نگهداری از رایانه

کورش درودگر

مدیریت برنامه ریزی تلفیقی شرکت ملی نفت ایران

k_doroodgar@yahoo.com

چکیده

نگهداری و حفظ کارایی و وضعیت مناسب رایانه به کاربر کمک می کند تا به نحو احسن از رایانه استفاده نماید. علاوه بر دستگاههای دیگر منازل و ادارات که فقط مراقبت فیزیکی نیاز دارند، رایانه ها به مراقبت نرم افزاری نیز نیاز دارند. در این مقاله روشهایی برای نگهداری از رایانه پیشنهاد شده است.

کلمات کلیدی

کارایی رایانه، امنیت اطلاعات، امنیت شبکه، ویروس رایانه ای

مقدمه

رایانه در مقایسه با لوازم خانگی از پیچیدگی بیشتری برخوردار است. نگهداری و حفظ کارایی و جلوگیری از خرابی آن نیز نیاز به دقت و توجه بیشتری دارد.

در این مقاله روشهایی برای محافظت از کامپیوتر برای حفظ کارایی و وضعیت مناسب آن در مدت زیاد و محافظت از سیستم عامل و نرم افزارها و اطلاعات شخصی ارائه شده است. همچنین روشهایی برای جلوگیری از دزدی اطلاعات و افزایش امنیت سیستم در برابر ویروسهای رایانه ای توصیه شده است.

مراقبت فیزیکی

دسته ای از مراقبت های لازم از رایانه عملیاتی است که باعث افزایش طول عمر سخت افزار رایانـه و حفـظ کارایی آن می شود. این موارد عبارتند از:

۱- غبار گیری مرتب رایانه. غبار روی قطعات رایانه می تواند باعث گرفتگی پورتهای ورودی خروجی یا اتصال کوتاه الکتریکی شود. همچنین باعث می شود تهویه سیستم به خوبی انجـام نشـود و فضـای داخلی رایانه داغ شود که برای قطعات الکتریکی آن زیانبار است. برای این کار موقعی که سیم برق دستگاه را از پریز درآورده اید با یک دسـتگاه بـادگیر داخـل کـیس و کلیـه زوایای داخل آنرا تمیز نمایید. همچنین رایانه را در مکان تمیزی قرار دهید. مثلا در یک کارخانه بهتر است رایانه در دفتر مدیریت قرار گیرد و نه کارگاه.

۲- تمیز کردن لوازم جانبی. صفحه کلید رایانه را با بادگیر تمیز نمایید. در صورتیکه مایعی روی آن ریخت رایانه را خاموش نماییـد و صـفحه کلیـد را بـرای مـدتی بصورت وارونه قرار دهید تا خشک شود و سپس اسـتفاده نماییـد. اگـر حرکـت موشواره رایانه نیز با کندی و اختلال صورت گرفـت آنـرا تمیـز نماییـد. صـفحه نمایش را نیز با دستمال نرم مرطوب (آب را مستقیما روی صفحه نمایش نریزید) تمیز کنید.

۳- دور قرار دادن مایعات. در صورت ریختن مایعات روی هر قسمت از رایانه امکان آسیب رسیدن به آن وجود دارد. هیچگونه مایعاتی را در اطراف رایانه و روی کیس قرار ندهید.

۴- مرتب کردن میز کار و سیمهای رابط. مرتب شدن میز رایانه و سیمهای رابط علاوه بـر زیبـا سـازی محیط کـار، کشـش روی پورتهای رایانـه را کاهش می دهد و از خرابی و شکسـتن آن جلـوگیری مـی کند.

۵- خنک نگاه داشتن رایانه. همانطوری که در مورد قبل اشاره شد حرارت برای رایانه مضر است. برای کنترل حرارت تمیز نگاه داشتن رایانه، قرار دادن کیس در سایه و خنک کردن دمای محیطی موثر است. مطمئن شوید که فنهای پردازنده، منبع تغذیه و کیس درست کار می کند. برای لپ تاپ نیز می توان از فنهای خنک کننده استفاده کرد. کیس رایانه را در مکانی قرار دهید که اطراف آن خالی باشد و از تهویه مناسبی برخوردار باشد. گاهی کیس رایانه را با دست لمس نمایید. حرارت آن نباید از دمای اتاق بیشتر باشد و گرنه اشکالی در تهویه آن وجود دارد.

