# افزایش امنیت به میزان ۸۰ درصد



به دليل اين كه هر روز ترفندهاي جديدي براي ويروسي كردن و

هک كردن كاربران شخصي به وجود مي آيد تصميم گرفتم در

اين مقاله مطالبي را ارائه كنم كه باعث افزايش ۸۰ درصدي

كامپيوتر شما شود .

هر روزه شما هدف حمله ها و خطرهاي بيشماري در اينترنت

قرار مي گيريد كه از نظر تعداد مي توان ۹۵ تا از هر صد حمله را

متوقف كرد ولي همين ۵ خطر باعث كاهش امنيت به مقدار ۲۰٪

مي شوند چون اين خطرها توسط افراد عادي و تازه كار نيست و

عاملان آنها در كار خود بسيار تبحر دارند ، در اكثر موارد مي

توانند از تمام مرزهاي امنيتي بگذرند و به طور كامل به مقصود

خود برسند.

۱- استفاده از يک نرم افزار ضد هكر با آخرين به روز رساني ها

كه من **Black ICe** را پيشنهاد مي كنم چون نيازهاي كاربران

حرفه اي و تازه كار را به طور كامل برطرف مي كند.

۲- استفاده از ویروس کشهاي **Norton Anti Virus 2004** و **McaFee** که اگر **Pack** کامل باشد خیلي بهتر است { پک کامل شامل برنامه هاي **FireWall** و **Privacy Policy** و **Anti Spam**مي باشد} توجه داشته باشید که نرم افزارهاي فوق را از سایتهاي اصلي آنها بگیرید و اقدام به خرید آنها نکنید ، چون اکثر شرکتهایي که سي دي هاي آنتي ویروس را جمع آوري مي کنند اصلا به این نکته توجه نمي کنند که این برنامه ها باید از سایت اصلي باشند و در بسیاري از موارد نسخه هاي کرک شده و گاها ویروسي را از سایتهاي غیر قانوني یا به اصطلاح **Warez** مي گیرند و این خود باعث مي شود که برنامه قابلیت هاي خود را از

دست بدهد .

من پيشنهاد مي كنم نسخه هاي نمايشي يا زمان دار اين برنامه ها را دانلود كنيد و سپس با دادن سريال نامبر آنها را رجيستر كنيد.



۳- سطح ايمني و ويروس كشي را در حالت **High** بگذاريد تا تمام فايلها ، با هر پسوندي كه هستند ويروس كشي شوند و توجه داشته باشيد ويروس كش **McaFee** حالتي را با عنوان **Heuristic** دارد، كه به معني اكتشافي است و در اين حالت ويروس كش، به طرز هوشمندانه اي اقدام به ويرس يابي مي كند و توجه داشته باشيد خيلي از فايلهاي ويروسي در اين حالت مشخص مي شوند.

در حقیقت این نوع ویروس ها دو زیست هستند و مرتبا تغییر مي

کنند و از این رو ویروس کش، در حالت عادي نمي تواند آنها را

بیابد.



**4: Service Pack**هاي ویندوز را دانلود کنید و همیشه

ویندوز خود را به روز نگه دارید . البته با سرعت پایین اینترنت در

ایران این کار عملا غیر ممکن است و به همین خاطر شما مي

توانید**Service Pack** هاي ویندوز را از طریق سي دي

خریداري کنید و استفاده از برنامه **Auto patcher XP 4.0**

نیز پیشنهاد مي شود چون این برنامه حاوي اصلاحیه هاي

ماکروسافت براي ویندوز ایکس پي مي باشد.

۵- تنظیمات صحیح خود سیستم عامل و عدم به اشتراک گذاري

فایلها .



این تنظیمات عبارتند از غیر فعال کردن **NetBios** و سرویس

**Remote Assistance**و بستن مسیر ورودي کرم

**MsBlaster** که حفره آن همیشه ممکن است خطر ساز باشد.

۶- عدم استفاده از برنامه هاي به اشتراک گذاري فایل از جمله

**Kazza**که به علت نقص هاي بیشمار و همراه داشتن برنامه هاي

جاسوسي استفاده از آن دیوانگي است.

