Clean files در منوی کلیک راست هم پس از اجازه کاربر فایل های ویروسی را حذف کند؟

در حالت عادی با کلیک راست بر روی یک درایو و انتخاب گزینه Advanced Options و سپس زدن فرمان Clean Files عملیات اسکن و پاکسازی آغاز شده و کلیه ویروس های یافت شده به صورت خودکار پاکسازی می شوند و نمونه ای از آنها در قرنطینه ذخیره می گردد. برای تغییر این وضعیت به حالت کسب اجازه از کاربر تنظیمات زیر را اعمال کنید **(این کار برای کاربران عادی توصیه نمی شود و تنها برای کاربران حرفه ای کاربرد دارد):**

آنتی ویروس خود را گشوده و دکمه F5 را بزنید تا پنجره تنظیمات آن ظاهر شود. از پنل سمت چپ بخش On-demand Computer Scan را کلیک کنید. سپس از پنل راست دکمه از منوی Selected Profiles نوع پروفایل اسکن را انتخاب نمایید. پروفایل اسکن کلیک راست عبارت Context menu scan می باشد لذا منوی Selected Profiles را بر روی گزینه Context menu scan قرار دهید. سپس از قسمت پایین اولین دکمه Setup را بزنید. بعد از پنجره ظاهر شده از بخش چپ گزینه Cleaning را کلیک کرده و در قسمت راست زبانه میله افقی را به سمت عبارت NoCleaning بکشید و پنجره را Ok کنید.

در منوی Selected Profiles چهار نوع پروفایل اسکن وجود دارد:

Context menu Scan: پروفایل اسکن از طریق کلیک راست

In-dept scan: پروفایل اسکن عمیق سیستم که از طریق اسکن نوع Custom scan از محیط آنتی ویروس انجام میشود.

My profile: پروفایل سفارشی کاربر که در بخش Custom scan قابل استفاده است.

Smart Scan: پروفایل استفاده شده در اسکن Smart Scan که فرمان آن از محیط آنتی ویروس صادر میشود و کلیه درایو ها را به صورت خودکار اسکن و پاکسازی می کند.

هر یک از ۴ پروفایل فوق را می توان به روش گفته شده ویرایش کرد و تنظیمات پاکسازی آن را بر روی NoCleaning قرار داد.

با قرار دادن تنظیمات پاکسازی بر روی Nocleaning اگر در هنگام اسکن فایل ویروسی یافت شود پاکسازی نمی شود و در انتهای عملیات پنجره ای به شکل زیر ظاهر میشود و لیست کلیه فایل های ویروس را نمایش می دهد. حال کاربر با استفاده از منوی موجود در جلوی هر ویروس (Action) می تواند یکی از گزینه های زیر را انتخاب کند :

Clean : پاکسازی ویروس (در صورت عدم امکان پاکسازی ، ویروس حذف خواهد شد)

Delete : حذف ویروس

No Action : عدم حذف ویروس

اگر تعداد ویروس های یافت شده زیاد بود نیازی نیست تک تک منوی های Action را تغییر دهید. کلید های Ctrl+A را بزنید تا همگی انتخاب شوند سپس بر روی یکی از آنها راست کلیک کرده و یکی از گزینه های ... Set Action to را انتخاب نمایید تا برای تمام گزینه های انتخاب شده لحاظ شود.



سوال ۳۴ : ویندوز سیستم را تعویض کرده ام و در هنگام نصب آنتی ویروس کد فعال سازی قبلی تائید نمی شود و برای کد فعال سازی جدید هم پیغام "حق ثبت این سریال به پایان رسیده است" نمایش داده میشود ؟

اگر بعد از تعویض ویندوز در یک سیستم (بدون تعویض هارددیسک یا تعویض سیستم) ، کد فعال سازی قبلی تائید نشود و در هنگام دریافت کد فعال سازی پیغام " حق ثبت این سریال به پایان رسیده است " نمایش داده شود ممکن است مشکل از یکسان نبودن نوع و نگارش ویندوز قبلی و ویندوز جدید شما باشد. برای مثال اگر آنتی ویروس خود را بر روی ویندوز XP فعال کرده باشید و حال ویندوز Seven را نصب کرده اید ممکن است کد فعال سازی ویندوز XP در ویندوز SEVEN تائید نشود (بر عکس این قضیه نیز ممکن است اتفاق بیافتد). در این حالت معمولاً شناسه ۱۰ رقمی سیستم نیز با ویندوز قبلی متفاوت خواهد بود . این مشکل به دلیل قدیمی بودن درایور های ویندوز های XP و به خصوص نگارش SP2 می باشد. برای حل این مشکل اطلاعات زیر را آماده کرده و با پشتیبانی شرکت کامیران به صورت آنلاین و یا تلفنی تماس حاصل نمایید :

- شماره سریال ۱۶ رقمی نرم افزار (مندرج در کارت لایسنس آنتی ویروس)
- شناسه ۱۰ رقمی کامپیوتر در ویندوز جدید (در یکی از روش های فعال سازی ۱ تا ۴ این شناسه قابل مشاهده است.)
- شماره پیگیری نصب در ویندوز جدید (این شماره در برنامه نصب قابل مشاهده است. سی دی آتی ویروس را درون سیستم قرار داده و پس از نمایش نمائنگ و تائید قرارداد ، در پایین صفحه شماره پیگیری نصب شما درج شده است .)
- نوع ویندوز قبلی و نوع ویندوز جدیدی که نصب کرده اید.

