**تنظيمات سخت افزاري و نرم افزاري**

🞏 به صورت زمان بندي شده منظم از داده ها و پرونده ها پشتيبان گيري نماييد.

🞏 سرور هاي خود را (شامل سرورهاي ايميل و فايروال) با نرم افزار ضد ويروس محافظت نماييد.

🞏 در تمام كامپيوترهاي ايستگاه كاري ضد ويروس نصب كنيد.

🞏 گزينه محافظت از ويروس را در تنظيمات CMOS (در صورت وجود) فعال كنيد.

🞏 فايروال شبكه اي را نصب و به طور مناسب تنظيم نماييد.

🞏 يك فايروال نرم افزاري را مانند ZoneAlarm يا فايروال ويندوز (در ويندوز ايكس پي) در كليه كامپيوترهاي ايستگاه كاري نصب كنيد.

🞏 فقط پورت هاي مورد نياز را در تنظيمات فايروال باز بگذاريد. توجه ويژه به پورت هاي مورد استفاده نرم افزارهاي FTP يا اشتراك فايل مانند iMesh ، Kazaa ، Gnutella ، Morpheus و Grokster داشته باشيد.

🞏 به طور منظم شبكه خود را براي بررسي پورت هاي باز اسكن كنيد.

🞏 كامپيوترهاي ايستگاه كاري را طوري محدود كنيد كه كاربران عادي نتوانند نرم افزارهاي غير مجاز مانند برنامه هاي تأييد نشده دريافت ايميل، چت، FTP و برنامه هاي اشتراك فايل نصب نمايند.

🞏 در صورت امكان فايل هاي حساس سيستم عامل (مانند win.ini، system.ini، autoexec.bat ، config.sys ، boot.ini) را با مشخصه فقط خواندني تنظيم كنيد تا تغييري در آنها داده نشود.

🞏 مجوز هاي دسترسي به رجيستري ويندوز و ساير فايل هاي سيستم عامل را به گونه اي تنظيم كنيد كه از تغييرات غير مجاز آنها جلوگيري شود.

🞏 ضد ويروس را طوري تنظيم كنيد كه در صورت قديمي شدن بانك اطلاعات شناسايي ويروس، به شما اخطار بدهد.

🞏 سرور ها را طوري تنظيم كنيد كه تمامي فايل هاي ورودي و خروجي را براي شناسايي ويروس اسكن كنند.

🞏 تمامي انواع فايل ها را موقع اسكن ويروس انتخاب نماييد؛ مانند فايل هاي zip ، exe و dll.

🞏 از نرم افزارهايي استفاده كنيد كه فايل هاي را قرنطينه مي كنند. اين كار باعث مي شود كه كاربران نتوانند به فايل هاي آلوده دسترسي پيدا كنند و ويروس را منتشر نمايند.

🞏 در صورتي كه اشكالي پيش نمي آيد در كامپيوترهاي ايستگاه كاري حساس، دسترسي به درايو فلاپي را از طريق CMOS با كلمه رمز محدود كنيد. اگر اين امكان وجود ندارد حداقل گزينه بوت از طريق فلاپي را غير فعال نماييد.

🞏 اخطار صوتي را براي زمان تشخيص ويروس فعال نماييد.

🞏 پاسخ كاربران به ضد ويروس را به هنگام برخورد و كشف ويروس روي حداقل گزينه قابل قبول مانند پاكسازي يا قرنطينه تنظيم كنيد و اجازه انصراف از ترميم را به كاربران ندهيد.

🞏 محافظت از ويروس هاي ماكرو را در نرم افزارهايي مانند ورد و اكسل فعال نماييد.

🞏 فهرست استثناء فايل ها (file exclusion) را در ضد ويروس طوري تنظيم كنيد كه فايل هاي exe و dll حتما ويروس يابي شوند؛ چون اغلب ويروس ها به اين نوع فايل ها حمله مي كنند.

🞏 ديسكت هاي راه انداز اضطراري را ايجاد و نگهداري كرده، دكمه حفاظت از نوشتن را فعال نماييد.

