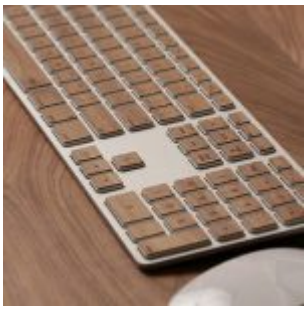
صفحه کلید(کیبورد)

□□□□ □□□□ ها که البته آن ها را با نام کیبورد «Keyboard» نیز می شناسیم، به شکل ها و اندازه های مختلفی برای کامپیوتر های شما ارائه می شوند، ولی این کیبورد ها فقط به پورت های مخصوص Mini-DIN یا USB متصل می شوند. بسیاری از صفحه کلیدها با یک تبدیل فروخته می شوند که می توانید در مورد پورت Mini-DIN یا USB انتخاب آزاد داشته باشید. فیش صفحه کلید معمولاً به رنگ بنفش می باشد.

مهمترین ابزار جانبی کامپیوتر شما، کارت گرافیک، چاپگرو یا حتی مانیتور آن نیست. حیاتی ترین بخش سخت افزار (البته بعد از پردازنده)، صفحه کلید است. صفحه کلید از نظر فناوری، زیاد پیچیده نیست و به همین دلیل هنگامِ بررسی ها اصلاً به طور کافی مورد توجه قرار نمی گیرد ولی مطمئناً در راحتی، سلامتی، و کارآیی شما هنگام کار با رایانه، مؤثر است.

کافی است تنها نگاهی به آمار رو به رشد بیماری های ناشی از فشار مداوم (RSI) بیندازیم. در حالی که مردم هر روز ساعات بیشتری از وقت خود را در پشت کامپیوتر مشغول به کار هستند، احتمال ایجاد صدمات دائمی توسط صفحه کلیدهایی که در طراحی آنها از نظر فیزیولوژیکی دقت لازم به عمل نیامده است بیشتر می شود.

مرور اجمالی صفحه کلید

برای ارتقای صفحه کلید دلایل مختلفی می تواند وجود داشته باشد که یکی از مهمترین آنها، دلایل ارگونومیکی است. وسایل ارگونومیکی مانند صفحه کلیدها، صندلی های کار، نیمکت ها و … ، باید به گونه ای طراحی شوند که حداقل فشار را به بدن انسان وارد کنند. عدم توجه به این امر می تواند طی مدت زمان طولانی، باعث ایجاد صدمات جدی شود. در واقع انتخاب یک صفحه کلید مناسب در راحتی کار مؤثر

است.

علاوه بر این شما می توانید از انواع مختلف صفحه کلیدها برای برآورده کردن نیاز هایتان استفاده کنید. صفحه کلیدهای فشرده فضای کمتری از میز کار شمار را اشغال می کنند، صفحه کلیدهای بیسیم از امواج مادون قرمز و یا سیگنال های رادیویی استفاده می کنند و صفحه کلیدهای چند رسانه ای حاوی بلندگو، میکروفن و کنترل های صوتی می باشند. حتی صفحه کلیدهایی وجود دارند که داخل آنها یک اسکنر جاسازی شده است. با این حال و با وجود این تنوع، تمام وسایل عملکرد مشابهی دارند.

طریقۀ کار صفحه کلیدها

برخلاف آنچه به نظر می رسد، ساختار صفحه کلید چندان هم ساده نیست و دارای یکی طراحی هوشمند است … یک تراشه کوچک که «کنترل کننده صفحه کلید» نامیده می شود، نقش مفسر را بازی می کند و فرامین حاصل از فشرده شدن کلیدها را، به ورودی های قابل تشخیص برای پردازنده مرکزی کامپیوتر، تبدیل می کند.

صفحه کلید «کیبورد» رایانه

نحوۀ کار آن بدین صورت است : کلیدهای صفحه کلید به طور منظم بالای یک شبکه حساس قرار گرفته اند. این شبکه، ضربه های وارد بر کلیدهای را تشخیص می دهد و برای انجام این کار (تشخیص فشرده شدن کلیدها)، کنترل کننده صفحه کلید به طور دائم، وضعیت هر نقطه بر

روی شبکه را که متناظر با یک کلید در صفحه کلید است، کنترل می کند. کنترل کننده، این کار را با ارسال سیگنال های متقاطع از بالا و کناره های شبکه انجام می دهد.

انواع صفحه کلید

اکثر مردم فکر می کنند که همۀ صفحۀ کلیدها یکسان هستند، ولی اینطور نیست و سازندگان صفحه کلیدها همواره تکاپوی ساخت صفحه کلید هایی با شکل، اندازه و قابلیت های متفاوت هستند. فشار کمتر به کاربر هنگام کار با صفحه کلید، هدف اولیه بسیاری از این طرح ها بوده است. صفحه کلیدهای چند تکه، صفحه کلیدهای شیبدار، صفحه کلیدهای مرسوم به QWERTY، صفحه کلیدهای با قابلیت کار با یک دست و … نمونه هایی هستند که در این راستا ساخته شده اند.

از نظر قابلیت های اضافی، سازندگان صفحه کلید، ادوات جانبی بسیاری نظیر اسکنر، ماوس پد و سیستم های صوتی را نیز به صفحه کلیدهای خود اضافه کرده اند. فلسفۀ این کار این است که هر کامپیوتر رومیزی، یک صفحه کلید به همراه خود دارد. پس فضای میز کار شما خواه یا ناخواه توسط این صفحه کلید اشغال می شود. اما چرا از این فضا بیشتر استفاده نکنیم؟

در زیر ما فقط انواع کیبورد را نام می بریم :

- صفحه کلیدهای استاندارد
- صفحه کلیدهای چند تکه
- صفحه کلید چند منظوره
- صفحه کلیدهای بی سیم
- صفحه کلیدهای ارگونومیک

تصمیم گیری برای خرید کیبورد رایانه

خرید صفحه کلید، تا حد زیادی سلیقه ای است ولی در عین حال تأثیر زیادی بر کارآیی شما دارد. علاوه بر سلیقه شخصی، باید مواردی همچون فضای کاری که در اختیار دارید، شرایط ارگونومیک و احیاناً نیاز به یک صفحه کلید چند منظوره را نیز مد نظر قرار دهید.

نکتۀ جالبی که در مورد صفحه کلید وجود دارد این است که انتخاب آن، تا حد زیادی به سلیقه شخصی شما بستگی دارد. ممکن است از یک صفحه کلید خوشتان بیاید و یا برعکس. قیمت، مشخصات و آگهی های

مختلف نمی تواند سلیقه شما را خیلی تغییر دهد. به همین خاطر، بهتر است که قبل از خرید یک صفحه کلید، آن را امتحان کنید. در صورت امکان، از فروشنده بخواهید به شما اجازه دهد که چند صفحه کلید را امتحان کنید.

صفحه کلیدی را انتخاب کنید که کلیدهای فرعی آن به دلخواه شما باشد. بعضی از تایپیست ها به صفحه کلیدهایی علاقه دارند که هنگام فشار دادن خیلی پایین می روند و ضربه وارد بر کلید را کاملاً احساس می کنند، در حالی که برخی دیگر به صفحه کلیدهایی علاقه دارند که هنگام فشار دادن خیلی پایین نمی روند و نرم تر هستند. موارد زیر نکاتی هستند که شما هنگام خرید صفحه کلید باید مد نظر داشته باشید. مابقی کار، طبق سلیقه شخصی خودتان است :

- **سخت یا نرم بودن کلیدها :** دقت کنید که کلیدها خیلی نرم، یا خیلی سخت نباشند! آیا هنگام فشار دادن ضربه ای به عنوان نشانه فشرده شدن حس می کنید یا تنها عکس العملی آرام دریافت می کنید؟
- **روی کلیدها :** به بالای کلیدها توجه کنید. آیا آنها برای کمک به افزایش دقت، حاشیه و دندانه گذاری شده اند یا نه؟ آیا هنگام فشار دادن کلید صاف و لغزان به نظر می رسد.
- **صدای کلیدها :** شما صفحه کلید بدون سر و صدا را ترجیح می دهید یا صفحه کلیدی که هنگام ضربه زدن به آن، صدای ضربه را بشنوید؟ آیا این صفحه کلید هنگام تایپ کردن صدا می دهد یا نه؟
- **ساختار صفحه کلید :** این صفحه کلید سبک است، با سنگین؟ موقع تایپ کردن ثابت و بدون سر و صدا است یا نه؟ مواظب باشید که صفحه کلید پیچ و تاب نامتناسب نداشته باشد.
- **کابل صفحه کلید :** صفحه کلیدی بخرید که کابل بلندی داشته باشد. بیشتر صفحه کلیدها دارای کابل کوتاهی هستند که این کوتاهی کابل، هنگام کار، آزادی عمل شما را محدود می کند.

طریقۀ مراقبت از صفحه کلید

صفحۀ کلید بیش از هر قطعه دیگر کامپیوتر ممکن است به خاطر عدم استفادۀ صحیح، آسیب ببیند. هارددیسک و CD ROM درایو، در داخل جعبۀ کامپیوتر و در مکانی مطمئن قرار گرفته اند. مانیتور هم در مکانی نسبتاً ایمن قرار گرفته است. ولی کیبورد در مقابل شما و در میان وسایل کار شما و چای و قهوه و … قرار گرفته است.

خوشبختانه صفحه کلیدها به گونه ای ساخته شده اند که به آسانی نتوان آسیب های جدی به آن وارد نمود. مکانیسم عملکرد کلیدهای صفحه کلید در عین ساده بودن، از استحکام خوبی برخوردار است. علاوه بر آن و آسیب رساندن به اتصالات کلیدها و یا مدار موجود در صفحه کلید، جلوگیری می کند. این محافظ به گونه ای تعبیه شده است که از نفوذ مواد خارجی در زیر هر کلید جلوگیری می کند. با وجود این، باز هم امکان بروز مشکل وجود دارد.

منبع:www.downloadarticle.ir

مودم ها هم ویروسی می شوند؟

امنیت در همه چیز مهم ترین اصل است امنیت مودم ها و دسترسی های به نت نیز از این قضیه مستثنی نیست هکر ها هم خدا خیرشان بدهد علاقه وافری به استفاده از حفره های امنیتی و اشکالات بوجود آمده تولید کنندگان است که می تواند میلیون ها کاربر را تحت اشعاع قرار دهد

امنیت در همه چیز مهم ترین اصل است. امنیت مودم ها و دسترسی های به نت نیز از این قضیه مستثنی نیست. هکر ها هم خدا خیرشان بدهد علاقه وافری به استفاده از حفره های امنیتی و اشکالات بوجود آمده تولید کنندگان است که می تواند میلیون ها کاربر را تحت اشعاع قرار دهد. اکنون نیز کافی است با پستی دیگر از برسام همراه باشید تا از امنیت مودم یا روتر خود اطمینان کامل پیدا کنید.