۷- عدم استفاده از **Internet Explorer.** خیلي از برنامه

هاي جاسوسي و**Trojan** ها فقط در صورتي دانلود و در نتيجه

فعال مي شوند كه صفحه مربوطه توسط **Internet**

**Explorer**باز شود، همچنين خيلي از كرمهاي اينترنتي در

صورت اجرا شدن و باز بودن صفحه اينترنت اكسپلورر گسترش

پيدا مي كنند. پيشنهاد مي كنم از يک مرورگر ديگر به جاي

**Internet Explorer**استفاده كنيد و قابليت هاي **PlugIn** و

**Java Script**آن را نيز غير فعال كنيد .

در اين ميان مرورگرهاي **Opera** و **Mozilla** از همه محبوب

تر و كارآمد تر هستند ولي باز هم **Opera** را به دليل پشتيباني

از زبان فارسي و افزايش سرعت اينترنت و قابليت هاي بيشمار

پيشنهاد مي كنم.

۸- افزايش امنيت **Internet Explorer.**

با همه اين احوال موقعيتي پيش مي آيد كه بايد از مرورگر

استاندارد اينترنت يعني **Internet Explorer** استفاده كنيد به

همين خاطر روش هاي افزايش امنيت **Internet Explorer**

را نيز بيان مي كنم.

**cookie**ها را بعد از قطع شدن از اينترنت پاک كنيد ، البته اگر

مدت طولاني به اينترنت وصل بوده ايد و در وبلاگ يا ايميل خود

وارد شده ايد نيز حتما اين كار را در حين كار با اينترنت نيز بكنيد.

در صورتي كه به محتويات **Temporary Internet Files**

نیز نیاز ندارید آنها را هم پاک کنید، براي انجام این کارها مراخل

زیر را دنبال کنید



**Delete < Option Internet < Internet Explorer**

**Internet Option < Cookie , Internet explorer**

<

**Delete Files... 8.1**:

جلوي کوکي هايي که مي توانند خطرناک باشند را بگيريم. براي

اين کار مراحل زير را طي کنيد و حالت **Medium High** را

انتخاب کنيد **internet Explorer > Internet Option**

**> {tab} Privacy 8.2:** استفاده از برنامه هاي ضد پاپ آپ

براي اينكه خيلي از **PopUp** ها باعث قفل شدن و در نتيجه بسته شدن **IE** مي شوند و حتي مي توانند حاوي كدهاي مخرب و ويروس نيز باشند.بهترين برنامه هايي كه براي اين كار وجود دارد **Zero PopUp**و **AdWare 6.0** است ، البته **Adware** بسيار بهتر است. ۸,۳: پاک کردن و غير فعال کردن ذخيره سازي پسورد توسط **IE** که پسورد وبلاگ و ايميل **Hotmail** از اين جمله مي باشند .

براي انجام اين كار مراحل زير را طي كنيد **Internet Explorer > Internet Option > {tab} Content > Auto Complete**و سپس دكمه **Clear Password** را مي زنيم و بعد از آن تيک گزينه **User Names &**

**Passwords on Forms**را بر مي داريم. صفحاتي كه عكس

يا عكسهاي آنها نمايان نمي شود را **Refresh** نكنيم ، چون اين

يكي از روشهاي آلوده سازي كامپيوتر قرباني به ويروس يا

تروجان است و براي ديدن عكس مذبور روي آن كليك راست

بزنيد و سپس گزينه **Show Picture** را بزنيد .

