درک مفاهیم سیستم عامل



احتمالاً پیش از این اصطلاح سیستم‌عامل را شنیده‌اید، اما ممکن است در مورد معنی دقیق آن اطمینان نداشته باشید.

اصولاً سیستم‌عامل نرم‌افزاری است که چگونگی تعامل کاربر و کامپیوتر را مدیریت می‌کند.

این نرم‌افزار چگونگی استفاده و دسترسی نرم‌افزارها به سخت‌افزارها را تحت نظر داشته و در مجموع نقش اصلی را در عملکرد کامپیوتر بر عهده دارد.

می‌توان سیستم‌عامل را به عنوان برنامه اصلی کامپیوتر در نظر گرفت که این برنامه، دیگر برنامه‌های موجود روی کامپیوتر را اجرا و مدیریت می‌نماید.

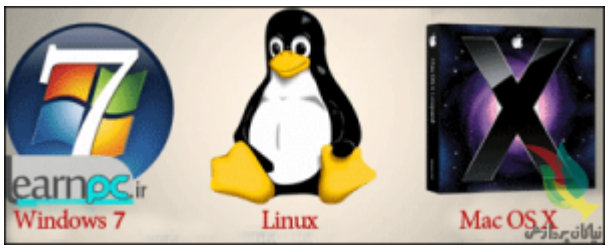
در واقع سیستم‌عامل، ستون فقرات کامپیوتر و مهمترین برنامه‌ی کامپیوتر می‌باشد، چرا که همه‌ی امور مربوط به کامپیوتر را کنترل می‌کند.

این امور شامل: اختصاص حافظه به برنامه‌ها، کپی کردن فایل‌ها از یک درایو به درایو دیگر و در کل مدیریت فایل‌ها، دریافت دستورات از طریق ماوس و صفحه کلید و سایر دستگاه‌های جانبی، ارسال دستور به دستگاه‌های جانبی، اعلام زمان و تاریخ و غیره می‌شود.

بدون سیستم‌عامل نمی‌توان از کامپیوتر استفاده نمود. معمولاً از قبل یک سیستم‌عامل بر روی کامپیوتر نصب می‌شود، اما اگر چند سال از خرید کامپیوتر شما گذشته باشد، ممکن است تمایل به ارتقاء سیستم‌عامل به آخرین نسخه ارائه شده توسط شرکت سازنده را داشته باشید.

سیستم‌عامل‌های متنوعی در بازار وجود دارد، پرطرفدارترین سیستم‌عامل

در کامپیوترهای شخصی، ویندوز است. در حال حاضر، آخرین نسخه‌ی ویندوز، ویندوز ۷ می‌باشد.در سیستم‌عامل MAC، جدیدترین سیستم‌عامل MAC OS 10 نام دارد و البته آخرین نسخه، ۱۰٫۶ snow leopard است.



این دو سیستم‌عامل، مشهورترین سیستم‌عامل‌ها می‌باشند. احتمالاً نام Linux را نیز شنیده‌اید، Linux نیز یکی دیگر از سیستم‌عامل‌های پرطرفدار است.

عموماً هر کامپیوتر یا دستگاهی که برنامه‌هایی بر روی آن اجرا می‌شوند، دارای سیستم‌عامل می‌باشد.

کنسول‌های بازی مانند Xbox ،V وPS3، همگی دارای سیستم‌عامل می‌باشد. تلفن‌های همراه نیز، سیستم‌عامل دارند.

علاوه بر مدیریت کامپیوتر و برنامه‌های آن که هدف اصلی سیستم‌عامل می‌باشد، اکثر سیستم‌عامل‌ها مانند ویندوز و مک، دارای برنامه‌هایی به صورت Built-in می‌باشد.این برنامه‌ها با نام‌های Applications، Programs، Apps و Softwares نیز شناخته می‌شوند.

این برنامه‌ها می‌توانند برنامه‌های ساده‌ی واژه‌پرداز، برنامه‌هایی برای مدیریت عکس‌ها، برنامه‌هایی برای دریافت و ارسال ایمیل و مانند آن‌ها باشند.

در بعضی موارد می‌توان بر برنامه‌های موجود در سیستم‌عامل، برنامه‌های دیگری نیز نصب کرد.

به عنوان مثال، هردو سیستم‌عامل ویندوز و مک دارای نرم‌افزارهای مرورگر وب به صورت Built-in می‌باشد. اما کاربر می‌تواند برنامه‌های ساخته شده توسط شرکت‌های دیگر را نیز مورد استفاده قرار دهد.



بعضی برنامه‌ها را می‌توان از سایت شرکت سازنده به صورت رایگان دانلود نمود. اما بعضی دیگر باید خریداری شوند. این مسئله به برنامه‌ی مورد نظر بستگی دارد.

نکته‌ای که در این مبحث وجود دارد این است که همواره باید مراقب باشید که نسخه‌ای از برنامه را دانلود و یا خریداری نمایید که مخصوص سیستم‌عامل شما ساخته شده باشد.