۶- رایانه را به روش صحیح خاموش نمایید. رایانه را بصورت ناگهانی و با قطع برق خاموش نکنید و از روش معمول خاموش کردن توسط سیستم عامل استفاده نمایید. اگر چه به نظر می رسد این مسئله فقط می تواند باعث مشکلات نرم افزاری شود ولی می تواند به قطعات داخلی دستگاه نیز آسیب برساند.

۷- رایانه را بدرستی جابجا نمایید. در صورت حمل نادرست رایانه و وارد شدن ضربه به آن ممکن است به سخت افزار خصوصا دیسک سخت (Hard Disk) آسیب وارد شود.

۸- از محافظ برق استفاده نمایید. نوسانات برق می تواند آسیب جدی به رایانه وارد نماید. استفاده از محافظ برق از وارد شدن شوک به رایانه جلوگیری می نماید. در صورتیکه امکان داشته باشد از UPS استفاده نمایید تا علاوه بر وارد نشدن شوک، در صورت قطع برق رایانه خاموش نشود.

۹- خاموش و روشن نکردن زیاد رایانه. اگر در طول روز از رایانه زیاد استفاده می نمایید آنرا روشن باقی بگذارید زیرا روشن باقی ماندن آن آسیب کمتری از خاموش و روشن کردن پی در پی در بر خواهد داشت. خاموش و روشن شدن باعث سرد و گرم شدن قطعات الکترونیکی رایانه می شود که باعث کاهش عمر آن خواهد شد. در مواقعی که از رایانه استفاده نمی کنید فقط مونیتور را خاموش نمایید تا در مصرف برق صرفه جویی شود.

نگهداری از اطلاعات

با ورود دستگاههای دیجیتال به بازار، زندگی ساده تر شده است. مثلا با آمدن دوربینهای عکاسی دیجیتال تعداد عکسهای

بیشتری توسط مردم گرفته می شود. زیرا عکسبرداری به راحتی صورت می گیرد و هزینه آن نیز کمتر از دوربینهای قدیمی نگاتیوی است. اما دنیای دیجیتال با خود مشکلاتی را به همراه آورد. به سرعت حجم اطلاعات بالا رفت و نگهداری از آن بصورت مشکل بزرگی درآمد. زیرا به همان راحتی که اطلاعات بدست می آمد می توانست از دست برود.

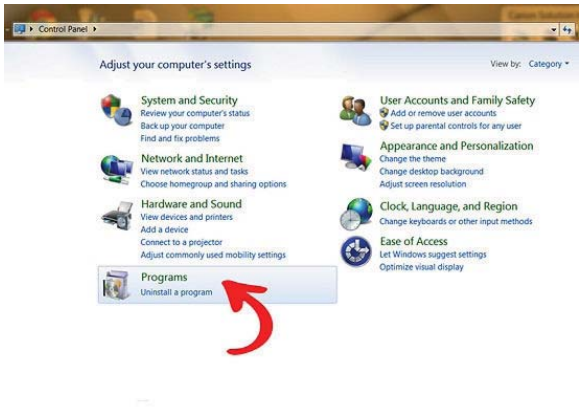
برای جلوگیری از خرابی اطلاعات و از دست رفتن آن موارد زیر پیشنهاد می گردد:

۱- دستگاههای ذخیره سازی اطلاعات مثل دیسکت و هارد دیسک را دور از میدان مغناطیسی قرار دهید. میدان مغناطیسی می تواند اطلاعات را خراب یا نابود کند.
۲- بسته به اهمیت اطلاعات یک یا چند نسخه پشتیبان (backup) از آن در مکان دیگر داشته باشید. معمولا پشتیبان گرفتن از اطلاعات، فراموش شده یا پشت گوش انداخته می شود و موقعی که خرابی اتفاق می افتد تبدیل به فاجعه می شود. بنابرین همین الآن از اطلاعات مهم خود پشتیبان تهیه نمایید.

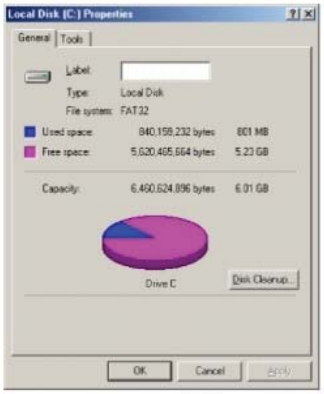
حفظ کارایی سیستم

برای جلوگیری از کند شدن رایانه و حفظ کارایی آن باید ملاحظات زیر را بصورت مرتب در نظر داشت:

۱- برنامه های غیر لازم را پاک کنید. برنامه هایی که نصب می شوند فضایی از دیسک را اشغال می کنند و باعث کندی رایانه شما خواهد شد. همچنین بعضی از نرم افزارهایی که بر روی رایانه نصب می کنید، خود را بصورت startup ثبت می نمایند. این برنامه ها در لحظه شروع سیستم عامل بصورت اتوماتیک اجرا می شوند که باعث کندی بالا آمدن سیستم و اشغال فضای حافظه می شود.