ممكن است سايتي حتي قسمتهاي ديگرش نيز به درستي باز نشده

باشد در اين صورت نيز **Refresh** نكنيد و آدرس آن سايت را

در صفحه اي جديد وارد كنيد. ٨,٤: استفاده از برنامه هاي ضد

برنامه هاي جاسوسي يا همان **Anti SpyWare** و **Anti**

**AdWare**كه بهترين آنها **Adware 6.0** و **SpyHunter** و

**SpySweeper**مي باشند و آنها را به ترتيب از سايتهاي زير

مي توانيد دانلود كنيد **www.download.com** و

**www.tooto.com** و **www.webattack.com** نكته:



برنامه **AdWare** تنها اشكالي كه دارد اين است كه بايد ابتدا يک

فايل كوچک را دانلود كنيد و بعد از اجراي آن به طور خودكار

برنامه اصلي كه حجم زيادتري دارد دانلود مي شود و شما نمي

توانيد آن را با برنامه هاي افزايش دهنده سرعت دانلود كنيد و

همچنين برنامه اصلي را در اختيار نخواهيد داشت تا بعد از تعويض

ويندوز دوباره آن را نصب كنيد و هر بار كه ويندوز نصب مي

كنيد بايد آن را دوباره دانلود كنيد. نكته۲: برنامه **SpyHunter**

بيشتر به درد كاربران حرفه اي تر مي خورد و خود كاربر بايد

جلوي فايلهايي را كه به اينترنت وصل مي شوند را با شناخت كافي

كه دارد بگيرد ولي اين برنامه خيلي كم حجم قابليت كنترل

**Spyware**ها و كد هاي مخربي كه در خود سايت قرار

دارند {به صورت فايل جداگانه نيستند} و با آن لود مي شوند را

دارد و همه آنها را به طور اتوماتيک **Block** مي كند .

همچنين با كمک اين برنامه مي توانيد جلوي ارسال اطلاعات را كه

توسط هر تروجاني ارسال مي شود را بگيريد و حتي بهترين آنتي

ويروس ها هم ممكن است كه يک تروجان جديد را نشناسند و اين

برنامه از اين نظر بهترين انتخاب است. نكته۳: برنامه

**SpySweeper**يک برنامه بسيار عالي است كه به داعما در حال

بررسي كوكيه ها و ديگر برنامه هاي مخرب احتمالي است و به

طور خودكار كوكي هاي خطرناک را پاک مي كند. اين برنامه

داراي يک سكنر **Spyware** هم هست و شما مثل ويروس كش

ها مي توانيد درايوهاي خود را بررسي كنيد ولي با اين تفاوت كه

اين برنامه به جاي ويروس ، برنامه هاي جاسوسي را پيدا و پاک

مي كند. تنها اشكالش هم اين است كه برنامه **Dap** كه براي

دريافت تبليغات و رجيستر شدن مرتبا به سايتش مراجعه و

اطلاعات ارسال مي كند را به عنوان برنامه جاسوسي مي شناسد و

آن را پاک مي كند.

۹- از چه سايتي برنامه **Download** مي كنيم .ابتدا بايد سايت

مورد نظر را از آدرس فايلي كه براي دانلود وجود دارد را ببينم

**}**مثلا **www.tooto.com/spyhunter.zip** را داريم و

بايد به سايت **www.tooto.com** برويم{ و مطمئن شويم كه

برنامه مربوطه براي همين سايت است و هيچ وقت برنامه ها را از

سايتهاي ثالث نگيريم چون هيچ دليل منطقي براي كار آنها وجود

ندارد و بدون شک برنامه اي كه ما از آنها مي گيريم داراي

ويروس يا تروجان است و اين نكته بايد بسيار مورد توجه

شركتهاي رايت سي دي و سايتهايي باشد كه برنامه براي دانلود

معرفي مي كنند .