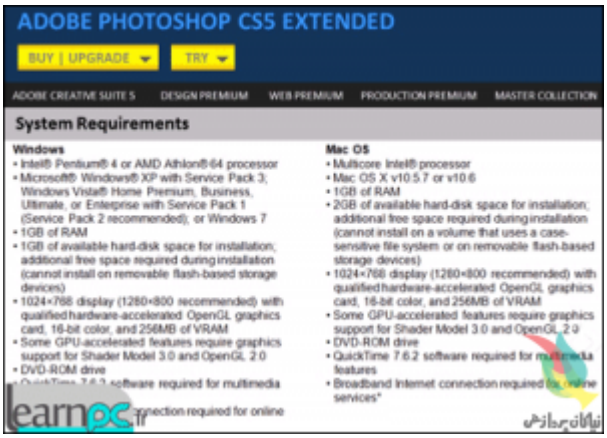
به عنوان مثال اگر سیستم‌عامل کامپیوتر شما ویندوز است، باید از برنامه‌های ویندوز استفاده نمود. و اگر از سیستم‌عامل مک استفاده می‌کنید مجبور به نصب آن نسخه‌ای خواهید بود که با مک هماهنگ باشد.

در بسیاری از موارد تولیدکنندگان نرم‌افزار، دو نسخه از محصولات خود را منتشر می‌نمایند که یکی مخصوص ویندوز و دیگری مخصوص مک می‌باشد. البته نرم‌افزارهای زیادی نیز تنها با یکی از سیستم‌عامل‌ها هماهنگ‌اند.



چه نرم‌افزار را دانلود کرده و چه از فروشگاه خریداری کرده باشید، بخشی به نام system requirements یا سیستم مورد نیاز را مشاهده خواهید کرد.

در این بخش سیستم‌عامل و حداقل قطعات مورد نیاز مانند CPU، RAM ، فضای روی هارد دیسک و غیره برای اجرای برنامه دیده می‌شود.



به این ترتیب می‌توانید به توجه به نیازمندی‌های نرم‌افزارهای مختلف، نرم‌افزار مورد نظر را انتخاب کنید.

مقایسه کامپیوترهای Laptop و Desktop



درهنگام انتخاب و خرید کامپیوتر، یکی از اولین تصمیماتی که باید بگیرید، انتخاب بین کامپیوترهای Desktop یا رومیزی و Laptop یا نوت بوک می‌باشد، شما در تصویر زیر نمونه‌ای از این کامپیوترهای را مشاهده می‌کنید.



لپ تاپ ها نوت بوک نیز نامیده می‌شوند، این کامپیوتر ها با قابلیت حمل و نقل طراحی شده‌اند لذا اغلب وزنی کم‌تر از دو یا سه کیلوگرم دارند، همچنین مانیتور، صفحه کلید و موس به طول Built-in در آن‌ها وجود دارد، بنابراین برای استفاده از Laptop نیز نیازی به اتصال به ابزارهای جانبی وجود ندارد،

هنگامی که از کامپیوتر صحبت می‌کنید واژه Desktop یا رومیزی می‌تواند معانی متفاوتی داشته باشد.

اما در این مورد واژه‌ی Desktop به کامپیوترهایی اشاره دارد که روی میز محل کار یا در کنار آن قرار می‌گیرد، این کامپیوتر مانیتور، صفحه کلید و موس Buit-in ندارد، اما معمولاً این قطعات به هنگام خرید درون جعبه کامپیوتر قرار دارد، پیش از راه‌اندازی کامپیوتر این قطعات باید به کیس اصلی متصل شود، کامپیوترهای Desktop برای جابه‌جا شدن طراحی نشده‌اند، چنانچه واقعاً قابلیت حمل و نقل برای شما اهمیت دارد، بهتر است یک Laptop خریداری کنید، امروزه Laptopها به قدرتمندی رقبای رومیزی خود نیستند، برای اینکه لپ‌تاپی به قدرتمندی Desktop خریداری کنید باید پول بیشتری بپردازید، کامپیوترهای Desktop این مزیت بزرگ را دارا می‌باشند که به راحتی قابل ارتقا هستند، می‌توان از پورت USB برای اضافه کردن هارد دیسک‌های اکسترنال به لپ تاپ‌ها استفاده نمود. اما Desktopها علاوه بر پورت‌های USB بیشتر دارای اسلات‌های داخلی برای افزودن انواع Expansion Card یا هارد درایوهای داخلی یا اینترنال و یا درایوهای نوری می‌باشند.

چنانچه قصد دارید از کامپیوتر بیشتر در محیط خانه یا محل کار استفاده نموده و یا نیازی به جابه‌جا کردن آن ندارید، می‌توانید مانیتور بزرگتری نیز انتخاب نمایید، مانیتوری که از مانیتور لپ تاپ بسیار بزرگ‌تر باشد، بزرگ‌ترین مانیتور لپ تاپ نهایتاً به ۱۹ اینچ می‌رسد، ا□:/□. ا می‌توان مانیتوری با اندازه‌های ۲۳، ۲۷ و ۳۰اینچ و یا حتی بزرگ‌تر از مانیتورهای Desktop نیز انتخاب کرد.

البته امروزه اکثر لپ‌تاپ‌ها قابلیت اتصال با مانیتورهای دیگر را نیز دارند، اما همچنان قیمت لپ‌تاپ‌ها بالاتر است، بنابراین اگر واقعاً به قابلیت حمل و نقل کامپیوتر نیازی ندارید بهتر است یک کامپیوتر Desktop خریداری نمایید.

خاموش کردن فایروال در ویندوز xp



در این پست آموزش تصویری **خاموش کردن فایروال در ویندوز ایکس پی** (xp) را برایتان آماده کرده ایم. روشن بودن این دیواره امنیتی نه چندان قدرتمند علاوه بر مشکلاتی که میتواند در بحث شبکه های کامپیوتری به وجود آورد میتواند بر اتصال اینترنت سیستم و حتی بعضا کاهش سرعت اینترنت تاثیر گذار باشد و از طرفی در صورتی که روی کامپیوتر شما آنتی ویروس وجود داشته باشد (که البته ضروری است وجود داشته باشد) روشن بودن FireWall ویندوز دیگر معنی ندارد. با این تفاسیر در ادامه مطلب با ما باشید تا فایر وال پیش فرض ویندوز ایکس پی را غیر فعال نماییم.