تجارت مودم و ساخت آن، دست کمی از تجارت تلفن های اندروید نیست! سازندگان این وسایل ارتباطی، تعداد زیادی از دستگاه های مختلف را تولید کرده و همینطور به ارائه آپدیت های جدید نیز اهمیتی نمی

دهند که کاربران را نسبت به حمله آسیب پذیر تر می کنند.

چگونه از نیمه تاریک روتر خود مطلع شویم؟

تغییر تنظیمات سرور DNS راهی است که هکر ها برای تغییر مسیر به یک دی ان اس مخرب از آن استفاده می کنند. هنگامی که به یک سایت متصل می شوید برای مثال سایت بانکی تان دی ان اس تغییر یافته شما را به یک سایت مخرب و سوء استفاده کننده به جای سایت اصلی راهنمایی می کند. البته این اتفاق معمولا رخ نمی دهد و بعضی اوقات دی ان اس قادر به پاسخگویی نیست و شما را به سایت اصلی توسط پوشش دهنده اینترنت خودتان راهنمایی می کنند. به طور معمول درخواست های دی ان اس کند نشانه ای از داشتن چنین مشکلی است.

البته دچار شدن به چنین مشکلی بسیار واضح است و سایت های مخرب هیچ گاه از اتصالات و امنیت HTTPS استفاده نخواهند کرد.

البته هکر ها (حمله کنندگان اطلاعاتی) از تبلیغات ورودی، نتایج جستجوی تغییر یافته یا تلاش برای نصب فایل های دانلود شده نیز استفاده می کنند.

بیشترین حملات از طریق فایل های مخرب جای سازی شده جاوا اسکریپت در یک سایت می باشد. پس از این که کد جاوا اسکریپت بر یک دستگاه متصل به سیستم وای فای شما اجرا می شود، این کد توانایی دسترسی به اینترفیس را خواهد داشت که تنها در شبکه شما موجود است.

البته در این میان، بعضی از مودم ها دارای یک اینترفیس مدیریت از راه دور هستند که با یوزر و پسورد پیشفرض همراه می شود. برخی از روبات ها می توانند این مودم ها را پیدا کرده و به آن ها دسترسی پیدا کنند. البته داستان به همین جا ختم نمی شود و می توانند تنظیمات دیگری را نیز درگیر کنند از جمله UPnP

نحوه بررسی

یکی از علائم شایع حمله به دی ان اس، مشاهده تغییر در سرور آن می باشد. در این مورد، باید به اینترفیس مبتنی بر وب مودم تان رفته و تنظیمات سرور دی ان اس را بررسی نمایید. معمولا در این مورد در صورتی که خودتان تغییری ایجاد نکرده باشید، نحوه دی ان اس به صورت منوال یا دستی خواهد بود و شبیه به ۰.۰.۰.۰ می باشد.

از بین بردن و محافظت بیشتر اگر احیانا با تغییر در دی ان اس مواجه شدید، باید به تنظیمات مودم رفته، ابتدا آن را روی حالت آتوماتیک تنظیم نمایید و سپس آن را با روش های زیر ایمن تر نمایید:

۱) نصب آپدیت های فریم ویر؛ برای اطمینان از نصب آخرین آپدیت کافی است به سایت تولید کننده و یا پوشش دهنده اینترنت خود مراجعه نمایید.

۲) غیر فعال سازی امکان دسترسی از راه دور؛ با رفتن به صفحه مدیریت وب مودم، این امکان را نیز غیرفعال نمایید.

۳) گذرواژه خود را تغییر دهید؛ گذرواژه خود را به کلمه ها و اعدادی تغییر دهید که قابل حدس نباشند.

۴) UPnPرا تغییر دهید؛ حتی اگر این قابلیت آسیب پذیر هم نباشد، تکه ای از برنامه های مخرب موجود در شبکه داخلی شما می تواند از

آن سوء استفاده نموده و دی ان اس شما را تغییر دهد زیرا هر درخواستی که از طرف شبکه لوکال شما باشد را می پذیرد.

منبع:www.aftabir.com

پس از مرگ، چه بر سر اطلاعات آنلاین افراد می‌آید؟

آیا از خود پرسیده‌اید هنگامی که فردی می‌میرد، چه اتفاقی برای حساب‌های بانکی، حساب ای‌میل و پروفایل‌های او در شبکه‌های اجتماعی می‌افتد؟

دیوید ایگلمن، نویسنده و عصب‌شنای مشهور یک داستان کوتاه به نام «کلید مرگ» دارد که در مجموعه داستان‌های او به نام «مجموع» منتشر شده است. او در این داستان به زندگی آنلاین افراد پس از مرگ آنها می‌پردازد. در بخشی از این داستان آمده است: «در ابتدای دوران کامپیوتر، افراد در حالی می‌مردند که پسوردهایشان را فقط خودشان می‌دانستند و پس از مرگشان هیچ کسی نمی‌توانست به فایل‌هایشان دسترسی داشته باشد. گاهی ممکن بود این فایل‌ها برای یک شرکت ارزشی حیاتی داشته باشند؛ در این حالت شرکت به بحران برمی‌خورد. به همین دلیل بود که برنامه‌نویسان کلید مرگ را اختراع کردند.»

ایگلمن سپس درباره این کلید خیالی توضیح می‌دهد: «کلید مرگ به این نحو کار می‌کند که کامپیوتر هر هفته یک بار به کاربر می‌گوید رمز عبورش وارد کند تا مطمئن شود که او زنده است. وقتی برای چند هفته کاربر این رمز را وارد نکند، کامپیوتر به این نتیجه می‌رسد که او از دنیا رفته است و سپس پسورد او را به فرد دیگری می‌دهد که نفر

اول تعیین کرده است. به این ترتیب، افراد از کلید مرگ استفاده می‌کنند تا شماره حساب‌ها و رمز عبورهای خود را به ورثه منتقل کنند، آخرین پیام خود را به بازماندگان بدهند و اسرار ناگفته خود را فاش سازند.»

ایگلمن در داستان خود نوشته که از این کلیدهای مرگ می‌توان استفاده کرد تا پس از مرگ افراد، آنها باز هم برای بازماندگانشان پیام‌های تبریک بفرستند یا زمانی که فرزندانشان به سن بلوغ رسیدند، دارایی‌های پدر و مادر متوفی‌شان پس از سال‌ها به آنها ارث برسد. او پا را فراتر از این گذاشت و دنیایی را به تصویر کشید که در آن افراد پس از مرگ همچنان به ای‌میل‌ها پاسخ می‌دهند و جامعه‌ای مجازی از مردگان به وجود آورده‌اند.

شاید برایتان جالب باشد بدانید که داستان ایگلمن، بیشتر از آن که خیال‌پردازی باشد به واقعیت نزدیک است! اکنون شرکت‌های بسیاری هستند که کنترل میراث مجازی افراد را در دست می‌گیرند؛ این میراث می‌تواند شامل چیزهای زیادی شود: از پروفایل آنها در شبکه‌های اجتماعی و گالری‌های عکس‌های آنلاین تا رمز عبور حساب‌های بانکی.

سایت‌های یادبود زیادی در اینترنت به وجود آمده‌اند. در سایتی مانند www.respectance.com سنگ قبرهای آنلاین وجود دارند و می‌توانید برای افراد از دنیا رفته، یک شمع مجازی روشن کنید. افرادی که می‌خواهند پس از مرگشان در این سایت برایشان صفحه یادبود ایجاد شود، باید به ازای هر سال یادبود ۳۰ دلار پیشاپیش بپردازند. سایت‌های بسیار دیگری هم در این زمینه وجود دارند.

یکی از این سایت‌ها را خود ایگلمن به نام www.deathswitch.com ساخته است. می‌توان به صورت رایگان در این سایت عضو شد. در این حالت، هر چند وقت یک بار یک ای‌میل برای اعضا می‌آید و در آن از آنها خواسته می‌شود روی یک لینک کلیک کنند. اگر آنها این کار را برای مدتی طولانی انجام ندهند، سایت فرد را مرده می‌پندارد و برای لیست افرادی که فرد در زمان حیات ساخته بود یک ای‌میل می‌فرستد و خبر مرگ او را به آنها می‌دهد. این سایت امکان این را می‌دهد که در این ای‌میل‌ها، پسوردهای افراد درگذشته هم به دست افرادی برسد که خود فرد تعیین کرده بود.

اگر فردی بمیرد، سایت‌های شبکه‌های اجتماعی به راحتی پسورد او را در اختیار بستگانش نخواهند گذاشت، چرا که ممکن است اطلاعات شخصی

فرد در پروفایل او باشد و نخواهد که پس از مرگش، فرد دیگری از این اطلاعات باخبر شود. یا ممکن است ای‌میل‌هایی داشته باشد که بخواهد حتی پس از این که از دنیا رفت هم کسی آنها را نخواند.

بیش از یک میلیارد نفر در دنیا به اینترنت متصل هستند و به این ترتیب، سرنوشت دارایی‌های دیجیتال آنها یکی از دغدغه‌های امروز به شمار می‌رود. مقالات آکادمیک بسیاری در این باره نوشته شده و وکلا دارند درباره قوانین مربوط تحقیق می‌کنند تا مشخص شود پس از مرگ افراد، چه اتفاقی برای میراث دیجیتال آنها بیفتد.

سه رویکرد به مرگ کاربران

Google

اگر یک کاربر گوگل بمیرد، این شرکت ای‌میل او را به سادگی در اختیار نزدیک‌ترین فرد به او نخواهد گذاشت. کمپانی اصرار دارد که اسناد بسیاری را دریافت کند، از جمله گواهی مرگ و مدرکی که نشان دهد فرد راضی بوده که ای‌میل او به آن فرد برسد. تقریبا یک ماه طول می‌کشد تا اسناد بررسی شود و کنترل ای‌میل به وارث برسد.

Yahoo!

یاهو می‌گوید که اگر اعضای خانواده فرد درگذشته درخواست بدهند، اکانت ای‌میل او را خواهد بست. با این حال این شرکت اجازه دسترسی به ای‌میل فرد را به بازماندگان نخواهد داد. البته اگر فرد درگذشته پیش از مرگ پسورد خود را به افراد مورد اعتمادش داده

باشد، یاهو دسترسی آنها به ای‌میل او را نخواهد بست.

MySpace

اگر بازماندگان، پسورد فرد درگذشته را در اختیار نداشته باشند، به سختی خواهند توانست به پروفایل او در MySpace دسترسی یابند. این شرکت هرگز یک پروفایل را به دلیل غیرفعال بودن در مدتی طولانی نمی‌بندد. اما با این حال، اگر افراد تمایل داشته باشند می‌توانند به این سایت درخواست بدهند که پروفایل فرد درگذشته پاک شود. در این حالت آنها باید گواهی مرگ، گواهی تولد و نامه وکالت را به این شرکت بدهند تا بتوانند این کار را انجام دهند. همچنین اگر ثابت شود که فرد درخواست کرده پسورد او به یکی از بازماندگان داده شود، این کار پس از انجام مراحل قانونی انجام می‌شود، هر چند که پسورد او تغییر یافته و کلمه عبور جدیدی برای او مشخص می‌شود و به فردی که از نظر قانونی وارث پروفایل است داده می‌شود.