معمولا سايتهايي كه برنامه هاي شركتهاي ديگر را براي دانلود مي

گذارند اسم هاي عجيب و غريب و طولاني دارند { اين دو آدرس

را مقايسه كنيد **www.tooto.com/spyhunter.zip, :**

**{www.aktami.cu.ne/pub~/spyhunter.zip**يكي

ديگر از مشخصه هاي سايتهايي كه برنامه هايي كه براي دانلود

گذاشته اند متعلق به خودشان نيست اين است كه آنها ليست هاي

طويلي از برنامه هاي مختلف دارند كه همگي آنها از همان**}**

سايت **Domain{**و بدون توضيح وقسمت **Help** و از اين جور

چيزها براي دانلود وجود دارد و بايد بدانيد سايتي كه برنامه

خودش را براي دانلود گذاشته اولا تعداد محدودي برنامه دارد ،

ثانيا برنامه را همراه **Tutorial** و **Help** و خيلي چيزهاي ديگه

معرفي مي كنه و آدرس درست و حسابي داره ، همچنين در

سايت اصلي برنامه، عكسها و **Screen Shot** هايي از برنامه

مورد نظر وجود دارد. سايتهايي كه آدرس آنها مثل **IP** هست

بسيار خطرناكند و ممكن است **Admin** آن سايت با بدست

آوردن **IP** شما كه از طريق ديدن كردن شما از آن سايت به

دست او مي رسد اقدام به هک كردن شما بكند يا همانطور كه

گفتم برنامه كه در آن سايت براي دانلود قرار گرفته حاوي

ويروس يا تروجان ... باشد. حال ممكن است اين سوال پيش بيايد

كه فلان برنامه داراي محدوديت زماني يا عملكرد است ، و اگر ما

آن برنامه را از اين سايتهاي دانلود نكنيم چگونه مي توانيم

محدوديت آن را از بين ببريم و در جواب سوال شما بايد بگم كه

ابتدا نسخه **Trial** يا **Demo** برنامه را سايت اصلي بگيريد و بعد

از آن كرک آن برنامه را كه حجم خيلي كمي هم دارد را از

سايتهايي كه براي اين منظور مي باشند دريافت كنيد ، البته در

موارد بسيار نادري اتفاق مي افتد كه كرک مربوطه حاوي ويروس

است. ولي احتمال ويروسي شدن توسط آن خيلي كمتر از دريافت

نسخه كامل كرک شده برنامه است و بهتر است از كركهايي كه

شماره سريال در اختی‌ار شما مي گذارند استفاده كنيد و كركهايي

كه به جاي فايل اصلي جايگزين مي شوند خيلي مطمئن نيستند و

حتي ممكن است از قابليت برنامه بكاهند و برنامه انطور كه بايسته

و شايسته است كار نكند.

به سايت هايي كه برنامه ها را كرک مي كنند و آنها را براي

دانلود مي گذارند سايتهاي **Warez** يا غير قانوني مي گويند .

براي پيدا كردن سايت اصلي برنامه بايد در گوگل به اين صورت

جستجو كنيد:



۱۰ - **Official Site + Name Of Program** همیشه به

آيكن و پسوند عكسهايي كه از طريق چت مي گيريد توجه كنيد و

از طرف مقابل بخواهيد كه عكسش را به ای‌می‌ل تان بفرستد

چون خود ياهو داراي **Norton Anti Virus** مي باشد و فايل

قبل از دانلود شدن **Scan** مي شود و فقط در مواردي نادر

ممكن است **Yahoo** ويروسي كه همراه عكس هست را نشناسد

به همين خاطر عكس مربوطه را با ويروس كش **McaFee**

ويروس كشي كنيد

۱۱- از کار انداختن **System Restore .** همانطور که مي دانيد فايلهايي که پسوند هاي سيستمي مثل **dll , exe** و غيره داشته باشند، پس از پاک کردن يا اعمال تغييرات در **System Restore**ذخيره مي شوند و اين مسئله زماني خطر ساز مي شود که يک فايل ويروسي را به صورت دستي يا به کمک برنامه هاي ضد ويروس يا ضد **Spyware** پاک **{Delete}**يا تميز **{Clean}**کرده ايد، ولي غافل از اينکه ويندوز اين فايلها را در جايي ديگر حفظ کرده است و همچنان ويروس به فعاليت خود ادامه مي دهد. براي از کار انداختن **System Restore** مراحل زير را دنبال کنيد **: Control Panel > System >**

**{tab} System Restore > Turn off**

۱۲- **System Restore on All Drive** شاید زیاد اتفاق افتاده باشد که از طریق چت یا از یک سایت مشکوک عکس **Download** کرده باشید و نگرانید که این فایل حاوي تروجان یا ویروس مخصوص فایلهاي **JPG** باشد و به همین خاطر عکس مربوطه را در کافي نت باز کنید و کلید **F11** را بزنید و سپس کلید **Print Screen** را فشار دهید و بعد از آن برنامه **Paint** را باز کنید و **Ctrl + V** را بزنید و حالا مي توانید عکس را با خیال راحت با هر پسوندي ذخیره کنید. شاید بپرسید چرا براي این کار از برنامه هاي **Picture Converator** استفاده نکنیم و در جوابتان باید بگویم که ممکن است در فرایند تبدیل فایل ممکن

است کدهاي ويروس نيز ترجمه شده و همراه عکس **Convert** شده باقي بماند ولي در روش فوق، فرايند تهيه عکس هيچ نيازي به عکس مشکوک به ويروس ندارد .