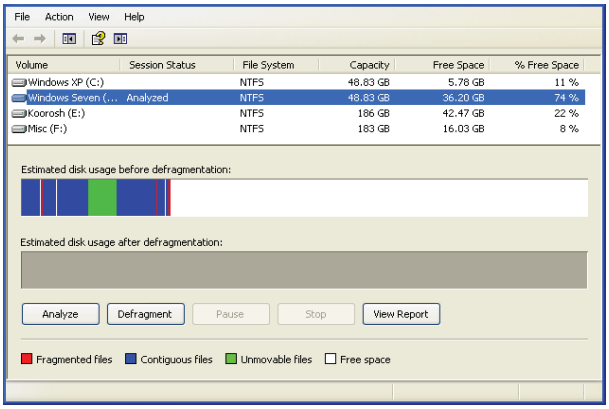
۲- فضای دیسک خود را آزاد بگذارید. سیستم عامل قسمتی از فضای دیسک را برای حافظه اصلی بصورت مجازی استفاده می کند. در صورت پر بودن دیسک خصوصا پارتیشنی که سیستم عامل بر روی آن نصب است، این فضا کم خواهد شد که باعث کندی سیستم عامل شما خواهد شد.



بنابراین سعی کنید فایلهای اضافی را پاک کنید. از طریق Disk Cleanup می توانید فایلهایی که از طریق اینترنت آمده اند یا فایلهای درون Recycle Bin را پاک نمایید.

۳- خرابی دیسک را چک کنید. بوسیله نرم افزارهایی مثل Scandisk دیسک دستگاه را چک کنید که اگر فایلی یا قسمتی از دیسک خراب شده است ترمیم شود.

۴- مرتب کردن فایلها و دیسک. در صورتیکه فایلهای روی دیسک سالم و مرتب باشند، دسترسی به آنها با سرعت بیشتری صورت می گیرد و در نتیجه سرعت سیستم افزایش پیدا می کند. با پاک شدن و کپی فایلها به مرور زمان فایلها تکه تکه شده و توالی خود را روی دیسک از دست می دهند. در این صورت زمان دسترسی به فایلها افزایش پیدا می نماید. برای رفع این مشکل از Disk Defragmenter استفاده نمایید. این نرم افزار تکه های فایل را در کنار هم قرار می دهد.



۵- بروز نگهداشتن نرم افزارها. سیستم عامل و نرم افزارها را به روز نگاه دارید و از طریق اینترنت آخرین تغییرات را اعمال نمایید. این کار باعث می شود آخرین درایورهای سخت افزاری نصب و اشکالات نرم افزارها برطرف شود. این عملیات در مجموع باعث افزایش کارایی سیستم خواهد شد.

۶- ایجاد دیسک راه انداز اضطراری. این دیسک حاوی اطلاعات و فایلهای ضروری برای راه اندازی سیستم در صورت خراب شدن سیستم عامل است.

امکان دیگر ساخت تصویری از کل دیسک بصورت پشتیبان با نرم افزارهای مخصوص (مثل Norton Ghost یا Acronis True Image) است که در صورت خرابی سیستم عامل می توان نسخه قبلی را بازگرداند.

ملاحظات امنیتی

برای اینکه از اطلاعات خود محافظت نماییم و همچنین جلوی نفوذ دیگران را بگیریم و از خرابی رایانه جلوگیری نماییم لازم است موارد زیر را رعایت نماییم:

۱- انتخاب سیستم عامل و نرم افزارها.

سیستم عامل برنامه اصلی هر رایانه ای است که عملیات زیادی چون زمانبندی اجرای برنامه های دیگر، تخصیص حافظه و ایجاد زیر ساخت نرم افزارها را انجام می دهد. بیشتر PC ها از سیستم عامل Windows و رایانه Apple از سیستم عامل Macintosh استفاده می کند.