نبرد با شرکت‌ها

وقتی مادربزرگ جرمی تومن درگذشت، او به فکر این افتاد که در صورت مرگ خودش چه خواهد شد. تومن که یک طراح وب است می‌گوید: «مادر

بزرگ من مرتبا به هات‌میل سر می‌زد. هنگامی که او دنیا را ترک کرد، هیچ کدام از اعضای خانواده نمی‌دانستیم رمز عبورش چیست تا بتوانیم به اکانت ای‌میل او دسترسی داشته باشیم. ما وارد دعوای حقوقی بسیار بزرگی با شرکت مایکروسافت – مالک هات‌میل – شدیم و سرانجام هم در گرفتن رمز عبور او ناکام ماندیم. حالا از خودم می‌پرسم پس از مرگ من چه اتفاقی برای دارایی‌های آنلاین من خواهد افتاد؟ مساله فقط این نیست که به همسرم پسوردهایم را بدهم، مساله این است که من دارایی‌های دیجیتال بسیاری دارم که برخی از آنها برای شرکتی که برایش کار می‌کنم اهمیت فوق‌العاده‌ای دارد و همسرم حتی نمی‌داند کجا به دنبالشان بگردد.»

یکی از سخنگوهای شرکت یاهو در این باره می‌گوید: «ارتباطات ای‌میلی محتوایی خصوصی و محرمانه است و ما نمی‌توانیم این اطلاعات بسیار شخصی را بدون رضایت فرد به افراد دیگری منتقل کنیم.» هنگامی که یک آدرس ای‌میل در یاهو به نام خود ثبت می‌کنید، این شرکت در بخش شرایط اعلام می‌کند که محتوای ای‌میل شما قابل جابجایی نیست. این کار به دلیل این انجام می‌شود که خیال کاربران از بابت حفظ حریم شخصی‌شان راحت باشد.

شرایط معکوس

البته گاهی هم شرایط برعکس است. مثلا پس از مرگ غیرمنتظره ویلیام برنیستر، روزنامه‌نگار مشهور در سال گذشته، استفانی خواهر او از کمپانی فیس‌بوک خواست که پروفایل او را پاک کند. او این درخواست را به دلایل امنیتی داشت، چرا که اطلاعاتی که ویلیام روی فیس‌بوک گذاشته بود می‌توانست باعث شود تبهکاران بتوانند هویت او را بدزدند. او همچنین می‌گفت که افراد غریبه مرتبا به فرد درگذشته ای‌میل می‌دهند و به شماره تلفن او زنگ می‌زنند و این باعث ناراحتی شدید او شده است.

فیس‌بوک صفحه شخصی او را به صفحه یادبود تبدیل کرد. در این حالت، اطلاعات شخصی فرد از صفحه‌اش پاک می‌شود و تنها دوستان او می‌توانند پروفایلش را ببینند. دیوار پروفایل پاک نمی‌شود تا دوستان بتوانند پیام‌های یادبود خود را روی آن قرار دهند. صفحات افراد در حالی به حالت یادبود می‌رود که یکی از اعضای خانواده آنها یا یکی از دوستان آنها گواهی مرگشان را ارسال کند.

ذخیره آنلاین اطلاعات مهم

جرمی تومن با بهره‌گیری از تجربه‌ای که داشت، یک کمپانی به نام Legacy Locker بنا نهاد. این شرکت به افراد اجازه می‌دهد پسوردهایشان را به صورت آنلاین ذخیره کنند. در این حالت اگر فردی بمیرد، بستگان او می‌توانند با ارسال مدارکی که نشان از مرگ او داشته باشد این اطلاعات را دریافت کنند. این کار راه حلی آسان به نظر می‌رسد، اما مشکلات بزرگی نیز دارد. مثلا چطور می‌توانید به یک شرکت اعتماد کنید و اطلاعات بسیار مهم خود را یکجا در اختیارش قرار دهید؟ یا این که چطور می‌توانید مطمئن شوید سایت پس از مرگ کاربران همچنان به فعالیت خود ادامه می‌دهد؟

باب استیوارت، موسس شرکت VitalLock که با نام «بانک سوییس داده‌ها» هم شناخته می‌شود در این باره می‌گوید: «ما از رمزگذاری‌های بسیار قدرتمندی استفاده می‌کنیم. این کار در سمت کاربر انجام می‌شود و به همین دلیل داده‌ها حتی در مسیر انتقال به سرورهای ما هم قابل خوانده شدن نیستند.»

اما اگر چنین شرکت‌هایی ورشکسته شوند یا توسط شرکتی دیگر خریداری شوند چه می‌شود؟ چنین اتفاقی افتاده و بعضی از سایت‌هایی که قرار بود خدمات پس از مرگ ارائه دهند، خودشان به مرگ دچار شدند. با این حال، دو شرکت VitalLock و iForem که خدمات مشابهی ارائه می‌کند از روش خاصی استفاده می‌کنند. استیون پیرالدی، موسس شرکت iForem می‌گوید: «ما ۳۰ درصد از درآمدهایمان از هر فروش را به یک صندوق کاملا مستقل منتقل می‌کنیم تا مطمئن شویم که به مشکل مالی برنخواهیم خورد. همچنین از فناوری‌های ساده و استانداردهای باز استفاده می‌کنیم تا با انقراض فناوری‌ها، در آینده دچار مشکل نشویم.»

اثبات مرگ

مزیت بزرگ داشتن یک سرویس تحت وب این است که به هر فردی در دنیا می‌توانید سرویس بدهید. اما نکته منفی آن این است که چطور می‌توانید از مرگ یک نفر مطمئن شوید؟ شاید بتوان از چنین سرویس‌هایی سوء استفاده کرد و این کار می‌تواند تبعات فاجعه‌باری به همراه داشته باشد. استیوارت می‌گوید بستگان افراد درگذشته یا مامور اجرای وصیت‌نامه او باید اسنادی مانند گواهی تولد، گواهی مرگ و سند وکالت را به صورت فیزیکی به شرکت VitalLock بفرستند تا از مرگ فرد اطمینان حاصل شود؛ این یعنی بازگشت به همان نقطه اول، یعنی جایی که بستگان فرد درگذشته با اضطراب به دنبال این هستند

که شرکت را مجاب کنند که فرد درگذشته است.

در هر حال، استیوارت می‌گوید شرکتش قصد دارد راه حل دیگری را در پیش بگیرد. طبق این راه حل، شرکت او به افراد ای‌میل می‌زند و اگر آنها پاسخ ندادند، به گروهی از معتمدان فرد (که خود او لیست آنها را تهیه کرده) ای‌میل می‌زند و از آنها می‌خواهد بگویند که آیا فرد مرده است یا نه. نتیجه آرای معتمدان نشان‌دهنده این خواهد بود که آیا به راستی این اتفاق افتاده است یا نه. البته خود فرد می‌تواند مشخص کند که آیا رأی مثبت تمامی معتمدان لازم است یا این که اگر اکثریت آنها رأی به مرگ او دادند کافی است.

اما پس از مرگ این سایت‌ها چه خدماتی ارائه می‌دهند؟ شرکت iForem حتی سال‌ها پس از مرگ فرد هم در تاریخ‌هایی خاص پیام‌هایی از طرف او می‌فرستد. مثلا، افراد می‌توانند هر سال در روز تولد همسر و فرزندانشان برای آنها کارت تبریک بفرستند و به آنها بگویند که چقدر دوستشان داشته‌اند. آنها می‌توانند سال‌ها پس از مرگشان، فارغ‌التحصیل شدن فرزندشان را تبریک گفته و به او بگویند چقدر دوست داشتند در آن هنگام می‌توانستند پیشش باشند. پیرالدی می‌گوید: «تصور کنید این سرویس چقدر می‌تواند تسلی‌بخش باشد. اگر فرض کنید یک خواهر دارید که در استرالیا زندگی می‌کند و تنها ارتباط شما با او کارت تبریکی است که به مناسبت کریسمس برایتان می‌فرستد، اگر این کار پس از مرگ او هم ادامه پیدا کند برای شما به نظر می‌رسد که انگار او نمرده است. البته، یک خط باریک بین تسلی خاطر بازماندگان و عصبانی کردن آنها وجود دارد، خطی که نباید از آن عبور کرد.»

شرکتی که شکست خورد

در سال ۲۰۰۴ بود که ظفر مجید، مدیر شرکت مشاوره‌ای Alphatalk یک سرویس به نام MyLastEmail.com به راه انداخت. در صورتی که کاربران این سرویس می‌مردند و گواهی مرگ آنها هم ارائه می‌شد، شرکت ای‌میل‌هایی به افرادی که کاربر در نظر گرفته بود می‌فرستاد و اطلاعاتی نظیر پسورد ای‌میل و رمز عبور حساب بانکی آنها را برای این افراد ارسال می‌کرد.

مجید می‌گوید تقاضای کمی برای سرویس او وجود داشت، چرا که شبکه‌های اجتماعی خدمات مشابه را به شکل رایگان ارائه می‌دادند و MyLastEmail که از کاربران پول می‌گرفت آینده چندان درخشانی پیش

رو نداشت.

به همین دلیل بود که مجید کار روی سایت را متوقف کرد و سایت او در وضعیتی برزخی است. او می‌گوید: «هنوز به این ایده اعتقاد دارم، اما به نظر می‌رسد نمی‌توان کسب و کار خوبی از این طریق به راه انداخت.»

برای مجید بسیار مهم بود که خدمات او از نظر مالی به مشکل برنخورد: «اگر این اتفاق بیفتد چطور می‌توانید تضمین کنید که سایت شما مثلا ۲۵ سال بعد هم کار کند؟»

او همچنین نگران امنیت است: «باید به شدت به یک شرکت اعتماد داشته باشید تا تمام اطلاعات مهم و حیاتی خود را به آن بسپارید.» اخیرا شرکت T-Mobile UK دچار یک رسوایی بزرگ شد، چرا که برخی از کارکنان فاسد آن، اطلاعات مشتری‌ها را به رقیبان می‌فروختند. اگر این اتفاق برای MyLastEmail یا سرویس‌های مشابه روی دهد چه؟

منبع:computernews.ir

عادات نادرست کاربران کامپیوتر

۱ـ عدم نصب ابزارهای امنیتی

تصور داشتن یک زندگی مجازی آرام بدون استفاده از ابزارهای امنیتی به منظور شناسایی و حذف انواع بدافزارها عملا دور از انتظار است. امنیت تنها در اطلاع دقیق از محتویات لینک‌ها و باز نکردن ایمیل‌های ناشناس خلاصه نمی‌شود. این روزها در امان ماندن از انواع بدافزارها و تکنیک‌های پیشرفته نفوذ و دسترسی امن به اطلاعات، بدون استفاده

از مجموعه‌ای حرفه‌ای از ابزارهای امنیتی عملا غیرممکن است.