۱۳- هرگز اسم کامپيوتر **{Computer Name}** خود را واقعي ندهيد. هکرها مي توانند اسم کامپيوتر شما و در نتيجه اسم شما را بيابند و براي جلوگيري از اين کار يک اسم مستعار براي خود انتخاب کنيد. همچنين از وارد کردن اسم و مشخصات واقعي خود در برنامه هايي مثل **Photoshop** و غيره که در زمان نصب از شما اسم و مشخصات مي خواهند نيز خودداري کنيد.



۱٤ - ويروس کش **Panda** را نصب نکنيد چون فايل اصلي

اجرايي آن ويروسي است و توسط ويروس كش معروف **Iris**

شناخته مي شود ولي چون اين ويروس كش ورژن جديد ندارد

كاربران تازه كار با آن اشنايي ندارند ولي كاربراي قديمي مثل

خودم :-) اين ويروس كش را به خوبي مي شناسند. چند وقت پيش

كه مي خواستم اين ويروس كش را دانلود كنم در گوگل سرچ

كردم ولي آن را پيدا نكردم و در عوض به مطلبي بر خوردم مبني

بر اينكه اين ويروس كش ۸۰٪ ويروس هاي ويندوز ۹۵ و ۹۸ را

مي شناسد ولي اين ويروس كش در ويندوز ايكس پي اجرا نمي

شود و ارزشش را دارد كه يک ويندوز ۹۸ نصب كنيد با اين برنامه

يک بار كل هاردتون را **Scan** كنيد و حداق! ل ۲ يا ۳ تا ويروس

پيدا خواهد كرد، البته اين ويروس كش را بايد مثل **Mcafee** در

حالت **Heuristic** قرار دهيد و شناسايي ويروس توسط اين

ويروس كش تا حد زيادي بستگي به تنظيمات صحيح دارد.



شركتي كه سي دي برگ سبز ٤ را توليد كرده ويروس كش **Iris**

را نيز درون اين سي دي **Application Collection** قرار

داده ولي با كمال تاسف اين شركت چون به تنظيمات درست اين

ويروس كش آشنا نبوده يک فايل ويروسي كه در اين سي دي

وجود دارد را شناسايي نكرده و در حال حاظر فايلي كه در اين

شاخه قرار دارد حاوي ويروس است **Amuse > Joke**.به

همين خاطر من فايل تنظيمات اين ويروس كش را ذخيره كردم تا

در اختيار كاربران عزيز قرار دهم ومي توانم آن را از طريق ايميل

براي شما ارسال كنم و به راحتي توسط برنامه آن را **Load** كنيد .



مهمترين و شايد خطرناک ترين ويروسي كه تا كنون توسط هيچ ويروس كشي شناخته نشده است ويروس **Win95.CIH** است كه فقط **Iris** آن را مي شناسد و به شدت توسط سي دي و ديسكت در حال گسترش است و اين ويروس كم كم درون كامپيوتر رخنه مي كند ، تا جايي كه تمام برنامه ها و فايلهاي شما را آلوده مي كند و از دلايلي كه ممكن است شما به وجود ويروس در كامپيوترتان پي نبريد اين است كه فايلهايي كه حاوي اين ويروس هستند از كار نمي افتند و برنامه ها و فايلها كماكان با مشكلاتي اجرا مي شوند و اين خود دليل ديگري است كه كاربران

آن فایل را پاک نمي کنند و حتي آن را به دیگران نیز مي دهند .

بدون اقراق من آ۱ † را در کامپیوتر تمام دوستانم پیدا کردم و از

تمام عزیزاني که این مقاله را مي خانند تقاظا دارم که کامپیوتر

خود را توسط این ویروس کش **Scan** کنند تا این ویروس ریشه

کن شود در آخر هم باید بگم موفقیت یا عدم موفقیت این

ویروس کش بستگي به تنظیمات صحیح دارد.