🞏 از هارد ديسك هايي كه در ايستگاه هاي كاري معمولي استفاده مي شوند، كپي استاندارد (image) تهيه كنيد. زماني كه براي نصب مجدد سيتسم عامل و نرم افزار ها نيساز به فورمت مجدد هارد ديسك باشد، داشتن اين كپي روي هارد باعث سريع تر شدن زمان راه اندازي و آماده سازي سيستم خواهد شد.

🞏 تمامي مودم هاي داخلي را از كامپيوتر هاي ايستگاه كاري خارج كنيد، تا اتصال آن ها به اينترنت فقط از طريق فايروال سازمان باشد.

🞏 كلمات رمز ساده يا پيش فرض را براي سرور ها، تجهيزات شبكه، كاربران مدير شبكه و امثالهم استفاده نكنيد.

🞏 شبكه ي سازمان را به طور مرتب بررسي كنيد تا كاربران غير مسؤول انفورماتيك، سيستم عامل سرور بر روي آن ها نصب نكنند.

**سيستم عامل و ديتابيس ويروس**

🞏 به طور مرتب آخرين به روز رساني هاي امنيتي و ترميمي را در سيستم عامل هاي سرور و كلاينت خود نصب كنيد. در صورت امكان سيستم 🞏 ها را طوري تنظيم كنيد كه به روز رساني ها مذكور را به طور خودكار دريافت كنند. (automatic updates)

🞏 به طور منظم و زمان بندي شده فايل هاي ديتابيس ويروس ها را به روز رساني نماييد و در صورت امكان نرم افزار ضد ويروس خود را طوري 🞏 تنظيم كنيد كه به صورت خودكار از طريق سايت كمپاني سازنده ي ضد ويروس يا يك سرور داخل سازمان به روز شود.

🞏 به روز رساني ها را بين كامپيوترهاي كلاينت توزيع كنيد. در صورتي كه سيستم عامل شبكه اي (NOS = Network Operating System) به شما امكان نمي دهد كه به روز رساني ها را از راه دور نصب (push) كنيد آنها را به صورت ضميمه ي ايميل (يا هر ابزار استاندارد ارتباطي كه استفاده مي كنيد) به كاربران تان ارسال كنيد..

🞏 يك سرور اختصاصي براي دريافت به روز رساني ها تنظيم كنيد كه كاربران از طريق اتصال به آن به روز رساني هاي مورد نياز خود را دريافت نمايند. با اين كار حداقل در مصرف پهناي باند اينترنت صرفه جويي خواهيد كرد.

🞏 به روز رساني ها را در صورت امكان از طريق دستورهاي اسكرپت ورود به سيستم (login script) براي كاربران ارسال نماييد.

🞏 در صورتي كه امكاني براي توزيع به روز رساني ها در شبكه نداريد، يك نرم افزار براي مديريت كلاينت هاي شبكه مانند

Novell Zenworks Configuration Management يا Sysmantec Altiris Client Management Suite خريداري كنيد. اين نرم افزار ها به شما امكان نصب از راه دور به روز رساني ها در كامپيوتر هاي اسيتگاه كاري را مي دهند.

🞏 هر زمان كه فايل هاي سيستم عامل به روز رساني مي شوند ديسك هاي راه انداز محافظ شده (write protected) خود را به روز رساني كنيد.

🞏 صرفا به يك منبع براي دانسته هاي امنيتي خود بسنده نكنيد. هميشه چند وب سايت امنيتي را بررسي كرده، براي دريافت اخطارها و خبرنامه هاي امنيتي در آن ها ثبت نام كنيد.

**مديريت حافظه هاي قابل انتقال مانند فلاپي ها، سي دي، دي وي دي، حافظه ي فلاش و ...**

🞏 حافظه هايي را كه از جاي نامعلوم دريافت مي كنيد استفاده نكنيد.

🞏 مقرراتي وضع كنيد تا كاربران ملزم شوند هر حافظه اي را كه از خارج از سازمان تهيه كرده باشند، حتما ويروس يابي كنند.