بعضی از کاربران با دلایلی غیرمنطقی مثل کند شدن سرعت کامپیوتر هنگام نصب ضدویروس و کندی سرعت اینترنت در صورت فعال بودن فایروال، باورهای اشتباه خود در زمینه عدم استفاده از ابزارهای امنیتی را توجیه کرده و حتی دیگران را هم به این کار تشویق می‌کنند.

در حالی که این دسته از کاربران باید عواقب عدم استفاده از ابزارهای امنیتی را تصور کرده و بعد تصمیم به نصب یا عدم نصب آنها بگیرند. برای مثال شاید نصب یک ضدویروس موجب کندی نامحسوس و قابل تحمل کامپیوتر شود، اما بهتر است ساعات مدیدی که صرف نصب مجدد ویندوز و درایورها به دلیل آسیب دیدن فایل‌های سیستم‌عامل از سوی بدافزارها می‌شود را هم در نظر داشت.

ضمنا بهتر است از نصب نسخه‌های مجانی ضدویروس یا فایروال شرکت‌های غیرمعتبر بپرهیزید؛ این گونه ابزارها به جای محافظت از اطلاعات اقدام به سرقت آنها می‌کنند!

۲ـ عدم پشتیبان‌گیری از اطلاعات

پشیمانی برای آن دسته از کاربران تنبل که از اطلاعات خود پشتیبان تهیه نمی‌کنند، سودی نخواهد داشت. این کاربران با بهانه‌های بی‌پایه و اساس، اطلاعات را در معرض خطرهای جبران‌ناپذیر قرار می‌دهند. ضمنا از کار افتادگی‌هارددیسک امری اجتناب‌ناپذیر است! بهتر است با شیوه‌های گوناگون پیشتیبان‌گیری آشنا شده و از نرم‌افزارهای حرفه‌ای این حوزه که نیازی به دخالت شما نداشته و کار را به صورت خودکار انجام می‌دهند، استفاده نمایید. همچنین بهتر است فایل‌های پشتیبان را روی هارددیسک اکسترنال قرار دهید.

۳ـ عدم پشتیبان‌گیری آنلاین

یکی از بهترین و امن‌ترین روش‌های موجود برای ذخیره‌سازی کاملا امن اطلاعات، ارسال آنها به فضای ابرهاست. سرویس Live شرکت مایکروسافت ۲۵ گیگابایت فضای کاملا مجانی در اختیار کاربران قرار داده و امکان آپلود انواع فایل‌های حجیم را میسر کرده است. البته در Gmail گوگل هم تقریبا ۸ گیگابایت فضا در اختیار دارید. با استفاده از نرم‌افزارهایی مثل Gmail Drive یا SkyDrive Explorer می‌توان این فضاهای رایگان ابری را در قالب درایو به ویندوز اضافه

کرد و با استفاده از قابلیت کشیدن و رها کردن (Drag & Drop) اقدام به پشتیبان‌گیری از داده‌های مهم نمود.

البته این راه حل فقط برای کاربران مرفه (از نوع بی‌درد) است که اینترنت پرسرعت دارند و می‌توانند به راحتی فایل‌ها را آپلود و دانلود کنند!

۴ـ پاسخ به هرزنامه‌های تبلیغاتی

یکی از دلایل مهمی‌که اسپمرها را تشویق به ادامه کار می‌کند، کلیک کاربران روی لینک‌های موجود در هرزنامه‌های تبلیغاتی و حتی پاسخ به این گونه ایمیل‌هاست. بله اسپمرها کلیک روی لینک‌های Remove me یا Unsubscribe me (به منظور حذف از لیست ارسال) را پاسخی از سوی کاربران محسوب کرده، از فعال بودن آن آدرس ایمیل مطمئن شده و سیل هرزنامه‌ها را با شدتی بیشتر به سوی کاربر هدایت می‌کنند.

در صورتی که پیام تبلیغاتی از سوی یک شرکت معتبر ارسال شده باشد، کلیک روی چنین گزینه‌هایی خطرناک نیست؛ البته فراموش نکنید که این روزها با حرفه‌ای‌تر شدن خرابکاران، جعل آدرس ایمیل شرکت‌های معتبر هم کار سختی نبوده و بهتر است در این گونه موارد نیز جوانب احتیاط را در نظر داشته باشید.

۵ـ حمل دستگاه‌های روشن

حمل نوت‌بوک روشن از اتاق خواب تا نشیمن ایرادی ندارد، اما جابه‌جایی آن مثلا از اداره تا منزل، پیاده‌روی طولانی، هنگام بالارفتن از پله‌ها و … بسیار خطرناک بوده و امکان وارد آمدن صدمات جدی به دستگاه وجود دارد. در چنین مواقعی که هارددیسک در حال چرخش است، امکان از کار افتادگی آن در هر لحظه وجود دارد.

از این رو توصیه می‌کنیم هنگام جابه‌جایی، نوت‌بوک یا نت‌بوک، آن را خاموش کنید، مگر اینکه مدل مورد استفاده از نمونه‌های مقاوم در برابر ضربه و تکان‌های شدید باشد. ضمنا ریسک افتادن دستگاه از دست را هم نباید فراموش کرد. در این گونه مواقع بهتر است از حالت Hibernate که در آن، محیط کار ذخیره می‌شود، استفاده نمود. دقت داشته باشید در حالت Sleep هر لحظه امکان روشن شدن اتفاقی وجود دارد.

۶ـ نوت‌بوک در رختخواب!

استفاده از نوت‌بوک در رختخواب اشکالی ندارد، اما پرز و کرک بالش و لحاف و … موجب گرفتگی پورت‌ها یا بسته شدن منافذ تهویه دستگاه و در نتیجه گرم شدن و در نهایت خرابی دستگاه خواهد شد. برای رفع این مشکل بهتر است از میز نوت‌بوک به منظور حفظ جریان هوا بین نوت‌بوک و سطوح پرزدار و همچنین خنکسازی دستگاه توسط فن استفاده کنید. فراموش نکنید که استفاده از نوت‌بوک در حالت درازکش یا دیگر وضعیت‌های بدنی نامطلوب، اثرات سو روی سلامت شما خواهد داشت.

۷ـ چاپ همه چیز

در صورت وجود نسخه دیجیتال یک سند چه نیازی به چاپ نسخه کاغذی وجود دارد؟ گاهی اوقات مطالب یک وب‌سایت نظرتان را جلب کرده و برای مطالعه بهتر آن را در قالب Word تنظیم و چاپ می‌کنید. بهتر نیست چنین سندی را تبدیل به فایل PDF کنید و به راحتی آن را در کامپیوتر یا حتی گوشی همراه مطالعه کنید. ضمنا چاپ کمتر، برابر با قطع کمتر درختان و ایفای نقشی هر چند جزیی در نجات کره زمین است.

۸ـ اظهار نظرهای آنلاین

در آغاز یک روز کاری بعد از نشتن پشت میز در اداره، برگه اخراج را روبروی خود خواهید دید و متوجه از دست رفتن شغل محبوب تان خواهید شد. اگر چه باور این مسئله تا حدودی سخت است اما امکان چنین اتفاقی دور از ذهن نیست. شاید یکی از اظهارنظرهای (کامنت‌های) قدیمی‌شما در مورد عملکرد یکی از همکاران که هم اکنون رئیس شرکت شده، علت اخراج شدن تان باشد.

البته بعید نیست در وب سایت یا وبلاگ شخصی خود، یا در نظرات شبکه‌های اجتماعی از شرکت به خاطر بی‌کفایتی مدیران و کارکنان هم گله کرده باشید. حال یکی از مسئولان یا کارکنان بانفوذ با مشاهده چنین اظهارنظرهایی که حتی آنها را با نام مستعار منتشر کرده‌اید، موجبات بیکار شدن‌تان را فراهم کرده است؛ پس حتی نام مستعار (نام کاربری در وب سایت‌ها) خود را نزد همکاران فاش نکنید.

امروزه مسئولان با یک جستجوی ساده نام و نام خانوادگی، آدرس ایمیل یا نام مستعار، قادر به مشاهده نظرات شما در اینترنت هستند. بهتر است جوانب احتیاط را رعایت کرده و از اظهارنظرهای بی‌مورد در فضای وب خودداری نمایید.

۹ـ رها کردن نوت‌بوک در خودرو

سارقان زیادی منتظر سرک کشیدن به درون خودروهای پارک شده هستند تا در صورت وجود چیزی با ارزش، دست به کار شوند. اگر نوت‌بوک خود را اغلب در خودرو به همراه دارید، باید احتیاط زیادی به خرج دهید. بهتر است هنگام پیاده شدن از خودرو نوت‌بوک را نیز با خود بردارید.

ضمنا استفاده از ابزارهایی موسوم به قفل سفر یا Travel Lock هم بد نیست. قفل سفر که نمونه‌های مختلفی دارد، به نوت‌بوک متصل شده و در صورت جدا شدن صدایی ناهنجار و بسیار بلند پخش می‌کند. ضمنا در ویندوز۷ و ویستا نیز با استفاده از ویژگی Bitlocker می‌توان کار رمزنگاری اطلاعات روی هارددیسک را به منظور عدم دسترسی دیگران به آنها انجام داد.

۱۰ـ عدم داشتن آدرس ایمیل اضافه

کاربران حرفه‌ای چندین آدرس ایمیل داشته و از هر کدام برای مقاصدی

خاص استفاده می‌کنند. برای مثال آدرس ایمیل شخصی، در اختیار دوستان درجه یک و افراد خانواده قرار گرفته و آدرس ایمیل کاری را برای مکاتبات کاری در نظر می‌گیرند.

بهتر است آدرس شخصی را در اختیار خبرنامه‌ها، سرویس‌های وب و … قرار ندهید، چرا که پیام‌های تبلیغاتی یا اطلاع‌رسانی‌های این گونه سایت‌ها شما را کلافه خواهند کرد. برای ثبت‌نام در بعضی سایت‌ها و استفاده از امکاناتی مثل دسترسی به لینک دانلود مجبور به وارد کردن آدرس ایمیل هستید؛ چنین سایت‌ها و سرویس‌هایی ایمیل‌ها را نگه‌داری کرده و بعضا تبلیغات خود را از این طریق به شما ارسال کرده و حتی گاهی اوقات آنها را به اسپمرها می‌فروشند.

علی‌رغم قول عدم استفاده تجاری از ایمیل‌ها از سوی این سایت‌ها، گاهی اوقات این اتفاق نیفتاده و به بازدیدکنندگان خیانت می‌شود. فراموش نکنید حتی در صورت متعهد بودن سایت، احتمال هک شدن پایگاه داده و دسترسی هکرها به ایمیل‌ها وجود دارد. یک ایمیل اضافی ساخته و در موارد ضروری آن را در اختیار وب‌سایت‌ها قرار دهید.

۱۱ـ عدم استفاده از کلیدهای میانبر

برخی از کاربران آشنایی بسیار کمی با میانبرهای کیبورد داشته و حتی نمی‌دانند فشار دادن کلیدهای Ctrl+C کار کپی و Ctrl+V کار Paste را انجام می‌دهد. البته یادگیری تمامی میانبرهای کیبورد و عادت به استفاده از آنها کار ساده‌ای نیست، اما هر چه میانبرهای بیشتری یاد بگیرید، سرعت شما در انجام کارها بیشتر خواهد شد. از هم‌اکنون ماوس را کنار گذاشته و استفاده از میانبرهای پرکاربرد را آغاز کنید.