خاموش کردن فایروال :



برای خاموش کردن فایروال ابتدا وارد کنترل پنل شوید؛ (**آموزش وارد شدن به کنترل پنل**) و روی گزینه **Windows Firewall** راست کلیک کرده و روی گزینه open کلیک کنید، (میتوانید روی این گزینه **دابل کلیک** کنید)

در مرحله بعد **پنجره تنظیمات فایروال** را خواهید دید، off – not recommended را بگذارید برای این کار کافیست داخل دایره ای که در کنار متن مشخص شده کلیک کنید.

کار تمام است، حالا با کلیک کردن روی گزینه ok این پنجره بسته میشود و شما **فایروال ویندوز** را خاموش کرده اید، برای روشن کردن دوباره دیواره آتش کافیست تیک کنار گزینه on – recommended را فعال کنید.

انواع کامپیوتر



PC یا Personal computerها، کامپیوترهای معمولی هستند و با مشخصات مختلفی ارائه می‌شوند.

Laptopها که به آن‌ها notebook نیز گفته می‌شود، نوعی از کامپیوترها می‌باشند که تمام اجزای آن در یک قسمت جمع‌آوری شده‌اند.



Laptopها با استفاده از یک باطری داخلی کار می‌کنند و برای

محل‌هایی که دارای برق نیستند بسیار مناسب‌اند.

همچنین در مواردی که قصد دارید کامپیوترتان را همراه خود حمل کنید، laptopها بهترین گزینه می‌باشند.

در مورد این کامپیوترها در بخش‌های دیگر بیشتر توضیح خواهیم داد.

Polmtopها مانند laptopها بدون برق کار می‌کنند، اما حجم آن‌ها بسیار کمتر است.

به این رایانه‌ها personal digital assistant یا PDA نیز گفته می‌شود.



انواع دیگری که در سازمان‌های بزرگ کاربرد دارد، Mainframeها و supercomputerها می‌باشند.



Mainframeها در سازمان‌های بزرگ مانند بانک‌ها به کار می‌رود. که اطلاعات چند شعبه به آن متصل شده است.

Supercomputerها نیز قوی‌ترین کامپیوترهای موجود می‌باشند که چندین میلیون پردازش و محاسبه را در یک ثانیه می‌توانند انجام دهند.

از این کامپیوترها معمولاً در آزمایشگاه‌های تحقیقاتی و در پردازش‌هایی که برای انسان چندین سال به طول می‌انجامد استفاده می‌شود.

تمیز کردن صفحات لمسی



پاک‌کردن صفحه‌های لمسی گوشی‌های هوشمند و تبلت‌ها کار سختی نیست. به هیچ کیت یا روش مخصوصی برای تمیز کردن نیاز ندارید. فقط باید بدانید که چه کارهایی را نباید انجام دهید! بعضی از روش‌ها و وسایل ممکن است به صفحه‌های لمسی آسیب بزنند. اگر این‌ها را بدانید، با ساده‌ترین چیزهایی که دم دستتان است می‌توانید در طی چند ثانیه، تمامی ناپاکی‌ها مثل چربی و گرد و غبار را از روی گوشی و یا تبلتتان پاک کنید.



چه کارهایی را نباید انجام داد

بیایید قبل از این‌که بگوییم چگونه می‌توان به راحتی صفحه‌های لمسی را تمیز کرد، بگوییم که چه کارهایی را هرگز نباید انجام دهیم.
هرگز از مواد شوینده‌ی شیمیایی که پایه‌ی الکلی دارند و یا حاوی آمونیاک هستند استفاده نکنید! اگر برای تمیزکاری حتما نیاز به مایع دارید، می‌توانید از مقدار کمی آب برای این‌کار استفاده کنید. همچنین می‌توانید مواد شوینده‌ی مخصوص این‌کار را خریداری کنید. به

طور مثال می‌توانید از iKlenz که مورد تأیید شرکت اپل است استفاده کنید؛ امّا باز هم می‌گویم که هیچ‌نیازی به خرید چیز به‌خصوصی ندارید.

هرگز از پارچه‌های زبر، حوله‌های کاغذی و یا حتی دستمال کاغذی که باعث وارد شدن آسیب به صفحه‌ی لمسی می‌شود استفاده نکنید. در عوض می‌توانید از پارچه‌های میکروفیبری (معمولاً برای تمیز کردن شیشه‌ی عینک نیز مورد استفاده قرار می‌گیرند) که انحصاراً برای این‌کار ساخته شده‌اند استفاده کنید.هرگز از مقدار زیادی آب برای تمیز کردن استفاده نکنید. اگر به آب نیاز دارید، همان‌طور که پیش‌تر گفته‌شد، می‌توانید پارچه‌ی میکروفیبری خود را با مقدار کمی آب خالص و یا مواد شوینده‌ی مخصوص تَر کنید. در هرِ حال پیشنهاد می‌شود اگرِ از مایع جهت شست‌وشو استفاده می‌کنید، حتماً نمایشگر دستگاه یا کلاً خود دستگاه را خاموش کنید.و پیش‌وپا افتاده‌ترین یادآوری این‌که هرگز برای پاک‌سازی، فشار غیر متعارف به صفحه وارد نکنید!یادآور می‌شوم که توصیه‌های ذکر شده در این نوشتار مخصوص صفحاتی‌ست که با هیچ محافظ صفحه‌ای محافظت نمی‌شوند. بدیهی‌ست اگر از محافظ صفحه استفاده می‌کنید، می‌توانید وسواس کمتری به خرج دهید!