با ارائه اطلاعات فوق به واحد پشتیبانی شرکت کامیران ، مجوز نصب شما بر روی ویندوز فعلی صادر می گردد . این حالت ممکن است برای هر سیستم تنها یک بار اتفاق بیافتد و همانطور که گفته شد علت عدم هماهنگی ویندوز قبلی و ویندوز جدید است. پس از فعال سازی مجوز جدید توسط واحد پشتیبانی ، می توانید با استفاده از یکی از ۴ شیوه فعال سازی ، همانند ویندوز قبلی کد فعال سازی جدیدی دریافت نمایید . دقت نمایید که کد فعال سازی دریافتی جدید ، برای ویندوز فعلی و کد فعال سازی قبلی شما برای ویندوز قبلی همچنان معتبر خواهد بود. لذا هر دو کد فعال سازی را در کارت لایسنس یادداشت نمایید تا در صورتی که مجدداً ویندوز قبلی خود را نصب کردید از آن استفاده نمایید.

سوال ۳۵ : می خواهم آنتی ویروس را بر روی سیستمی نصب کنم اما پیغام " حق ثبت این سریال به پایان رسیده است " نمایش داده میشود علت چیست ؟

همانطور که می دانید هر یک از سریال های آنتی ویروس های اورجینال تنها بر روی یک سیستم نصب می شوند و در صورت نصب همزمان بر روی دو سیستم لایسنس آنها باطل شده و منقضی خواهند شد. لذا اگر شما این آنتی ویروس را قبلاً بر روی سیستم دیگری نصب کرده اید نمی توانید به صورت همزمان بر روی سیستم دوم نیز نصب نمایید. لذا برای نصب آنتی ویروس بر روی سیستم دوم پک جدیدی را تهیه نمایید.

اما اگر آنتی ویروس قبلاً بر روی همین سیستم نصب بوده است و بعد از تعویض ویندوز ، پیغام مذکور ظاهر میشود باید طبق توضیحات سؤال ۳۴ عمل نمایید.

اگر هارد دیسک و یا قطعات سیستم خود را به صورت کامل تعویض کرده اید نیز ممکن است این پیغام ظاهر شود که در این حالت اگر مطمئن هستید که آنتی ویروس شما بر روی هارد دیسک قبلی نصب نیست با پشتیبانی تلفنی شرکت تماس گرفته و ارتقای هارد دیسک یا سیستم خود را گزارش دهید تا مجوز نصب بر روی سیستم ارتقاء داده شده صادر شود. دقت نمایید که صدور مجوز ارتقاء سیستم برای هر آنتی ویروس تنها یک بار صادر خواهد شد. برای صدور مجوز ارتقای سیستم یا هارد دیسک باید اطلاعات زیر را به واحد پشتیبانی تلفنی شرکت کامیران اعلام نمایید :

- شماره سریال ۱۶ رقمی نرم افزار (مندرج در کارت لایسنس آنتی ویروس)
- شناسه ۱۰ رقمی جدید کامپیوتر (در یکی از روش های فعال سازی ۱ تا ۴ این شناسه قابل مشاهده است.)
- شماره پیگیری نصب جدید سیستم (این شماره در برنامه نصب قابل مشاهده است. سی دی آنتی ویروس را درون سیستم قرار داده و پس از نمایش نمابندگ و تأیید قرارداد ، در پایین صفحه شماره پیگیری نصب شما درج شده است.)
- نوع قطعات تعویض شده و علت تعویض آنها .

سوال ۳۶ : آیا بین چهار روش فعال سازی و عملکرد آنتی ویروس رابطه ای وجود دارد و کدام روش فعال سازی از همه بهتر است ؟

نوع و روش فعال سازی ارتباطی با عملکرد آنتی ویروس ندارد . شما بر اساس سلیقه و امکانات خود می توانید از یکی از ۴ شیوه استفاده نمایید . اما برای افرادی که دسترسی به اینترنت (حتی اینترنت کم سرعت Dialup) دارند روش ۱ و ۲ پیشنهاد میشود. زیرا در روش ۱ و ۲ (به خصوص روش ۱) امکان اشتباه در حد صفر می باشد . همچنین در روش ۱ و ۲ کلیه اطلاعات کاربر از قبیل نام ، شماره تماس و ایمیل او در بانک اطلاعاتی شرکت ثبت می شود و در هنگام اتمام اعتبار لایسنس آنتی ویروس ، به وسیله پیامک و ایمیل ، زمان تمدید لایسنس به اطلاع او میرسد. در حالت ۳ (پیامک) نیز شماره موبایل کاربر در سیستم ثبت می گردد و در زمان انقضای لایسنس ، پیامک هشدار برای او ارسال می شود. اما در شیوه ۴ (تلفن گویا) هیچ اطلاعاتی از کاربر در سیستم ثبت نمی شود و پیشنهاد می گردد در صورت استفاده از این روش بعداً از روش ۲ و ورود به سایت www.RegisterArea.com اطلاعات خود را در سایت شرکت ثبت نمایید تا در هنگام سررسید تمدید لایسنس ، پیامک و ایمیل مربوطه برای شما ارسال شود.

اگر پاسخ سؤال خود را در مطالب فوق نیافتید می توانید سؤالات خود را به صورت تلفنی یا آنلاین با واحد پشتیبانی شرکت کامیران مطرح نمائید :

واحد پشتیبانی و فروش شرکت مهندسی کامیران :

0261 – 6517341 – 6615190

www.KAMIRAN.org
www.NOD32Antivirus.ir
www.NOD32Co.ir

سامانه پشتیبانی آنلاین شرکت مهندسی کامیران :

<http://www.kamiran.org/onlinesupport/livezilla.php>

سامانه دریافت پیامک :

30006863001919