۱۲ـ نصب نرم‌افزارهای غیرضروری

“چرا ویندوزم کند شده؟” این سوالی است که به شنیدن آن عادت داریم و عوامل گوناگونی در بروز آن نقش دارند: احتمالا ۳ نرم‌افزار مجزای پیام‌رسان، ۴ مرورگر اینترنتی مطرح و به همراه ۷ نوارابزار روی هر یک نصب کرده‌اید و فایل‌های زیادی روی دسکتاپ یا پوشه Documents ذخیره نموده‌اید و …

عده‌ای عادت به تست و بررسی انواع نرم‌افزارهای غیرضروری و ناشناخته مثل انواع و اقسام پخش‌کننده‌های چندرسانه‌ای، ابزارهای امنیتی، مرورگرهای مختلف، بازی، محافظهای صفحه نمایش و دیگر

موارد مشابه دارند. صرفنظر از مسایل امنیتی، نصب انواع ابزارهای غیرضروری مشکلاتی از قبیل کند شدن یا قفل کردن سیستم را برای کاربر به ارمغان می‌آورد. بهتر است چند ابزار مطرح برای نیازهای گوناگون خود در نظر گرفته و تنها از آنها استفاده نمایید.

ضمنا بسیاری از برنامه‌های ناشناخته مثل نوارابزارها به ندرت رد پایی از خود به جا گذاشته و حذف کامل آنها گاهی اوقات غیرممکن است، به طوری که تنها راهکار موجود برای حذف آنها نصب مجدد ویندوز است.

۱۳ـ بی توجهی به خطرات اینترنت

هر روز اخبار جدیدی در مورد جرایم اینترنتی از قبیل فاش شدن اطلاعات شخصی و قرار گرفتن عکس و فیلم‌های خانوادگی روی اینترنت در رسانه‌ها پخش می‌شود. توصیه اول برای کاهش خطرات اینترنت پرهیز از دوست‌یابی اینترنتی یا حداقل عدم اعتماد به چنین افرادی است.

هیچ‌گاه از تصاویر واقعی در پروفایل خود استفاده نکرده یا آن را به عنوان آواتار انتخاب نکنید. از قرار دادن فیلم‌ها و عکس‌های خانوادگی در اینترنت اجتناب کنید؛ اگر امکان خرابی چنین داده‌هایی وجود دارد، بهتر است آنها را روی حساب ایمیل یا فضاهای ابری ذخیره نمایید.

ایمیل یا حساب بانکی خود را از کامپیوترهای عمومی چک نکنید، زیرا احتمال نصب Keylogger سخت‌افزاری یا نرم‌افزاری در این سیستم‌ها و در نتیجه فاش شدن اطلاعات حیاتی، بسیار بالاست.

۱۴ـ استفاده از رمز عبور واحد در کلیه حساب‌های کاربری

بعضی افراد برای تمام حساب‌های کاربری از جمله ایمیل، حساب بانکی، شبکه‌های اجتماعی و … یک رمز عبور انتخاب می‌کنند. از این رو هکر با دستیابی به رمز عبور یکی از حساب‌های چنین شخصی امکان دسترسی به دیگر حساب‌ها را خواهد داشت.

از سوی دیگر انتخاب رمز عبورهای منحصر به فرد برای هر وب‌سایتی که در آن ثبت‌نام می‌کنید کار آسانی نیست؛ توصیه می‌کنیم از نرم‌افزارهای مدیریت رمز عبور مثل Roboform استفاده کنید.

ضمنا از قابلیت به خاطر سپاری خودکار رمز عبور در مرورگر نیز استفاده نکنید. امروزه مرورگرهای اینترنتی هدف اول خرابکاران

بوده و هر لحظه احتمال نفوذ به آنها و لو رفتن رمز عبورها وجود دارد. در صورت استفاده از کامپیوتر مشترک، ریسک مشاهده رمز عبور توسط دیگران را هم باید به جان خرید.

منبع:computernews.ir

چـــرا کامپیوترهـــا در انجـــام محاسبات ریاضی ناتوان هستند؟

کامپیوترها هنوز در انجام کارهای هوشمندانه مشکلات بسیاری دارند،

اما اینکه از آنها بخواهیم محاسبات را انجام دهند که انتظار زیادی نیست، هست؟

برنامه‌نویسان به خوبی می‌دانند که گاهی ماشین حساب آنلاین گوگل و برنامه اکسل مایکروسافت حتی از پس محاسبات ساده هم برنمی‌آیند. اما به هر حال، مشکلات گاه و بی‌گاه آنها را نمی‌توان اشکال دانست. در حقیقت، این مشکلات نشان نمی‌دهند که کامپیوترها در انجام کارهای ریاضی ناتوان هستند!

کامپیوترها محاسبات را به شیوه کاملا متفاوتی نسبت به انسان‌ها انجام می‌دهند و اغلب هم به پاسخ نادرست می‌رسند. برای آنهایی که هنوز متقاعد نشده‌اند که کامپیوترها قادر به انجام اعمال ساده ریاضی نیستند، با چند مثال شروع می‌کنیم.

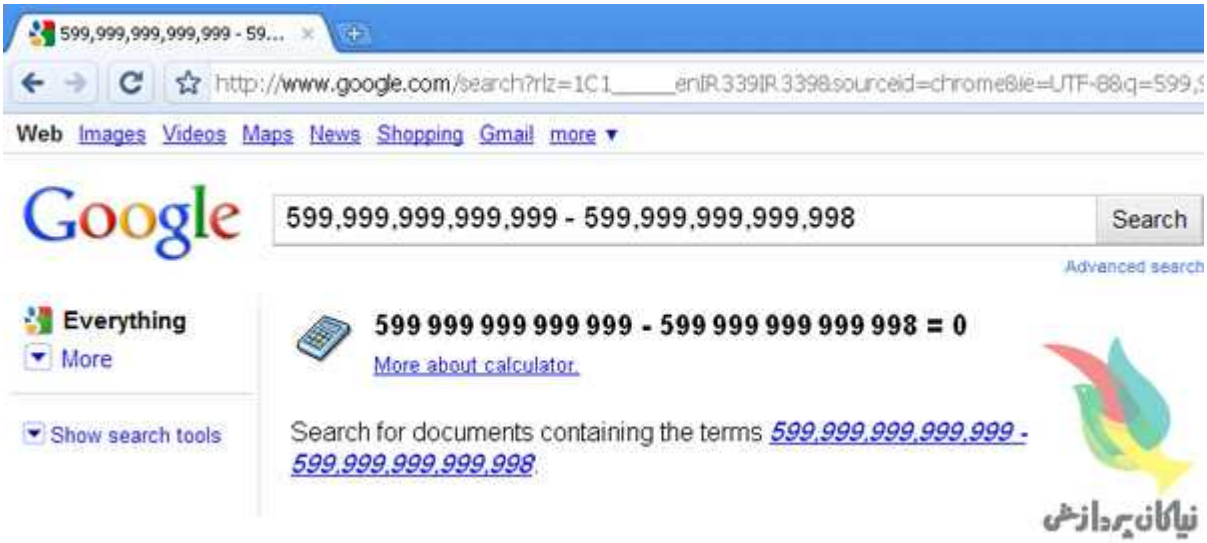
مثلا ماشین حساب گوگل را در نظر بگیرید. برای استفاده از آن کافیست عبارت ریاضی مورد نظر را در کادر جستجوی گوگل تایپ کنید و

آن را جستجو کنید تا نتیجه را ببینید، مثلا بنویسید sqrt+۹*۵ 3^(9) تا ببینید چه جوابی روی صفحه نمایش داده می‌شود. به طور حتم جواب درست است. اکنون محاسبه دیگری انجام می‌دهیم.

در کادر جستجوی گوگل عبارت زیر را تایپ کنید (شکل ۱):

۵۹۹,۹۹۹,۹۹۹,۹۹۹,۹۹۸ – ۵۹۹,۹۹۹,۹۹۹,۹۹۹,۹۹۹

مشخص است که پاسخ این عبارت ۱ است، اما گوگل اعتقاد دارد پاسخ این عبارت صفر می‌شود!



(شکل۱)

یا یک محاسبه ساده دیگر انجام دهیم. در یکی از سلول‌های یک فایل اکسل ۲۰۰۷ عبارت زیر را بنویسید:

=۸۵۰*۱٫۷۷

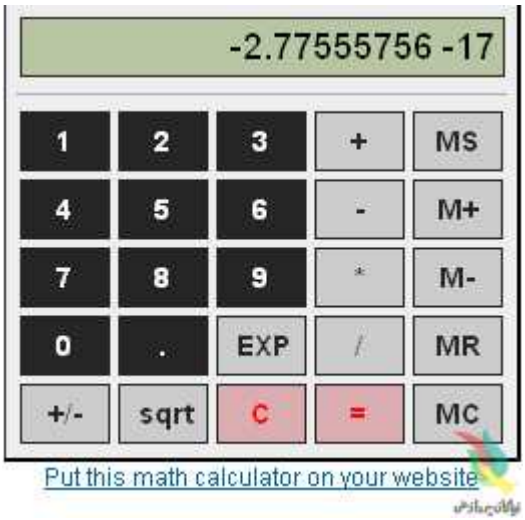
اگر این روش کار نکرد (یعنی در واقع کار کرد!)، این کار را در نسخه قدیمی‌تری از اکسل انجام دهید تا ببینید که اکسل به جای پاسخ صحیح که ۶۵۵۳۵ است، عدد ۱۰۰۰۰۰ را نشان می‌دهد. البته این ایراد در برخی از نسخه‌های اکسل درست شده است.

به همین ترتیب، در ماشین حساب‌های آنلاین (مانند http://calculator.net) عبارت زیر را محاسبه کنید:

۱٫۰ – ۰٫۹ – ۰٫۱

خواهید دید که به جای جواب صحیح که صفر است، با مقدار عجیب -

۲٫۷۷۵۵۵۷۵۶ E-17 روبرو می‌شوید که نماد علمی عدد -۰٫۰۰۰۰۰۰۰۰۰۰۰۰۰۰۲۷۷۵۵۵۷۵۶ است (شکل ۲).



(شکل۲)

این جواب خیلی از صفر دور نیست اما چرا ماشین حساب پاسخ صحیح را نداد، پاسخی که به حدی روشن است که حتی فردی که حساب ساده را هم بلد نیست می‌تواند آن را به دست آورد؟

روش انجام محاسبات در کامپیوتر

با آنکه کامپیوترها می‌توانند اعداد صحیح را نگه دارند، اما برای محاسبات عمومی ریاضی اعداد را در قالب ممیز شناور (Floating Point) ذخیره می‌کنند که روشی بسیار کارآمد در زمینه صرفه‌جویی در مصرف حافظه است.