یک پارچه‌ی میکروفیبری تهیه کنید

برای تمیز کردن یک صفحه‌ی لمسی، تنها چیزی که واقعاً نیاز دارید، یک پارچه‌ی میکروفیبری است. اگر صفحه خیلی کثیف است، می‌توانید از مقدار کمی آب هم استفاده کنید (هرگز از مواد کفساز مثل صابون استفاده نکنید!).
ممکن است با خواندن "پارچه‌ی میکروفیبری" فکر کنید چیز خیلی منحصربه‌فردی‌ست! امّا اصلاً این‌طور نیست. این پارچه‌ها به وفور و به ارزانی یافت می‌شوند! اگر عینک دارید، حتماً هنگام خرید عینک، یک پارچه‌ی میکروفیبری نیز هدیه گرفته‌اید. این پارچه‌ها برای تمیز کردن انواع شیشه‌ها ساخته‌شده‌اند. چه می‌خواهد شیشه‌ی عینک طبی یا آفتابی باشد چه شیشه‌ی صفحات لمسی تلفن‌های هوشمند و تبلت‌ها. در هر صورت اگر پارچه‌ی میکروفیبری در اختیار ندارید، می‌توانید از پارچه‌های کتان هم استفاده کنید. البته انتظار نداشته باشید که همان نتیجه‌ای را که می‌توان با پارچه‌های میکروفیبری گرفت، با تی‌شرت کتان خود بگیرید!

اما چرا پارچه‌های میکروفیبری؟ همانطور که مشخص است، میکروفیبر یعنی الیافی بسیار ریز که با میکروسکوپ قابل مشاهده هستند و

“میکرو” پیشوندی‌ست برای چیزهای بسیار ریز! این الیاف بسیار ریز به هیچ‌وجه به سطوح صافی مثل شیشه آسیب نمی‌زنند؛ امّا اصل مطلب این‌جاست که این نوع پارچه‌ها، چربی‌ها و گرد و غبار را به جای این‌که روی صفحه به این طرف و آن طرف ببرند، به خود جذب می‌کنند! چند تکان کوچک پارچه‌ی میکروفیبری روی گوشی، تنها کاری‌ست که باید انجام دهید!

چگونه یک صفحه‌ی لمسی را تمیز کنیم؟

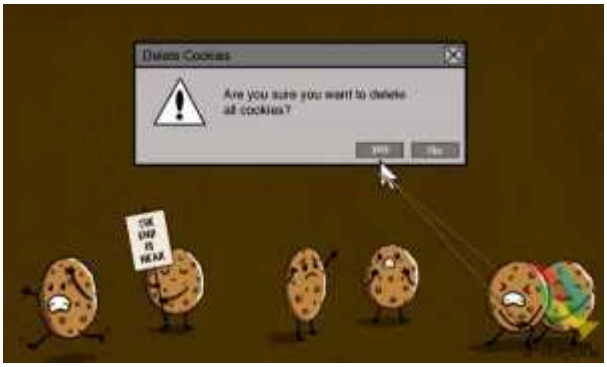
خوب، حالا که وسیله‌ی مورد نیاز عملیات را در دست داریم، می‌رویم به سراغ خود عملیات تمیزکاری!
دستگاه را خاموش کنید! می‌توان گفت این مرحله اختیاری‌ست. اگر از آب استفاده می‌کنید بهتر است این مرحله را انجام دهید. در کل، وسواس زیادی بده! ولی خوب، خاموش کردن دستگاه می‌تواند در دیدن کثیفی‌ها کمکتان کند!بصورت عمودی یا افقی و در یک جهت، پارچه‌ی میکروفیبری را روی صفحه بکشید. به طور مثال، پارچه را روی قسمت سمت چپ صفحه گذاشته و به آرامی و مستقیماً به سمت راست بکشید. حالا پارچه را از صفحه برداشته، کمی پایین‌تر برده و دوباره از چپ به راست بکشید. ممکن است بگویید انجام حرکات دایره‌وار سریع‌تر و راحت‌تر است. راست می‌گویید! ولی این‌کار باعث می‌شود کثیفی‌ها و به‌خصوص ذرات درشت‌تر روی صفحه کشیده‌شوند و باعث وارد آمدن آسیب شوند.

روش که گفته‌شد، امن‌ترین راه است.و برای بار چندم، اگر نیاز است، مقدار بسیار بسیار اندکی جهت تَر کردن پارچه استفاده کنید. از صابون و یا هیچ ماده‌ی افزودنی دیگری به آب بپرهیزید.اگر از آب استفاده کردید، حتما با گوشه‌ی دیگری از پارچه که خشک است، صفحه را خشک کنید. در این مرحله هم نیاز به اعمال وسواس بیش از حد نیست! اگر به اندازه‌ی کافی خشک نشد، بگذارید به طور طبیعی با هوا جریان هوا خشک شود!خلاصه‌ی قضیه، دستگاه را خاموش کنید، با پارچه تمیزش کنید! خشکش کنید. روشنش کنید!
حالا خود پارچه میکروفیبری را چطور تمیز کنیم؟ اگر پارچه بیش از حد کثیف شده‌است، می‌توانید از آب گرم و صابون استفاده کنید. هرگز از مواد شوینده‌ی شیمیایی حاوی الکل یا آمونیاک برای پاک کردن پارچه استفاده نکنید، چون ممکن است باعث وارد آمدن آسیب به الیاف پارچه شود.