سیستم عامل Windows به دلیل عمومیت بیشتر مورد حملات امنیتی بیشتری است. زیرا هکرها ترجیح می دهند تعداد بیشتری از رایانه ها را مورد حمله قرار دهند و بنابراین سیستم عاملهای معمول تر را انتخاب می نمایند. بنابرین امنیت بیشتر سیستم عامل Linux نسبت به Windows به خاطر قدرت بیشتر آن نیست و تنها به دلیل عمومیت کمتر است. تنها سیستم عاملی که تاکنون مورد حمله قرار نگرفته است سیستم عاملی است که هنوز به بازار نیامده است. بنابرین انتخاب سیستم عامل با عمومیت کمتر خطرات کمتری دارد.

در هر صورت و با انتخاب هر سیستم عاملی، مهم است که آنرا به روز نگاه دارید. سیستم عامل ویندوز حداقل ماهی یکبار بروز می شوند ولی سیستم عاملهای دیگر کمتر بروز می شوند. خوب است که آپدیت سیستم عامل خود را بصورت اتوماتیک درآورید تا همواره به روز بماند.

اگر چه سیستم عامل پاشنه آشیل امنیت سیستم است ولی نرم افزارهای دیگر نیز امنیت سیستم را به مخاطره می اندازند. از آن جمله مرورگر اینترنت است. مرورگر Mozilla Firefox بسته های امنیتی خود را سریعتر از Internet Explorer ارائه می نماید. همچنین به دلیل Open Source بودن آن به متخصصان امنیت شبکه امکان می دهد نقاط ضعف آنرا سریعتر پیدا نمایند. از مزایای دیگر Firefox امکان Add-Ons آن است که آنرا تقویت می نماید. سه Add-Ons امنیتی که پیشنهاد می شود عبارتند از: NoScript، Better Privacy و HTTPS Everywhere.

NoScript جلوی اجرای برنامه ها از نوع Java، JavaScript، Flash ، Silverlight و غیره را بصورت خودکار می گیرد و از کاربر پرسش می نماید. کاربر می تواند با یک کلیک اجازه دهد یا جلوگیری نماید. بعضی از ویروسها از این طریق با رویت یک سایت بدون اینکه کاربر متوجه شود به رایانه منتقل می شوند.

Better Privacy به کاربر کمک می کند تا بتواند flash cookie ها را پاک کند. Cookie ها با مراجعه به سایتها برای ثبت وضعیت ایجاد می شوند و به راحتی با پاک کردن History قابل پاک شدن هستند. Flash Cookie (Super Cookie) نوعی Cookie است که پایدارترند و به راحتی قابل پاک شدن نیستند.

HTTPS Everywhere باعث می شود در رویت صفحات وب از پروتکل HTTPS استفاده شود (البته برای سایتهایی که این پروتکل را پشتیبانی می کنند). این پروتکل برای رمز کردن ارتباطات اینترنتی است و مسیر امنی ایجاد می نماید که از دزدیده شدن اطلاعاتی نظیر نام کاربری و رمز عبور و صفحات رویت شده جلوگیری می نماید.

برای امنیت بیشتر مرورگر خود دستورالعملهایی وجود دارد که می توانید با مراجعه به آدرس www.us-cert.gov/reading_room/securing_browser/ مطالعه نمایید.

نرم افزارهای رایج دیگر مثل Adobe Acrobat Reader که برای رویت مستنداتی به فرمت pdf کاربرد دارد نیز دریچه ای برای نفوذ خرابکاران است. خیلی از متخصصین امنیت استفاده از نرم افزارهایی که از عمومیت کمتری برخوردارند مثل Foxit PDF Reader را توصیه می کنند.

همچنین توصیه می شود آخرین نسخه Flash Player را نصب نمایید. آخرین آپدیتها را می توانید از آدرس http://get.adobe.com/flashplayer/ تهیه نمایید.

Java نیز یکی دیگر از دریچه های نفوذی است که توصیه می شود نصب نکنید یا آنرا غیر فعال نمایید. روش غیر فعال کردن آن را می توانید در آدرس زیر پیدا کنید.

http://www.infoworld.com/t/web-browsers/how-disable-java-in-your-browsers-210882

۲- جلوگیری از ورود ویروسهای رایانه ای

ویروسهای رایانه ای برنامه هایی هستند که خود را با کپی کردن تکثیر می نمایند و فایلها و نواحی سیستمی را آلوده می نمایند. بعضی از آنها بدون خطر هستند و فقط خود را روی فایلهای دیگر و رایانه های دیگر تکثیر می کنند ولی بعضی از آنها اطلاعات شما را می دزدند، فایلها را خراب می کنند، سرعت سیستم را کاهش می دهند یا باعث هنگ کردن سیستم می شوند.