مثلا نمایش ممیز شناور با دقت دوگانه، از ۶۴ بیت برای ذخیره هر عدد استفاده می‌کند و در آن می‌توان اعداد از ۱۰۳۰۸- تا ۱۰۳۰۸ (یعنی منفی و مثبت یک با ۳۰۸ صفر در مقابلش) را ذخیره کرد. همچنین اعداد کسری حتی به کوچکی ۳۰۸-۱۰ (صفر، ممیز، ۳۰۷ صفر و سپس ۱) هم قابل ذخیره‌سازی هستند.

به همین ترتیب اگر از همین ۶۴ بیت برای ذخیره اعداد صحیح استفاده شود، می‌توان از اعداد ۹,۲۲۳,۳۷۲,۰۳۶,۸۵۴,۷۷۵,۸۰۸- تا ۹,۲۲۳,۳۷۲,۰۳۶,۸۵۴,۷۷۵,۸۰۷+ را البته بدون قسمت اعشاری در آن نگه داشت.

اما چگونه این حجم انبوه از اعداد در تنها ۶۴ بیت جا می‌گیرند؟

پاسخ این است: تقریب! از آن ۶۴ بیت، یکی برای نمایش علامت به کار می‌رود که نشان دهد عدد مثبت است یا منفی. ۵۲ بیت برای مانتیس (خود عدد) استفاده می‌شوند و ۱۱ بیت دیگر توان را نشان می‌دهند (یعنی اینکه چند صفر باید گذاشته شود و ممیز هم کجای عدد قرار می‌گیرد).

با آنکه طیف گسترده‌ای از اعداد را می‌توان به شیوه ممیز شناور نشان داد، اما دقت در عمل کمتر از قالب اعداد صحیح است چون تنها ۵۲ بیت برای این کار در نظر گرفته شده است. در عمل، ۵۲ بیت باینری تنها قادر به نشان دادن یک عدد ۱۶ رقمی مبنای ده است و اعدادی که رقم ۱۷ام آنها با هم فرق دارند، از دید کامپیوتر معادل در نظر گرفته می‌شوند.

به همین دلیل است که گوگل مقدار ۵۹۹,۹۹۹,۹۹۹,۹۹۹,۹۹۹ – ۵۹۹,۹۹۹,۹۹۹,۹۹۹,۹۹۸ را صفر می‌داند؛ البته مشخص است که مانتیس ماشین حساب گوگل کمتر از ۵۲ بیت است.

اما چرا محاسبه ۰٫۱ – ۰٫۹ – ۱٫۰ برابر با صفر نمی‌شود؟ به نظر می‌رسد شاید این موضوع ربطی به محدودیت ۶۴ بیتی نداشته باشد، چون ما با اعداد کوچکی سر و کار داریم. اما این طور نیست.

کامپیوترها اعداد را در مبنای دو ذخیره می‌کنند. عدد ۰٫۱ در مبنای ده تنها یک رقم معنی‌دار دارد، اما در نمایش مبنای دو مانتیس آن چندین عدد است که مرتبا تکرار می‌شوند. یعنی، از هر چند بیت که می‌خواهید برای ذخیره اعداد استفاده کنید، ۰٫۱ در مبنای دو هرگز با دقت قابل نمایش نخواهد بود.

تفاوت بین جواب محاسبه شده و پاسخ درست معمولا بسیار جزیی است و شاید این خطا را بی‌اهمیت بشمارید. اما این خطاها می‌توانند روی هم انباشته شده و تبعاتی جدی داشته باشند.

پردازشگری که تقسیم بلد نبود

اینتل، پنتیوم که پنجمین نسل پردازنده‌های x86 بود را در مارس ۱۹۹۳ به بازار عرضه کرد. در نسل‌های پیشین، برخی پردازنده‌ها تنها قادر بودند اعمال محاسباتی را روی اعداد صحیح انجام دهند. اما تمامی پنتیوم‌ها همگی یک واحد ممیز شناور (FPU) داشتند که قطعه‌ای سخت‌افزاری بود و کار محاسبات ممیز شناور را انجام می‌داد و باعث شده بود سرعت پردازنده به شدت عالی باشد، چون محاسبات اعشاری روی

اغلب پردازنده‌هایی که این واحد را نداشتند باید با استفاده از عملیات اعداد صحیح و به صورت نرم‌افزاری انجام می‌شد.

اما این کار در نهایت به زیان اینتل تمام شد. در ژوئن ۱۹۹۴ و کمی پس از آغاز فروش کامپیوترهای مبتنی بر پنتیوم، تامس نایسلی که استاد ریاضی دانشگاه لینچبرگ ویرجینیا بود متوجه شد برنامه‌ای که نوشته در هر بار اجرا جواب‌های متفاوتی می‌دهد.

او همان برنامه را روی ماشین‌های مختلف اجرا کرد و متوجه شد مشکل زیر سر پردازنده پنتیوم، و به ویژه دستور FDIV آن است که برای تقسیم اعداد با ممیز شناور به کار می‌رود. با آنکه این مشکل تنها روی بخشی جزیی از تقسیم‌های ممیز شناور تاثیر می‌گذاشت، اما می‌توانست نتایج بدی به همراه داشته باشد. مثلا تقسیم ۴۱۹۵۸۳۵ بر ۳۱۴۵۷۲۷ منجر به جواب ۱٫۳۳۳۷ می‌شد، در حالی که پاسخ درست ۱٫۳۳۳۸ بود.

FPU پنتیوم از الگوریتم SRT برای تقسیم اعداد ممیز شناور استفاده می‌کرد. هر چند روش‌های ساده‌تر و روشن‌تری هم برای تقسیم اعداد وجود دارد، اما الگوریتم SRT سرعت بسیار بالاتری نسبت به سایر روش‌ها داشت. عملکرد SRT به زبان ساده به این ترتیب بود که در یک جدول به دنبال یک سری مقادیر می‌گشت. این جدول حدود ۱۰۰۰ خانه داشت، اما به دلیل خطای تولید پنج خانه آن پر نشده بود.

با آنکه اندری گرو، مدیر اجرایی اینتل بر این باور بود که این مشکل یک کاربر معمولی را هر ۲۷ هزار سال یکبار به دردسر می‌اندازد، اما تخمین IBM بسیار بالاتر از اینتل بود: یک مشکل به ازای هر ۲۴ روز.

در نهایت اینتل تصمیم گرفت پردازنده‌های تولید شده را از بازار جمع کرده و آنها را با پردازنده‌های بهتر جایگزین نماید، پیشنهادی که مورد استقبال چندانی هم قرار نگرفت. با این حال باعث شد کاربران کامپیوتر برای اینتل لطیفه بسازند؛ مانند این: می‌دانید چند طراح پنتیوم برای عوض کردن یک لامپ لازم است؟ پاسخ: ۱٫۹۹۹۰۴۲۷۴۰۱۷ نفر!

در خطاهایی که تاکنون دیده‌ایم مشکل این بوده که اعداد در مانتیس جا نمی‌گرفته‌اند. اما با توجه به طیف بسیار گسترده اعدادی که می‌توانند در قالب ممیز شناور جا بگیرند، احتمال این خطاها بسیار کم است.

اما هنگامی که صحبت از اعداد صحیح می‌کنیم، اوضاع می‌تواند وخیم‌تر شود. یک متغیر صحیح ۶۴ بیتی حداکثر قادر به ذخیره عدد ۹,۲۲۳,۳۷۲,۰۳۶,۸۵۴,۷۷۵,۸۰۷ است. اگر به این عدد ۱ اضافه کنید، دچار سرریز (Overflow) شده و مقدار ۹,۲۲۳,۳۷۲,۰۳۶,۸۵۴,۷۷۵,۸۰۸- را به ما می‌دهد (به منفی پشت عدد دقت کنید). اتفاقی کاملا مشابه در اولین پرواز موشک آریان ۵ آژانس فضایی اروپا روی داد.

البته آن رویداد حتی ساده‌تر از این بود و تنها شامل کپی کردن یک عدد ذخیره شده در قالب ممیز شناور به محلی برای یک عدد صحیح بود. این محل ۱۶ بیت جا داشت و حداکثر عدد ۳۲۷۶۷ را می‌توانست ذخیره کند. البته عدد اصلی بزرگ‌تر از این بود و در نتیجه سرریز روی داد. این خطا مشکلات دیگر را در پی داشت و به طور خلاصه بگوییم: در نهایت آرین ۵ یکی از گران‌ترین آتش‌بازی‌های تاریخ دنیا شد (شکل ۳).

شکل ۳: موشک آرین ۵ قبل از انفجار در هوا

احتمالا از خود پرسیده‌اید آیا کامپیوترهای آینده این مشکلات را

برطرف می‌کنند یا نه. اما جالب است بدانید اغلب خطاهایی که به آنها اشاره کردیم، به جز مشکل سخت‌افزاری اینتل همه قابل پیش‌گیری بوده‌اند و عملا خطاهایی نرم‌افزاری به شمار می‌رفته‌اند.

مثلا خطای سرریز موشک آرین ۵ در اصل خطا نیست، چون پردازنده قرار بوده به این سبک کار کند. هر گاه سرریز روی می‌دهد، پردازنده Flag مربوط به آن را ۱ می‌کند تا برنامه متوجه شود.

اما برنامه‌نویسان آرین ۵ جایی برای بررسی Flag سرریز در برنامه در نظر نگرفته بودند و اگر این کار را می‌کردند، می‌توانستند اقدامات تصحیحی لازم را انجام دهند. به این ترتیب، برنامه‌نویسان باید مراقب خطاها باشند، هر چند که این کار به کاهش سرعت برنامه می‌انجامد.

در هر صورت، نتیجه برخی از تقسیم‌ها هرگز به صورت دقیق ذخیره نخواهد شد. دیدیم که یک تقسیم بر ۱۰ رشته‌ای نامتناهی در مبنای ۲ است. اما در مبنای ۱۰ هم با مشکلات مشابه برخورد داشته‌ایم؛ مثلا یک تقسیم بر ۳ مساوی می‌شود با ۰٫۳۳۳… تا بی‌نهایت.

می‌توان از روش‌های مختلفی برای حل مشکل استفاده کرد، مثلا جواب برخی عبارت‌های مشکل‌ساز را به صورت مجزا ذخیره کرد تا در صورت لزوم از آنها استفاده شود. درست است که کامپیوترها در انجام کارهای ریاضی ناتوان هستند، اما همیشه راهی برای حل این نقاط ضعف آنها وجود دارد. بنابراین بهتر است بگوییم برنامه‌نویسان در انجام کارهای ریاضی ناتوان هستند؛ اگر همه آنها نه، حداقل بعضی از آنها!