کوکی چیست و با امنیت ما چه می‌کند؟



اکثر مردم می‌دانند که کوکی‌هایی در گوشه‌کنار اینترنت پنهان شده‌اند و منتظرند که توسط اولین کسی که پیدایشان کرد خورده … اهم، اشتباه شد! درست نیست! بله، کوکی‌هایی در اینترنت (در واقع در World Wide Web یا همان WWW) هستند و واقعاً هم اسمشان‌کوکی‌ست، ولی خوشمزه که نیستند هیچ، حتی ممکن است برای امنیت شما مضر هم باشند!



چه در حال مشاهده‌ی نتایج یک جستجوی ساده در گوگل باشید، چه در حال ورود به فیسبوک و یا حتی در حال گپوگفت با دوستانتان در انجمن‌های اینترنتی، سر و کارتان با همین کوکی‌هاست. این کوکی‌ها در واقع مضر نیستند. اما مثل پسورد یا ایمیل‌ها اگر دست آدم‌های ناشایست بیفتند، می‌توانند بسیار مخرب باشند. با ما تا انتهای این نوشتار همراه باشید تا ببینیم چگونه می‌توانیم از خودمان محافظت کنیم.

واقعاً، کوکی‌ها چیستند؟

خیلی ساده بخواهیم بگوییم، کوکی‌ها فایل‌هایی هستند که در رایانه‌ی شما ساکن می‌شوند. کوکی‌ها وقتی وارد وبسایتی می‌شوید ساخته می‌شوند. کارشان هم این است که اعمال و رفتار و اطلاعات مهم شما را ذخیره کنند تا در ورود بعدی شما به همان وبسایت، نیازی به وارد کردن مجدد اطلاعات توسط شما نباشد و خودبخود این اتفاق بیفتد. پس این بندگان خدا در واقع مفید هم هستند! کوکی‌ها توسط سرورها و بعضی از برنامه‌ها قابل خواندن هستند.
مرورگر شما در واقع واسطه‌ایست بین رایانه‌ی شما و وبسایت مورد نظر. کوکی‌ها برای این ساخته می‌شوند که سایت‌ها با توجه به اینکه شما که هستید و چه می‌خواهید، محتوای مورد نظر را نشانتان دهد. کوکی‌ها می‌توانند طوری ساخته شوند که پس از مدت مشخصی خودبخود پاک شوند. البته می‌توان بصورت دستی هم هرگاه بخواهید آن‌ها را پاک کنید.

کوکی‌ها برای این ساخته شدند تا بجای اینکه حجم عظیمی از اطلاعات روی سرور سایت ذخیره شود، روی رایانه‌ی هر کاربر ذخیره گردد تا فشار زیادی به سرور وارد نیاید. بارها شده که در یک سایت لاگین کرده‌اید و صفحه را بسته‌اید و مجدداً گشوده‌اید و دیده‌اید که نیازی نیست دوباره لاگین کنید. این بخاطر وجود همین کوکی‌هاست. کوکی‌ها به سایت‌ها کمک می‌کنند تا شما را بشناسند. کوکی‌ها قادرند خیلی از چیزها را ذخیره کنند. مثلا قادرند مکان شما، نوع مرورگر شما و تنظیماتی که را انجام داده‌اید را نگهداری کنند تا بتواند در بازدیدهای بعدی‌تان از آن وبسایت به یاری‌تان بیایند.

کوکی‌ها چگونه ممکن است مضر باشند؟

کوکی‌ها برای راحتی و آسایش ساخته شده‌اند و در باطن بی‌ضررند. از ویروس‌ها می‌ترسید؟ نه! کوکی‌ها قادر به انتقال ویروس و بدافزار نیستند. پس خیالتان از این نظر راحت باشد. بگذارید شفاف بگویم، اگر کوکی‌ها نبودند، اینترنت فلج بود! اگر کوکی‌ها را پاک کنید، هر بار که وارد سایت‌های مورد علاقه‌تان مثل سرویس‌های گوگل، فیسبوک و … می‌شوید باید مجددا نام کاربری و رمز عبور خود را وارد کنید. واقعاً خسته کننده است!

از چه چیز کوکی‌ها باید ترسید؟

بدترین سناریوی ممکن این است که یک شخص ثالثی بتواند این اطلاعات رد و بدل شده بین شما و سرور را شنود کند! با این حساب می‌تواند با نام کاربری شما در سایت‌هایی که عضوشان هستید لاگین کند و … . اما آنقدر ها هم نگران نباشید. چون کوکی‌ها رمزنگاری (Encrypt) می‌شوند.
اما مدل دیگری از کوکی‌ها وجود دارند که نامشان "کوکی‌های ردیاب" (tracking cookies) است و می‌توان گفت برای راحتی شما ساخته نشده‌اند. کارشان این است که تمام فعالیت‌های شما را ثبت و ضبط می‌کنند و به این درد می‌خورند که سایت‌هایی مثل فیسبوک، بفهمند شما از چه چیزی بیشتر خوشتان می‌آید و تصمیم بگیرد که مثلاً چه نوع تبلیغاتی را نشانتان بدهد! اینجاست که امنیت و حریم خصوصی شما ممکن است خدشه دار شود.
بزرگترین مشکل این‌جاست که شرکت‌های ارایه‌دهنده‌ی تبلیغات می‌توانند تمام کارهایی که کرده‌اید را ببینند! اما شما حالا می‌توانید با کمی بازی کردن با تنظیمات مرورگر خود کاری کنید که ردپایتان ثبت و ضبط نشود.
حال این‌جا بحث اعتماد پیش می‌آید … آیا به این سایت اعتماد دارید؟ پس بگذارید کوکی بسازد. به سایتی اعتماد ندارید؟ در مرورگر خود کاری کنید که کوکی ذخیره نکند! به همین سادگی.
اگر می‌خواهید ببینید چه کوکی‌هایی بر روی رایانه‌تان ذخیره شده، می‌توانید از CookieSpy استفاده کنید. اگر هم می‌خواهید ببینید که فلان سایت چه کوکی‌هایی ایجاد می‌کند از Cookie-Checker استفاده نمایید.