🞏 تعدادي ديسكت (يا هر حافظه ي جانبي مشابه) بدون ويروس در سازمان تهيه كنيد كه كاربران در مواقع نياز كه با كامپيوتر خانه شان كار بكنند از آن ها استفاده نمايند. پس از بازگرداندن ديسك به داخل سازمان مجددا آن ها را ويروس يابي كنيد تا آلودگي احتمالي از كامپيوتر خانه شان به داخل سازمان منتقل نشود.

🞏 تمامي ديسكت (يا حافظه جانبي مشابه) هاي حاوي داده يا برنامه را در برابر نوشتن محافظت كنيد.

**ويروس يابي (scanning)**

🞏 كامپيوتر اختصاصي در نظر بگيريد كه به طور مداوم پوشه هاي حاو ي داده ها را در شبكه ويروس يابي كند.

🞏 به طور زمان بندي شده ويروس يابي كامل (Full Scan) را براي كامپيوترهاي ايستگاه كاري در نظر بگيريد به طوري كه كمترين تداخل و درگيري با كاربر پيش بيايد. مانند زمان ناهار يا ساعت غير كاري.

🞏 از حالت ويروس يابي پس زمينه (background scanning/stealth mode) استفاده كنيد كه كمترين تداخل با كاربر سيستم پيش بيايد.

🞏 اين امكان را كه كاربران بتوانند در كار ضد ويروس مداخله كنند، غير فعال نماييد.

🞏 حالت نظارت پس زمينه و ويروس يابي بلادرنگ (real time scanning) را براي تمامي كامييوتر هاي ايستگاه كاري فعال كنيد.

🞏 در صورت امكان از ابزار (add on/plug in) ويروس يابي براي مرورگر استفاده كنيد كه قبل از دانلود، فايل را ويروس يابي كند. اگر چنين ابزاري در دسترس نيست مطمئن شويد كه همه ي فايل هاي دانلود شده قبل از استفاده يا نصب ويروس يابي مي شوند.

🞏 در شركت هاي كوچك مي توانيد تاريخ آخرين ويروس يابي كامل را براي هر كامپيوتر ايستگاه كاري مستند كرده، به مسؤول انفورماتيك تحويل دهيد.

🞏 كامپيوترهاي جديد را خريده ايد اگر مي خواهيد از سيتم عاملي كه فروشنده نصب كرده استفده بكنيد، حتما قبل از استفاده ويروس يابي كنيد.

**ايميل**

🞏 سرور ايميل را طوري تنظيم كنيد تا ايميل هاي هرزنامه را – كه ممكن است حاوي ويروس يا كد مخرب باشند – حذف كند.

🞏 سرور را به گونه اي تنظيم كنيد كه بلافاصله براي مدير شبكه و كاربر مذكور اخطار امنيتي بفرستد كه پيغام آلوده به ويروس را باز نكند.

🞏 تمامي ايميل هاي وارده و صادره و فايل هاي ضميمه ي آن ها را ويروس يابي كنيد.

🞏 دانلود فايل هاي ضميمه ي غير كاري را در محيط كار ممنوع كنيد.

🞏 به كابران اجازه ندهيد كه جوك يا ايميل هاي زنجيره اي را ارسال كنند.

🞏 از يك سرويس ويروس يابي ايميل (خارج از شبكه) ثبت نام و استفاده نماييد كه حتي الامكان ايميل هاي آلوده وارد شبكه تان نشوند.

🞏 با فرستنده ي ايميل آلوده به ويروس تماس بگيريد يا ايميل بزنيد. چون اغلب ارسال كنندگان از ارسال ايميل آلوده آگاه نيستند.

🞏 يك روش ارتباطي ديگر براي زماني كه سرويس ايميل از كار بيفتد پيش بيني كنيد.

**كاربران**

🞏 روشي براي آموزش همه ي كاربران در باره ي سياست هاي امنيتي (مانند قانون ممنوعيت دانلود) پياده كنيد.

🞏 هر گونه نصب نرم افزار بايد با تأييد بخش انفورماتيك صورت گيرد.