منبع:computernews.ir

بهبود سرعت رایانه های قدیمی

رایانه های قدیمی را با کمترین هزینه, سریع و قدرتمند کنید

از روزی که رایانه خود را خریده‌اید، چند سال می‌گذرد؟ کم‌کم دارید نشانه‌هایی را از کاهش سرعت این سیستم در مواقعی که فشار کار بر آن زیاد است مشاهده می‌کنید. چاره کار چیست؟

باید دست به ارتقای این سیستم بزنید یا به فکر خرید رایانه جدیدی باشید. معلوم است با بودجه‌های محدود دانشجویی، حتما شما ارزان‌ترین گزینه را انتخاب می‌کنید. البته هر کسی ترجیح می‌دهد تا جایی که ممکن است، راه چاره‌ای برای استفاده از رایانه قدیمی‌اش پیدا کند تا برنامه‌ها و داده‌های خود را روی آن حفظ کرده و مجبور به پشتیبان‌گیری با بک‌آپ گرفتن از دیسک سخت رایانه قبلی و انتقال داده و نصب مجدد برنامه‌های نرم‌افزاری مورد نیاز خود روی یک رایانه جدید نشود. یک رایانه معمولی حدود چهار سال عمر مفید دارد. با وجود این، اگر در این مدت آن را در شرایط مناسبی نگهداری کنید، ممکن است بیشتر از اینها نیز عمر کند. البته این موضوع قطعی نیست و به خیلی از عوامل بستگی دارد.

گاهی ارتقای قطعات سخت‌افزاری سیستم می‌تواند کارساز باشد و وضع را بهبود بخشد، اما انجام این کار به صرف وقت و هزینه نیاز دارد. با وجود پیشرفت سریع سخت‌افزارها و افت قیمت سریع قطعات، گاهی خرید یک رایانه جدید مقرون به صرفه‌تر است.

پیش از این که به فکر خرید رایانه جدید بیفتید، هنوز کارهایی هست که شاید با انجام آنها بتوانید روح تازه‌ای به کالبد سیستم قدیمی خود بدمید و سرعت آن را به حالت اولیه‌اش برگردانید. برای این کار در نظر داشتن چند نکته ضروری است. یکی از مهم‌ترین نکات این است که شما چقدر باید هزینه کنید که رایانه‌تان به حالت اولیه‌اش برگردد. اگر سیستم شما یکی از آن سیستم‌های ارزان‌قیمت برای انجام کارهای ساده باشد، مطمئن باشید ارزش ارتقا و صرف هزینه را ندارد، زیرا شما با فناوری قدیمی سطح پایین سر و کار داشته و مجبورید برای بازگرداندن سرعت اولیه سیستم، تعداد زیادی از قطعات را عوض

کنید. به همین دلیل ممکن است ارتقای این سیستم قدیمی، به اندازه یک رایانه نو، هزینه روی دستتان بگذارد. البته راه‌های نرم‌افزاری نیز برای این کار هست، اما آن راه‌ها بیشتر برای رایانه‌های خیلی قدیمی کاربرد دارد. اگر رایانه شما زمان خرید جزو سیستم‌های سطح بالا باشد که فکر کنید ارزش ارتقا دادن را دارد، می‌توانید آن را با اضافه کردن مقداری حافظه رم ارتقا دهید.

ارتقای حافظه

افزایش مقدار رم که یکی از ساده ترین راه‌های ارتقای سیستم‌های قدیمی است، می‌تواند در بهبود سرعت آن مؤثر باشد. پیش از شروع به کار باید توجه داشته باشید همه رم‌ها یکسان نیستند. رم مورد استفاده در دسکتاپ با رم لپ‌تاپ‌ها فرق دارد. ابتدا باید تعیین کنید حافظه دستگاه شما از چه نوع و دارای چه سرعتی است. در حال حاضر حافظه رایانه‌ها شامل انواع DDR۲ ،DDR۱ و DDR۳ است که بیشتر مادربوردها فقط یک نوع از آنها را پشتیبانی می‌کند. در مرحله بعد باید مقدار باس و سرعت آنها را تعیین کنید. پس از فهمیدن پارامترهای مورد نیاز حافظه سیستم خود، باید به این موضوع پی ببرید که مادربورد سیستم شما تا چه مقدار حافظه را مورد پشتیبانی قرار می‌دهد. بعد از انجام این کارها می‌توانید با توجه به نیاز سیستم و بودجه خود به خرید مقدار حافظه‌ای که لازم دارید، از بین ماژول‌های رم موجود در بازار، یکی را انتخاب کنید.

نصب رم

برای نصب رم روی مادربورد دسکتاپ، ابتدا رایانه را خاموش کرده و از برق بکشید. سپس تمام کابل‌ها و لوازم جانبی متصل به آن را قطع

کنید. بعد از آن در کناری کیس رایانه را باز کرده و یکی از قسمت‌های فلزی داخل کیس را لمس کنید تا الکتریسیته ساکن بدن شما تخلیه شود. الکتریسیته ساکن می‌تواند قطعات داخلی رایانه شما را معیوب سازد. مادربورد سیستم را که برد الکترونیکی بزرگی است و همه قطعات رایانه به آن متصل می‌شود، پیدا کنید و محل شکاف‌های اتصال یا اسلات ماژول‌های رم را بیابید.

همه مادربوردها دست‌کم تعداد دو یا چهار عدد از این شکاف‌های اتصال حافظه که حدود ده سانتی‌متر طول داشته و ممکن است در رنگ‌های مختلف باشد، روی خود دارند. برای متصل کردن ماژول رم جدید، ضامن‌های کوچک پلاستیکی دو طرف این پایه‌های اتصال حافظه را به پایین بکشید. لبه قسمت فلزی طلایی رنگ ماژول حافظه را که از آنجا رم به شکاف مادربورد متصل می‌شود، با پایه اتصال مماس کنید و روی شکاف پایه قرار داده، نوک انگشتان اشاره و شست دست خود را روی دو طرف ماژول حافظه بگذارید و به پایین فشار دهید. رم با صدای کلیک مانندی جا می‌افتد.

حالا برای اطمینان از جا افتادن ماژول رم در شکاف اتصال، ضامن‌های پلاستیکی دو طرف پایه شکاف رم را بالا بکشید تا در فرو رفتگی نیم دایره دو طرف برد رم جا بیفتد. هنگام ارتقای سیستم، ممکن است چند ماژول رم با مشخصات مشابه اما با ظرفیت‌های متفاوت داشته باشید. برای مثال ممکن است یک ماژول رم ۵۱۲ مگابایتی در یکی از شکاف‌های حافظه از پیش متصل داشته باشید و بخواهید دو عدد ماژول رم دیگر یک گیگابایتی را در دو شکاف اتصال حافظه دیگر نصب کنید. برای این کار باید از نظر انتخاب شکاف‌های اتصال، ترتیبی را رعایت کنید که ما در اینجا راه آن را برای شما توضیح می‌دهیم.

اگر رایانه شما قدیمی و با حافظه‌های DDR است، شما باید ماژول‌های رم را به ترتیب بزرگی اندازه حافظه نصب کنید. در این نوع رایانه‌ها ماژول رم با بیشترین ظرفیت را در شکاف اتصال شماره ۰ (در رایانه پایه‌های شکاف اتصال رم از شماره ۰ شروع می‌شوند)، در مرحله بعد دومین ماژول رم از نظر ظرفیت در شکاف شماره ۱ و ماژول ۵۱۲ مگابایتی را در شکاف شماره ۲ نصب کنید. برای انواع رم جدیدتر DDR، DDR۲ و DDR۳ ترتیب تقدم شکاف‌های اتصال حافظه با روش کدگذاری رنگ‌هایشان شناخته می‌شود. در مثال بالا دو ماژول یک گیگابایتی در شکاف‌هایی با رنگ مشابه نصب می‌شوند (برای مثال A۱ و B۱) و ماژول ۵۱۲ مگابایتی در شکافی با رنگی متفاوت (مثلا A۲) نصب می‌شود.

نکته: این ایده خوبی نیست که رم‌هایی با ظرفیت‌های متفاوت در شکاف‌های اتصال با رنگ‌های مشابه نصب کنید، زیرا این کار می‌تواند ثبات کار رایانه شما را بر هم بزند. حالا مرحله اتصال رم به پایان رسیده است و شما باید برای اطمینان صحت کارکرد، آن را چک کنید.

آزمایش حافظه رم جدید

رایانه شما باید به‌صورت خودکار رم جدید را شناخته و از آن استفاده کند. برای حصول اطمینان از این امر رایانه خود را روشن کنید. در ویندوز ۷ به Statr»»Control Panel»»System و پس از آن به Security بروید. روی View amount of Ram and processor speed کلیک کنید. مقدار حافظه‌ای که سیستم نشان می‌دهد، باید بیشتر از گذشته باشد. موضوع دیگر ۳۲ بیتی یا ۶۴ بیتی بودن سیستم عامل (OS) است. ویندوزهای ۳۲ بیتی فقط می‌توانند تا سه گیگابایت حافظه رم را شناسایی و پشتیبانی کنند، اما ویندوزهای ۶۴ بیتی مقادیر بیشتری رم را شناسایی و پشتیبانی می‌کنند.

با یادگیری ۴۰ نکته لیسانس حل مشکلات رایانه بگیرید

۱- یک کاوشگر گوگل هوشمند باشید
هنگامی که با کدهای خطای خاص یا پیغام های ایراد سیستم عامل روبرو می شوید، گوگل می تواند یک دستیار بسیار خوب و عالی در کنار شما باشد. اینکه فقط در گوگل سرچ کنید “my PC is running slowly” یا «کامپیوتر من کند شده» احتمالا فایده چندانی ندارد.

بلکه باید تا حد امکان جزئیات ایراد پیش آمده را در کنار یکدیگر ذکر کرده و آنها را با علامت + به هم ربط دهید. همچنین برای جستجو به دنبال عبارات خاصی که به دنبال آن هستید، آن را در میان علائم "" بنویسید.

۲- برنامه بازیابی سیستم یا System Restore

قابلیت بازگشت به عقب در ویندوز به شما امکان می دهد تغییرات اخیر درون رجیستری، سخت افزار و نرم افزار کامپیوتر را به حالت قبل برگردانید. و البته این کار هیچ تاثیری روی فایل های شخصی که طی این مدت در کامپیوتر اضافه کرده اید، نخواهد گذاشت. اگر در چند روز اخیر مشکلی پیش آمده، این نقطه شروع خوبی برای حل آن است. System Restore را در کنترل پنل خواهید یافت.

۳- Safe Mode

با فشردن دکمه F8 هنگام بالا آمدن کامپیوتر می توانید به منوی بوت کامپیوتر دست یابید. حال با انتخاب گزینه Safe Mode به نسخه ای از ویندوز وارد می شوید که به جز درایورهای ضروری و برخی ابزارهای اولیه، هیچ چیز دیگری در آن لود نشده و ظاهری همانند سیستم عامل مایکروسافت در دهه ۹۰ دارد! از حالت Safe Mode می توانید برای حذف برنامه ها یا ابزارها استفاده کنید. یا اینکه برنامه های عیب یابی (trubleshooting) را اجرا کنید. به خصوص این گزینه هنگامی کارایی خوبی دارد، که شما به صورت عادی نتوانید وارد ویندوز شوید.