کارت شبکه (NIC) چیست؟



کارت شبکه (NIC) :

به مجموعه رایانه های متصل به یکدیکر که می توانند سخت افزار، نرم افزار یا داده ها را به اشتراک با هم بگذارند شبکه گفته می شود. برای ایجاد شبکه بین دو یا چند رایانه هر رایانه باید لااقل به یک کارت شبکه مجهز باشد. کارت شبکه در واقع یک ترمینال یا پایانه برای هر رایانه است که از طریق اتصال این ترمینال با ترمینال سایر رایانه ها شبکه تشکیل می یابد.



وظایف کارت شبکه عبارتند از:

- برقراری ارتباط لازم بین کامپیوتر و محیط انتقال .
- تبدیل داده: داده ها بر روی گذرگاه (bus) کامپیوتر به صورت موازی حرکت می نمایند. نحوه حرکت داده ها بر روی محیط انتقال شبکه به صورت سریال است. ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده)، داده ها را از حالت موازی به سریال و بالعکس تبدیل می نماید.

- اراثه یک آدرس منحصر بفرد سخت افزاری: آدرس سخت افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می شود. آدرس سخت افزاری موجود بر روی کارت شبکه، یک آدرس منحصربفرد را برای هر یک از کامپیوترهای موجود در شبکه ، مشخص می نماید. پروتکل هایی نظیرTCP/IP از یک سیستم آدرس دهی منطقی (آدرس IP)، استفاده می نمایند.



در شکل بالا یک نمونه کارت شبکه خارجی (اکسترنال) را مشاهده می کنید که با اتصال آن به یکی از پورت های یو اس بی فعال می شود.

افزایش کیفیت و محدوده شبکه بی‌سیم



استفاده از شبکه بی‌سیم این روزها دیگر خیلی ساده شده است. تنها کافی است یک روتر بیسیم را خریداری کنید و سپس پورت اینترنت آن را به دستگاه مودم ADSL خود وصل کنید. حال می توانید از تمامی دستگاه ها و سیستم هایی که در اختیار دارید به روتر خود وصل شوید و از اینترنت در تمامی آن سیستم ها استفاده کنید.

اما با وجود رشد استفاده از شبکه های بی سیم در خانه ها و شرکت ها بعضی از کاربران از کیفیت و محدوده‌ای که می توانند با آن به شبکه های بی سیم اتصال پیدا کنند ناراضی هستند. در این آموزش از تورتک با هم یاد می گیریم که چگونه شبکه بی‌سیم خانگی خود را تقویت کرده و با این کار کیفیت دریافت سیگنال و محدوده قابل

دسترس بودن سیگنال ها را افزایش دهیم.



چگونگی تقویت قدرت سیگنال های WiFi شبکه بی‌سیم

قبل از اینکه با انجام ترفندهایی قدرت و محدوده سیگنال های شبکه بی‌سیم خود را افزایش دهیم بهتر از با نکته‌ای آشنا شوید که در هنگام خرید روترهای خانگی به آن نیاز دارید. در هنگام خرید دستگاه روتر توجه داشته باشید که دستگاه مورد نظر از ارتباط بر مبنای استاندارد ۸۰۲.۱۱n پشتیبانی کند. در اینگونه ارتباط برخلاف نسخه قدیمی تر خود یعنی ۸۰۲.۱۱g که در بازار ایران نیز به راحتی پیدا می شود قدرت سیگنال و همچنین سرعت تبادل اطلاعات تغییر چشمگیری کرده است و شما با در اختیار داشتن یک روتر بر پایه ۸۰۲.۱۱n کمتر به مشکلاتی مانند قطعی در هنگام تبادل فایل های حجیم و ویدئو ها در بین دستگاه های متصل به شبکه بر می‌خورید.

اما در هر صورت ترفندهایی نیز برای افزایش کیفیت و محدوده سیگنال دهی شبکه های بی‌سیم خانگی وجود دارد که با آن ها در زیر آشنا می شویم.

1. **استفاده از DD-WRT :** در صورتی که نام مودم و یا دستگاه روتر شما در لیست دستگاه های سازگار با DD-WRT firmware وجود داشته باشد (مشاهده لیست) می توانید با دانلود این firmware (لینک دانلود DD-WRT) و نصب آن از طریق پنل

مدیریتی روتر خود حداقل چند متری را به محدوده شبکه بیسیم خود اضافه کنید و با این کار همچنین کیفیت سیگنال های شما هیچ تغییر خاصی نیز نمی کنند. در صورتی که دستگاه شما با این firmware سازگاری نداشت پیشنهاد می کنم از Tomato firmware استفاده کنید.