نرم افزارهای آنتی ویروس برای جلوگیری از ورود ویروس و در بعضی مواقع از بین بردن ویروسهایی که به رایانه وارد شده اند طراحی شده اند. این برنامه ها به دنبال الگوهایی می گردند که نشانگر آلودگی به ویروس خاصی است. به این الگو و رفتار امضاء ویروس می گویند.

بدلیل اینکه هر روزه ویروسهای جدیدی به دنیا عرضه می شود، لازم است آنتی ویروس شما مرتبا به روز شود تا از امضاء این ویروسها نیز مطلع گردد. بنابرین نصب آنتی ویروس کفایت نمی کند و به روز شدن آن نیز مهم است.

البته باید توجه داشت که در یک زمان نباید ۲ آنتی ویروس روی سیستم داشت. اینکار ممکن است باعث اختلال شود و سرعت سیستم را به شدت کاهش دهد.

۳- خطر برنامه های اشتراک فایل peer-to-peer

نرم افزارهای اشتراک فایل مستقیم به کاربران امکان می دهد فایلهای خود را روی شبکه به اشتراک بگذارند. این شبکه اشتراک روی رایانه هایی که همگی این نرم افزار را نصب کرده اند کار می کند. در حالیکه شما از منابع وسیعی و ارزشمندی از اطلاعات استفاده می کنید، این خطر وجود دارد که از طریق این گونه نرم افزارها ویروس به رایانه شما منتقل شود یا حتی کاربران به کلیه اطلاعات دیسک شما دسترسی پیدا نمایند.

۴- احتیاط در استفاده از اینترنت

الف) مراقب کلیکهای خود باشید. روی هر لینکی کلیک نکنید زیرا بعضی از سایتها مربوط به هکرها هستند و با وارد شدن به آنها رایانه شما آلوده خواهد شد. اگر پنجره ای (pop-up box) باز شد و حاوی پیغام هشدار یا تبلیغات بود روی آن کلیک نکنید. سایتهایی که نرم افزارهای کپی ارائه می کنند یا حاوی اطلاعات غیر اخلاقی هستند معمولا مرتبط با هکرها است و خطرناک است.

ب) مراقب دانلودهای خود باشید. دانلودهای غیر ضروری انجام ندهید و فقط از سایتهایی که اعتماد دارید دانلود کنید. بسیاری از فایلهای اجرایی که در اینترنت یافت می شوند آلوده به ویروس هستند.

پ) مراقب Spam ها باشید. به ایمیلهای دریافتی ناخواسته از افراد ناشناس spam گویند. روزانه در جهان میلیونها spam برای افراد مختلف فرستاده می شود که حاوی پیامهای تبلیغاتی یا صفحاتی برای فاش کردن اطلاعات شخصی به منظور تخریب یا دزدیدن اطلاعات است. بهترین کار برای مراقبت از اینگونه حمله، باز نکردن این ایمیلهاست. نرم افزارهای ایمیل نیز دارای فیلتر spam هستند و سایتهای ایمیل مثل yahoo و gmail نیز دارای فیلتر هستند و مرتبا به روز می شوند.

Spear phishing نیز از انواع این حمله است که در آن ایمیل دریافتی از افراد آشنای شما است. بنابراین جلوگیری از اینگونه حملات دشوارتر است. معمولا این ایمیلها حاوی پیشنهادهای اغوا کننده ای می باشد که شما را به باز کردن آن تحریک می کند.

در اینگونه ایمیل ها ممکن است اطلاعات account ایمیل یا شماره کارت اعتباری شما را تقاضا نمایند و با گرفتن آن از آن سوء استفاده نمایند. هیچگاه اینگونه اطلاعات را در سایتهایی که با دنبال کردن لینک باز می شوند وارد نکنید. اگر از سایتی مطمئن نیستید، می توانید بار اول رمز ورود را اشتباه وارد کنید اگر سایت معتبر نباشد آنرا می پذیرد.

ت) مراقب حملات مهندسی اجتماعی باشید. این گونه حملات با شناخت روانشناختی و اجتماعی سعی می کنند اطلاعات شما را بدزدند. مثلا ممکن است شما را مجاب کنند که برنامه ای را روی سیستم خود نصب نمایید و از آن طریق به اطلاعات شخصی شما دسترسی پیدا کنند. این کار از طریق باز شدن پنجره popup و دعوت به تماشای ویدئو یا باز کردن فایل می باشد و با یک کلیک روی لینک کار تمام است. گاهی پنجره ای باز می شود و نشان می دهد چک ویروس در حال انجام شدن است و سیستم شما آلوده به ویروس است و دعوت می کند برای خلاصی از ویروس ابزاری را دانلود کنید. روش دیگر نمایش یک ویدئو و دعوت برای نصب یک plugin برای امکان پخش اینگونه ویدئوها است.