🞏 هر گونه دانلود برنامه هاي تأييد نشده و نصب آن ها (مانند بازي يا اسكرين سيور) توسط كاربران را ممنوع كنيد.

🞏 كاربران را ملزم كنيد كه تحت هيچ شرايطي ديسك (يا هر حافظه ي جانبي) را - كه در خانه استفاده كرده اند – در سازمان استفاده نكنند، 🞏 مگر اين كه پشي از استفاده توسط مسؤول انفورماتيك ويروس يابي و تأييد بشود.

🞏 دسترسي به سايت ها را توسط مرورگر يا پروكسي محدود كرده، فقط به سايت هاي مورد تأييد اجازه دهيد.

🞏 مجموع اي از نرم افزار ها را كه كاربران براي انجام كارهاي خود استفاده مي كنند، تعيين نماييد و اجازه ندهيد نرم افزار ديگري را نصب كنند.

🞏 به كاربراني كه از راه دور به شبكه وصل مي شوند اجازه ي كپي فايل را ندهيد مگر اين كه كامپيوتري كه براي دسترسي از راه دور به كار مي رود توسط بخش انفورماتيك قابل بررسي و كنترل باشد.

**آموزش كاربران**

🞏 لينك هاي مربوط به دائره المعارف هاي ويروس ها را براي آشنايي و استفاده ي كاربران منتشر كنيد:

* Computer Associates <http://www3.ca.com/securityadvisor/virusinfo/browse.aspx>
* F-Secure <http://www.f-secure.com/v-descs/>
* Kaspersky <http://www.viruslist.com/en/viruses/encyclopedia>
* McAfee <http://www.mcafeesecurity.com/us/security/vil.htm>
* Symantec <http://www.symantec.com/avcenter/>
* TechRepublic's Virus Threat Center <http://www.virusthreatcenter.com/library.aspx>
* Trend Micro <http://www.trendmicro.com/vinfo/>

🞏 از كاربران بخواهيد كه در وقت آزاد شان، يا زماني كه متوجه ي آلودگي به ويروس مي شوند يا جهت بيشتر شدن اطلاعات شان در مورد ويروس ها، اين سايت ها را ببينند.

🞏 كاربران را تشويق كنيد كه در كامپيوتر خانه شان ضد ويروس نصب كنند. همني براي كامپيوترهايي كه از راه دور به شبكه تان وصل مي شوند ضد ويروس را الزامي كنيد.

🞏 كاربران را تشويق كنيد كه ايميل ها و فايل هاي مهم شان را در يك سرور كه شما به طور منظم پشتيبان مي گيريد، ذخيره نمايند.

🞏 كابران را تشويق كنيد كه به محض مشاهده ي ويروس روي كامپيوتر شان به شما اطلاع دهند تا بتوانيد تعقيب كنيد كه كدام ويروس ها در شبكه تان ظاهر مي شوند.

🞏 يك سايت اينترانتي يا وب سايت اختصاصي براي ارائه ي اطلاعات در مورد ويروس ها و لينك هاي مربوط به شركت هاي سازنده ي ضد ويروس ايجاد نماييد. در صورتي كه اين مورد را نمي توانيد انجام دهيد يك خبرنامه ي الكترونيكي تهيه كنيد كه همان اطلاعات را به كاربران ارايه دهيد.

🞏 كاربران را از خطرات و ويروس هاي جديد مطلع كنيد تا نسبت به اين موضوع هشيار تر باشند.

🞏 به كاربران تان روش صحيح محافظت از ويروس هاي ماكرو را آموزش دهيد. از آنان بخواهيد تا زماني كه از سالم و مورد تأييد بودن يك فايل مطمئن نشده اند، همه ي ماكرو ها را غير فعال نمايند.

🞏 كاربران خطا كار را جريمه كنيد. بدين ترتيب كه اگر كاربري مقررات وضع شده ي امنيتي را زير پا گذاشت يا ويروسي را وارد محيط كار كرد، بايد براي ويروس يابي دستگاه هاي آلوده شده به بخش انفورماتيك كمك كند.