2. **استفاده از ورق های آلمینیومی :** اکثر روترها بر روی خود یک آنتن دارند که اطلاعات و سیگنال ها را به تمامی جهت های ممکنه ارسال می کنند مانند یک لامپ معمولی که نور را پخش می کند. در صورتی که از دستگاه روتر خود در مرکز محدوده و یا خانه خود استفاده می کنید این ویژگی می تواند خیای مفید باشد اما اگر روتر شما در گوشه ای از خانه شما قرار دارد می توانید با استفاده از یک ورق آلمینیومی و حتی یک قوطی نوشابه آهنی باز شده بین دیوار و دستگاه روتر خود از هدر رفتن سگنال‌ها جلوگیری کنید و آن ها را دوباره به سمت محدوده کاری خود برگردانید. البته اگر می خواهید بهترین نتیجه ممکنه را از این ترفند بگیرید بهتر است کمی بر روی حالت ورق آلمینیومی در پشت روتر خود کار کنید و با انتخاب شکل های مختلف به بهترین حالت ممکن دست یابید.
3. **استفاده از نرم افزار InSSIDer :** این نرم افزار کاملاً رایگان می تواند وجود و قدرت سیگنال های شبکه بی‌سیم خانگی شما را نمایش دهد. بهتر است این نرم افزار را بر روی لپ تاپ خود نصب بکنید و سپس در نقاط مختلف خانه از دسترسی و کیفیت سیگنال های شبکه با خبر شوید. با کنار هم گذاشتن اطلاعات به دست آمده خود می توانید بهترین مکان قرار گیری دستگاه روتر را تشخیص دهید. برای دانلود این نرم افزار از لینک InSSIDer استفاده کنید.
4. **انتخاب بهترین مکان برای روتر :** یکی دیگر از مواردی که می‌تواند در بهبود کیفیت و محدوده شبکه های بیسیم تاثیر بگذارد انتخاب یک مکان صحیح برای دستگاه روتر شبکه شما است. توجه داشته باشید که در کنار روتر بی سیم خود نباید دستگاه بی‌سیم دیگری وجود داشته باشد و سعی کنید از اجسام آهنی که ممکن است سیگنال ها را در جهت بی استفاده ای بازتاب کنند دستگاه روتر شما دور باشد. همچنین سعی کنید در وسط محل استفاده از شبکه بی سیم و همچنین در نقطه بالایی نسبت به دیگر دستگاه ها روتر شما قرار بگیرد.
5. **استفاده از آنتن‌های uni-directional :** معمولاً دستگاه های روتر با یک آنتن از نوع omni-directional که کیفیت معمولی

نیز دارد فروخته می شوند ، پس اگر می خواهید محدوده و جهات پخش شدن سیگنال های شبکه بی‌سیم خود را افزایش دهید می توانید با خرید یک آنتن uni-directional قوی‌تر و نصب آن بر روی دستگاه روتر خود این کار را انجام دهید. اگر آنتن بهتری را در بازار برای خرید پیدا نکردید حداقل می توانید از آنتن های بهتر از مدل فعلی آنتن روتر خود که از تکنولوژی omni-directional در آن ها استفاده می شود را به راحتی پیدا کنید.

افزایش محدوده شبکه های بی‌سیم با استفاده از سخت افزارهای جانبی

یکی دیگر از مواردی که کاربران شبکه های بی سیم خانگی به آن نیاز پیدا می کنند این است که محدوده قابل دسترس بودن شبکه خود را افزایش دهند که برای اینکار بهترین روش ممکن استفاده از سخت افزارهای جانبی است که کمپانی های معروف ارائه می دهند. در زیر با تاثیر گذار ترین روش های ممکن برای افزایش محدوده شبکه های بیسیم WiFi آشنا می شویم.

1. **استفاده از دستگاه WiFi Repeater :** این دستگاه همانطور که از اسم آن پیدا است قابلیت این را دارد که سیگنال های ارسالی دستگاه روتر بی سیم شما را دریافت کند و آن ها را با کیفیت و قدرت اولیه در محدوده ای که قرار دارد دوباره در تمامی جهات بحش کند. بهترین حالت استفاده از این دستگاه در زمانی است که آن را در نقاطی قرار دهیم که بعد از آن ها دیگر سیگنال های دستگاه روتر ما در دسترس نیست تا بتوانیم محدوده شبکه خود را بدون نیاز به هیچ سیمی افزایش دهیم.
2. **استفاده از یک روتر دیگر :** یکی دیگر روش هایی که برای افزایش محدوده های شبکه بی سیم به شما پیشنهاد می کنیم خرید و استفاده از یک روتر دیگر در کنار روتر فعلی شما است. تنها کافی است روتر اصلی خود را به اینترنت متصل کنید اگر می خواهید در شبکه اینترنت قابل دسترس باشد و سپس با یک کابل به شیوه LAN

دستگاه روتر دوم را به روتر اصلی وصل کنید. جالب است بدانید در این روش می توانید تا ۱۰۰ پا دورتر دستگاه روتر دوم را قرار دهید چون برای دریافت اطلاعات از شبکه شما از یک سیم استفاده می شود.

3. **استفاده از یک Access Point :** با استفاده از یک دستگاه Access Point نیز می توانید به محدوده شبکه بی سیم خود وسعت بیشتری را بدهید مانند استفاده از WiFi Repeater که در بالا با آن آشنا شدیم. از مزایای این روش می توان به قابلیت اتصال سیستم های بیشتر به شبکه و از معایب آن می توان به قیمت بالای این دستگاه نسبت به یک روتر اشاره کرد.

آموزش رمز گذاری اسناد در word



ویژگی‌های جدید Office 2007 مانند امضای دیجیتالی و رمزگذاری به شما کمک می‌کنند تا اطلاعات محرمانه خود را قفل کرده و دور از چشمان جست‌وجوگر دیگران نگه دارید.