برای جلوگیری از این نوع حملات pop-up blocker مرورگر اینترنت را غیر فعال کنید تا اینگونه پنجره ها بصورت اتوماتیک راه اندازی نشوند. همچنین در صورتیکه پنجره ای باز شد آنرا با علامت X سمت راست بالای پنجره ببندید و نه با کلیدی که داخل پنجره پیشنهاد شده است.

ث) فایلهای مهم خود را کد گذاری کنید. همواره حتی با وجود رعایت همه نکات امنیتی امکان هک شدن یا دزدیده شدن رایانه وجود دارد. برای جلوگیری از سوء استفاده از اطلاعات مهم می توان آنها را کد گذاری کرد. در این صورت فایلها فقط با یک رمز ورود باز خواهد شد و افرادی که رمز را نداشته باشند قادر به استفاده از فایل نیستند. در بعضی از سیستم عاملها امکان کد کردن فایلها وجود دارد و در غیر اینصورت می توان از نرم افزارهای جانبی (مانند TrueCrypt) به این منظور استفاده کرد.

ج) مراقب سایتهای تقلبی باشید. بعضی از افراد، سایتهای جستجو مانند google را بازی می دهند تا در لیست جستجو و یا در ابتدای لیست قرار گیرند. معمولا اینگونه سایتها بدلیل کلیک زیاد مورد هدف هکرها قرار گرفته و آلوده به ویروس هستند. قبل از کلیک روی لینکهای یافت شده در سایتهای جستجو، خلاصه لینک را بخوانید تا از درستی سایت اطلاع حاصل نمایید.

چ) مراقب اطلاعات شخصی خود باشید. هیچگاه اطلاعات شخصی و محرمانه را با ایمیل ارسال نکنید و در سایتها وارد نکنید.

ح) با دقت تایپ کنید. گاهی هکرها سایتهایی مشابه سایتهای معروف ایجاد می کنند. موقعی که آدرس سایتی را وارد می کنید، دقت نمایید که اشتباهی رخ ندهد. همینطور آدرس لینکهایی که کلیک می نمایید را مطمئن شوید که درست است. خصوصا در مورد سایتهای حساس مانند بانکها مطمئن شوید که آدرس سایت درست است.

۵- مراقبت از هک شدن

نفوذ بیگانگان در رایانه شما به دلیل دزدی اطلاعات یا خرابکاری هک نامیده می شود. هکرها هر روز در تلاشند تا حفره های امنیتی جدیدی را برای نفوذ در رایانه ها بیابند. برای جلوگیری از هک شدن سعی کنید نرم افزارها و سیستم عامل خود را به روز نگاه دارید تا حفره های امنیتی را کاهش دهد. به این منظور آخرین نسخه نرم افزارها را نصب نمایید و آنها را مرتبا از طریق اینترنت آپدیت نمایید.

نصب یک دیواره آتش (Firewall) نیز می تواند از خطرات نفوذ جلوگیری نماید. این نرم افزار جلوی برقراری ارتباط از اینترنت به رایانه شما را می گیرد. هر رایانه ای که به اینترنت متصل می شود باید از Firewall استفاده نماید. انواع نرم افزاری و سخت افزاری آن وجود دارد و می توان برای اطمینان بیشتر از هر دو بصورت همزمان استفاده کرد ولی نباید از دو Firewall نرم افزاری همزمان استفاده نمود. در بعضی از سیستم عاملها بصورت پیش فرض Firewall وجود دارد ولی می توان آنرا غیر فعال کرد و نرم افزارهای دیگر نصب کرد.

یکی از روشهای جلوگیری از نفوذ به رایانه شما استفاده از کاربری از سیستم با حداقل دسترسی است. هیچگاه با کاربری با دسترسی administrator وارد نشوید زیرا در صورت نفوذ بیگانگان امکان نصب برنامه و هر گونه تخریبی روی همه امکانات سیستم که در اختیار admin سیستم است، وجود خواهد داشت.

همواره سعی کنید از رمز ورود قوی استفاده نمایید. بعضی از اطلاعات شخصی مانند ایمیل، فایلهای رمز شده، بانکهای اطلاعاتی و کارتهای اعتباری متصل به رمز عبور شماست. بنابرین سعی کنید رمز عبور مشکلی (شامل حروف کوچک و بزرگ و اعداد و علامات) استفاده نمایید و هر از چند گاهی آنرا تغییر دهید. همچنین رمز ورود خود را به کسی ندهید و جایی یادداشت نکنید زیرا ممکن است به دست کسی بیافتد.

بعضی از هکرها رمز ورود ایمیلها را بدست آورده و آنرا تغییر می دهند و از دست شما خارج می کنند. شما می توانید از طریق ایمیل ثانویه و پاسخ به پرسشهای امنیتی رمز ورود را تغییر دهید و ایمیل را بازیابی کنید. بنابرین حتما پرسشها و پاسخهای امنیتی را جدی بگیرید و برای ایمیل خود تعریف کنید و پرسش و پاسخهایی انتخاب نمایید که قابل حدس زدن نباشد.

ضمنا برای جلوگیری از ورود ویروس و نفوذ هکرها می توانید موقعی که نیازی به اینترنت ندارید رایانه را از اینترنت قطع کنید یا رایانه را خاموش نمایید.

۶- امحاء صحیح رایانه

اگر قصد فروش، هدیه یا دور انداختن رایانه خود را دارید، کارهایی را باید برای مطمئن شدن از اینکه ردی از اطلاعات شما در رایانه وجود نداشته باشد، انجام دهید. وقتی فایلی را پاک می کنید، در واقع محتویات آن پاک نمی شود و فقط علامتی برای آن زده می شود که دیگر وجود ندارد. بنابراین امکان بازگشت آن فایل با نرم افزارهای recovery هست.

برای اینکه مطمئن شوید که فایلها قابل بازگشت نیستند باید از نرم افزارهای مخصوصی برای خراب کردن آن استفاده نمایید (نرم افزارهایی مثل Eraser و KillDisk). حتی با فرمت کردن دیسک نیز امکان بازگشت اطلاعات وجود دارد و از آن بدتر حتی از دیسکی که اطلاعات جدیدی روی آن ریخته شده است نیز امکان بازگشت فایلها توسط هکرهای حرفه ای وجود دارد.

۷- امنیت استفاده از شبکه بی سیم (Wireless)

در حال حاضر استفاده از شبکه بی سیم بدلیل سهولت اتصال و بدون نیاز به سیم کشی افزایش یافته است. این نوع ارتباط برای اتصال رایانه ها، چاپگرها و سایر لوازم جانبی در شبکه داخلی شرکتها و ادارات و اتصال اینترنت خانه ها استفاده می شود. همچنین در بسیاری از مکانهایی مثل مدرسه، دانشگاه، کتابخانه، کافه، رستوران، فرودگاه و هتلها دسترسی اینترنت از طریق بی سیم فراهم است.

برای ورود به شبکه داخلی نیاز به ارتباط فیزیکی از طریق سیم نیست و از خارج ساختمان نیز می توان به شبکه وارد شد. تنظیمات اولیه این دستگاه های بی سیم به صورتی است که امکانات امنیتی خاموش است تا ارتباط به سهولت برقرار شود ولی ورود به این شبکه برای خرابکاران بسیار راحت است. این دستگاهها دارای مقدار اولیه اسم شبکه (SSID) و نام کاربری و رمز ورود مدیر شبکه مشخصی هستند. در صورتیکه اینها در موقع نصب عوض نشوند، به راحتی قابل استفاده برای هکرها خواهد بود.

دستگاههای بی سیم برای برقراری ارتباط امن از پروتکلهایی استفاده می کنند. پروتکل WEP که روشی قدیمی است مناسب نیست و به راحتی قابل هک شدن است در حالیکه پروتکل WPA2 قوی تر است و توصیه می شود از این روش امنیتی استفاده شود.

در ضمن اگر با رایانه خود به نقاط بی سیم رایگان متصل می شوید ممکن است سیستم شما در معرض خطر قرار گیرد زیرا این شبکه ها معمولا نا امن هستند و ممکن است به راحتی مورد حمله هکرها و ویروسها قرار گیرد.

خطراتی که در اینگونه شبکه ها وجود دارند ۳ دسته هستند:

الف) حمله فرد در میان (Man in the Middle) که در آن مراودات بین شبکه و رایانه شما شنیده شده و فرد خود را به عنوان شما جا می زند و حقوق دسترسی شما را استفاده می کند.