نرم‌افزار Word به عنوان اصلی‌ترین ابزار ایجاد اسناد، از هر ۹ کاربر ۵ نفر را به خود اختصاص می‌دهد و به کاربران این فرصت را می‌دهد تا در اسرع وقت نامه‌های مشتریان، گزارشات مالی رؤسا و حتی پروژه‌های عظیم اجرایی را آماده کنند.

اما حتی در عصر شبکه‌های بی‌سیم و با وجود برنامه‌های جاسوسی، بسیاری از افراد، اطلاعات حساس و مهم خود را بدون حفاظت رها می‌کنند.

نگران نباشید. ویژگی‌های جدید Office 2007 مانند امضای

دیجیتالی و رمزگذاری به شما کمک می‌کنند تا اطلاعات محرمانه خود را قفل کرده و دور از چشمان جست‌وجوگر دیگران نگه دارید.



امضای اسناد

نرم‌افزار Word 2007 یک ویژگی جدید امنیتی را برای اسناد، ارائه کرده است و آن امضای دیجیتالی است. شما می‌توانید به هر سند یک فیلد امضا اضافه کنید و به این ترتیب، فایل قفل شده و امکان انجام هیچ ویرایشی روی آن وجود نخواهد داشت؛ مگر اینکه امضای دیجیتالی حذف شود.

ممکن است هر فردی قادر به حذف امضا و ویرایش فایل باشد، اما سند امضا شده، مهر تائید شماست.

استفاده از رمزگذاری و کلمه عبور

امضای دیجیتالی، سند را در مقابل ایجاد تغییرات، حفاظت می‌کند و در واقع به آن اعتبار می‌بخشد؛ خصوصاً اگر از تصویر bitmap امضای حقیقی خود استفاده کنید. اما هنوز این امکان وجود دارد که اسناد امضا شده، باز و خوانده شود. بنابراین استاندارد AES (استاندارد رمزگذاری پیشرفته) به همراه یک کلید ۱۲۸ بیتی و SHA-1 به Word 2007 اضافه شده است. باید به این نکته توجه کنید که اگر سند موردنظر را به صورت دیجیتالی امضا کرده‌اید، دیگر حتی با اضافه کردن یک کلمه عبور هم نمی‌توانید آن را تغییر دهید.

فقط اسناد امضا نشده می‌توانند توسط کلمه عبور حفاظت شوند. روی

دکمه Office در قسمت بالای سمت چپ کلیک کنید، سپس گزینه Prepare و Encrypt Document را انتخاب کنید. کلمه عبوری را انتخاب کنید که حدس زدن آن دشوار باشد. از حروف کوچک و بزرگ و اعداد بهره گیرید و برای برخورداری از بالاترین میزان حفاظت، حداقل از ۸ کاراکتر استفاده کنید. حال روی OK کلیک کنید.

کلمه عبور را مجدداً وارد کنید. حال اگر هر فردی سند موردنظر را باز کند، باید کلمه عبور مربوطه را تایپ کند؛ در غیر این‌صورت دستیابی به متن غیر ممکن است.

به منظور اضافه کردن امضای دیجیتالی، ابتدا سند موردنظر را باز و یا ایجاد کنید. سپس روی زبانه Insert کلیک کرده و گزینه Signature Line در سمت راست را انتخاب کنید. روی OK کلیک و سپس مواردی از قبیل اسم، عنوان و آدرس پست الکترونیکی شخص امضا کننده (خودتان) را پر کنید. شما حتی قادرید تاریخ را هم به امضای خود اضافه کنید. سپس روی دکمه OK کلیک کنید. برای امضای سند، روی محل امضا دابل کلیک کنید. اسمتان را تایپ یا روی Select Image کلیک کنید تا فایل bitmap امضای حقیقی خود را انتخاب کنید. سپس روی Sign کلیک کنید.

از بخش‌های مهم سند حفاظت کنید

ممکن است فایل موردنظر خود را امضا و یا رمزگذاری کرده باشید اما تصمیم بگیرید که به دیگران اجازه دهید متن موردنظر شما را ویرایش کنند، اما این تغییرات کاملاً تحت کنترل شما باشد. در این حالت چه کار باید کرد؟ روی گزینه Review و سپس Protected Document (در قسمت راست) کلیک کنید و گزینه‌های قالب‌بندی را که دیگران می‌توانند ویرایش کنند، انتخاب کنید. برای مثال شما می‌توانید این اختیار را به آنها بدهید که مثلاً فونت را تغییر دهند ولی در اندازه آن تغییری ایجاد نکنند. همچنین شما می‌توانید از Track Changes استفاده کنید. در این صورت ویرایش صورت گرفته به صورت متمایز نمایش داده می‌شود. برای حفاظت از سند، گزینه Start Enforcing را انتخاب کرده و سپس رمز عبور را وارد و بعد تائید کنید.

کاربردهایی از غلتک ماوس که نمی‌دانید



شما می توانید برای بستن تب های اضافی در مرورگر اینترنتی خود به جای استفاده از دکمه ضربدر که نیاز هر تب، روی تب مورد نظر به وسیله غلتک ماوس کلیک کنید.

کافیست غلتک ماوس را بر روی لینک مورد نظر خود برده و توسط آن کلیک کنید، خواهید دیدی با این کار کنید در یک تب جدید باز خواهد شد.

همچنین می توانید برای بازکردن یک لینک در تب جدید در یک مرورگر کلید ctrl را نگه داشته و روی آن کلیک کنید.

تمامی موارد گفته شده در مرورگرهای فایبر فاکس، IE گوگل کروم واپرا قابل اجرا است.