ب) استراق سمع (Eavesdropping) که در آن اطلاعاتی که رد و بدل می شود را می دزدد. این کار با نرم افزارهای sniffer انجام می شود. این نرم افزارها می توانند بسته های اطلاعاتی شبکه را گرفته و اطلاعات آنرا استخراج نماید. این اطلاعات می تواند حتی شامل شماره و رمز کارت اعتباری شما باشد.

ج) نگاه کردن از بالای شانه که در این روش هکر فقط نظاره گر کارهایی می شود که شما انجام می دهید.

برای جلوگیری از سوء استفاده از اطلاعات شما باید مواقعی که از شبکه بی سیم استفاده نمی کنید آنرا در رایانه خود خاموش نمایید. در ضمن حالت اتصال اتوماتیک به بی سیم را روی رایانه خود خاموش کنید تا بدون اطلاع شما به شبکه ناشناس وارد نشود.

همچنین غیر فعال کردن اشتراک گذاری فایلها (File Sharing) تا حدودی جلوی دسترسی هکرها به فایلهای شما را می گیرد.

استفاده از VPN معتبر نیز می تواند امنیت اطلاعات شما را افزایش دهد. این نوع ارتباط در واقع ایجاد شبکه امن روی یک شبکه نا امن است. در شبکه VPN اطلاعاتی که رد و بدل می شود کدگذاری می شود و برای دیگران غیر قابل استفاده می شود.

مواقعی که از طریق اینترنت ایمیل خود را چک می کنید یا عملیات حساسی مثل کارهای بانکی انجام می دهید، از ارتباط امن استفاده کنید. به این منظور در قسمت آدرس سایت به جای http از https استفاده نمایید. این کار باعث استفاده از پروتکل امن SSL می شود و مشروط بر این است که

سایت مورد رویت این سرویس را پشتیبانی نماید. در این نوع ارتباط اطلاعات بصورت کد گذاری شده ردو بدل می شوند.

نتیجه گیری

رایانه ها هر روز در خطر خراب شدن، پاک شدن اطلاعات، دزدیده شدن اطلاعات و کم شده کارایی هستند. با استفاده از دستورالعمل ذکر شده در این مقاله می توان بر طول عمر رایانه افزود و از اطلاعات خود محافظت کرد.

مراجع

1) Maintaining Your Computer
http://support.gateway.com/s/manlib/notebooks/solo1150/8507028/maintain.htm

2) Maintaining Your Computer [Tim Fisher]
http://pcsupport.about.com/od/maintenance/u/maintain_your_computer.htm

3) 26 Tips to Keep Your Computer Up and Functioning [Reginald Adkins]
http://www.lifehack.org/articles/lifehack/26-tips-to-keep-your-computer-up-and-functioning.html

4) Troubleshooting & Maintaining Your PC All-in-One For Dummies [Dan Gookin]
http://www.dummies.com/how-to/content/troubleshooting-maintaining-your-pc-allinone-for-d.html

5) Top 10 things you should be doing to maintain your computer [Melissa Hermanson, 2008]
http://www.pugetsystems.com/labs/articles/Top-10-things-you-should-be-doing-to-maintain-your-computer-39

6) 5 Ways to Maintain Your Computer [whizkid, 2010]
http://pcwhiz.com/5-ways-maintain-your-computer

7) Tips on Maintaining Your Computer [2012]
http://www.support.com/blog/post/tips-maintaining-your-computer

8) How to Maintain Computers in an Organization [Linda Ray]
http://smallbusiness.chron.com/maintain-computers-organization-40391.html

9) Securing Your Computer to Maintain Your Privacy [2012]
https://www.privacyrights.org/fs/fs36-securing-computer-privacy.htm

10) How to Maintain a Computer System?
http://www.directron.com/howtomainsys.html

11) How to Properly Maintain Computer Hardware [Alex, 2013]
http://www.geo-win.com/how-to-properly-maintain-computer-hardware

12) How to Maintain a Healthy Computer

http://www.Hotweazel.com

13) How to maintain your computer safe and clean [Sehoon (Sean) Ahn, 2008]

14) Best practices for computer security [Sehoon (Sean) Ahn, 2008]
http://kb.iu.edu/data/akln.html

15) http://www.edge-online.org/tips-on-maintaining-computer-hardware-properly
16) http://www.wikihow.com/Maintain-Your-Computer

17) http://internet-security-suite-review.toptenreviews.com