۴- داغ شدن بیش از حد

اگر کامپیوترتان به طور تصادفی قفل می کند ولی در ظاهر هیچ مشکل نرم افزاری یا ایراد سخت افزاری خاصی ندارد، ممکن است دچار مشکل گرم کردن و داغ شدن بیش از حد باشد. بهتر است به فکر خرید فن یا خنک کننده جدیدی باشید، تا مشکل سیستم تهویه حرارتی لپ تاپ و کامپیوترتان حل شود.

۵- روشن بودن قابلیت اسکن لحظه ای

بخش زیادی از ایرادات سیستم ما (از سرعت و عملکرد پایین تا ریستارت های ناخواسته) به دلیل حضور موجودات خبیثی همچون ویروس و بدافزارها به وقوع می پیوندند. ناگفته پیدا است که باید آنتی ویروس و برنامه های ضد بدافزار خود را همیشه به روز نگه دارید و علاوه بر روشن گذاردن اسکنرهای آنها، هر از گاهی به کنترل سیستم تان هم بپردازید. همچنین یک گزینه تکمیلی استفاده از دو اپلیکیشن امنیتی بسیار خوب Spybot Search & Destroy و Microsoft’s own Safety Scanner در کنار نرم افزارهای امنیتی معمول سیستم است. مزیت مهم این برنامه ها آن است که با ابزارهای امنیتی قبلی سیستم تداخلی نداشته و در کنار آنها به خوبی کار خواهند کرد.

۶- پارازیت در پس زمینه

کارایی پایین و کندی که طی گذر زمان اتفاق می افتد، می تواند به دلیل برنامه ها و نرم افزارهای فراوانی باشد که روز به روز روی کامپیوتر بیشتر می شوند و اغلب آنها هم دوست دارند در پس زمینه کامپیوتر فعال بوده و مشغول انجام کاری باشند. Task Manager را

باز کنید تا میزان استفاده واقعی از رم و پردازنده کامپیوتر در حال حاضر را مشاهده کنید.
ساده ترین راه باز کردن تسک منیجر، راست کلیک روی تسک بار پایین دسک تاپ و انتخاب Task Manager است. اگر در میان سرویس ها و فرآیندهای این لیست مواردی را می یابید که با آن آشنایی ندارید یا وجود آنها در پس زمینه کامپیوتر چندان منطقی به نظر نمی رسند، برای جزئیات بیشتر یک جستجوی ساده در گوگل، بسیار راهگشا خواهد بود. پیدا کردن راهی برای حذف این برنامه ها از پس زمینه، می تواند کمک بزرگی به افزایش سرعت سیستم باشد.

۷- استارت آپ انتخابی
اگر در Task Manager مورد یا مواردی را یافتید که واقعا اضافی و به درد نخور بودند، بهتر است کنترل کنید آنها همراه با ویندوز، اجرا نشوند و بالا نیایند. برای این کار ابتدا پوشه Startup درون استارت منو را باز کرده و هر چیز به درد نخور را از درون آن حذف کنید.

برای کنترل بیشتر روی فرآیندهای استارت آپ ویندوز در ویندوز ۷، درون کادر جستجوی استارت منو عبارت msconfig را تایپ کنید. در پنجره باز شده می توانید جزئیات بیشتری در خصوص ابزارها و سرویس هایی که به طور خودکار هنگام بالا آمدن سیستم عامل همراه با آن اجرا می شوند، بیابید و آنها را کنترل کنید. برای کنترل فرآیندهای استارت آپ ویندوز ۸ هم بهتر است سری به راهنمای ساده کار با Task Manager در ویندوز ۸ بزنید.
احتمالا متعجب می شوید که چه قدر سرویس های زیادی همراه ویندوز بالا می آیند.

۸- بازیابی فایل ها
هنگامی که ویندوز فایلی را پاک می کند، واقعا آن را نابود نکرده و تبدیل به کدهای ۰ و ۱ نمی کند. بلکه به سادگی تنها ارجاع به آن را از سیستم آدرس دهی خود حذف نموده و آن بخش از دیسک را به عنوان فضای خالی علامت گذاری می کند. در صورتی که هنوز آن فضا با فایل دیگری جایگزین و رونویسی نشده باشد، ممکن است شما قادر به بازیابی فایل های تان باشید. نرم افزار Recuva یکی از بهترین و قدرتمندترین ابزارهای رایگان بازیابی فایل ها در ویندوز است.

۹- ویندوز بالا نمی آید
ویندوز از چندین گزینه بازیابی سیستم خوب (از جمله Safe Mode)

بهره می برد و شما می توانید هنگام بوت نشدن سیستم از آنها استفاده کنید. هنگام بالا آمدن کامپیوتر دکمه F8 را بزنید و از منوی بوت گزینه Last Known Good Configuration را انتخاب کنید تا ویندوز سعی کند تنظیماتی را که آخرین بار به درستی طبق آنها کار می کرده ، بازیابی کرده و بالا بیاید. راه دیگر جداسازی تمامی ابزارهای جانبی غیر ضروری از سیستم است. گاهی اوقات یک ابزار که به درستی پیکربندی نشده یا تنظیمات درستی ندارد، می تواند باعث هنگ کردن ویندوز طی فرآیند بالا آمدن شوند.

۱۰- بوق های مادر بورد

اگر پس از روشن کردن کامپیوتر مدت طولانی بدون هیچ اتفاقی می گذرد، و می بینید دستگاه با صدای بوق های بیپ مانندی خاموش شده و ویندوز بالا نمی آید، مشکل مربوط به سطوحی پایین تر از سیستم عامل و نرم افزار است. مادر بوردها معمولا بر اساس تعداد بوق های شان به شما اخطار می دهند اشکال از چه قسمتی است. به دفترچه راهنمای کامپیوترتان مراجعه کنید تا ببینید بوق آن چه معنی دارد. اگر هم آن را نگه نداشته اید، حتما یک نسخه آنلاین را در سایت کارخانه سازنده خواهید یافت.

۱۱- روشن نشدن دستگاه

اگر کامپیوتر یا لپ تاپ تان اصلا روشن نمی شود، و البته مشکل از پریزهای برق هم نیست؛ بهتر است نگاهی به کابل برق دستگاه یا شارژر/ باتری آن بیاندازید. بهتر است قبل از اینکه به دنبال جایگزین کردن بخش های مهمی همچون پاور دستگاه باشید، اول با هزینه ای کم، کابل های برق و باتری های آن را کنترل و تعویض کنید.

۱۲- فروم ها

اگر به اینترنت دسترسی دارید، بهتر است قبل از اینکه سراغ گوگل بروید، سری به فروم های رسمی کارخانه سازنده یا برنامه نویسان مرتبط با محصول تان بزنید. ممکن است با راه حل ها و راهنمایی های ویژه ای برای حل مشکلی روبرو شوید که شما هم اکنون با آن روبرو هستید. استفاده از فروم های محلی مرتبط با کامپیوتر هم گاهی می تواند کارساز باشد. درباره برخی نرم افزارها، گاهی اوقات برنامه نویس ها در فروم های مرتبط با آن، به رفع باگ و ایرادهای پیش آمده می پردازد.

۱۳- از مایکروسافت بپرسید

حتما موافقید که مایکروسافت کمابیش از سیستم های تحت سیستم عامل خودش سر در آورده و می تواند به حل مشکل آنها کمک کند. بهتر است از ابزار اتوماتیک FixIt مایکروسافت کمک بگیرید. این ابزار سعی می کند به جستجوی مشکل پرداخته و پس از یافتن آن، راه حلی برای اش بیابد یا حداقل راهنمایی لازم را در اختیارتان بگذارد.
برنامه Microsoft FixIt شماری از راه حل های ساده را پیش روی تان می گذارد.

۱۴- پاکسازی رجیستری
اگر چیز اشتباهی در فایل تنظیمات پر پیچ و خم رجیستری ویندوز اتفاق بیافتد، می تواند باعث بروز برخی ایرادها، قفل کردن نرم افزارها و حتی برخی ریستارت های گاه و بیگاه شود. اگر چه به هر ابزاری نمی توان اعتماد کرد، اما برنامه های فراوانی در اینترنت می توان یافت که به طور ویژه کارشان اسکن رجیستری برای یافتن و حل این مشکلات است.
Glary Registry Repair یکی از بهترین برنامه های موجود است که می تواند ایرادات رجیستری را رفع کند. به دنبال برنامه ای حرفه ای تر با امکانات بیشتر هستید؟ مسئولیت مشکلات پیش آمده با خودتان است. لطفا قبل از هر کاری، پشتیبان گیری از فایل رجیستری فراموش نشود.

۱۵- نصب دوباره ویندوز
در واقع این سیاست زمین سوخته است. اما واقعا آنقدر که فکر می کنید، موثر نیست. بسیاری از کامپیوترها و لپ تاپ ها با دیسک ریکاوری یا یک پارتیشن ریکاوری روی هاردشان عرضه می شوند. و شما با استفاده از آن می توانید دستگاه را به وضعیت اولیه اش (درست همانند هنگامی از کارخانه بیرون آمده) برگردانید. و البته لازم به ذکر نیست، پس از این کار باید تمامی نرم افزارهای تان را دوباره نصب کنید و تمامی اطلاعات شخصی روی کامپیوتر را از دست خواهید داد. پس لازم است قبل از انجام این کار، نسخه پشتیبانی از آنها تهیه کنید.

مشکلات سخت افزاری

۱۶- روی یک کامپیوتر دیگر امتحان کنید
استفاده از یک کامپیوتر دیگر برای تست موس، دوربین یا پرینتر خراب تان (یا حتی استفاده از یک پورت USB دیگر روی همین کامپیوتر) می تواند شما را از صحت عملکرد کامپیوترتان و وجود

خرابی در ابزار جانبی مطمئن کند. اگر با این آزمون ها مشکل برطرف شد، لطفا به جای سرزنش دوربین یا موس بیچاره، به دنبال حل مشکل کامپیوترتان باشید.

۱۷- درایورهای جدید

سری به سایت کارخانه سازنده زده و جدیدترین درایورها و Firmwareها را برای ابزار مورد نظرتان دانلود کرده و آنها را نصب کنید. با این کار فایل های آسیب دیده یا مشکل دار قبلی هم جایگزین خواهند شد، آخرین پچ های حل مشکلات اضافه خواهند شد و سازگاری با سخت و نرم افزارهای جدید در ابزارهای تان بهبود خواهد یافت.

۱۸- درایورهای قدیمی

گاهی اوقات ویندوز و ابزارهای جانبی بدون سوال از شما درایورهای جدید را نصب می کنند و به ندرت، این امر موجب بروز مشکل می شود. برای حل این مشکل و بازگشت به نسخه قبلی درایور، در کنترل پنل ویندوز به Device Manager رفته و در لیست موجود روی سخت افزاری که با علامت سوال زرد مشخص شده راست کلیک کنید. گزینه Properties را انتخاب کرده و در پنجره باز شده به تب Driver بروید. اکنون می توانید با کلیک روی دکمه Roll Back Driver به درایور قدیمی برگردید.

۱۹- حذف (Uninstall) درایورها

در همان صفحه Device Manager امکان حذف کامل هرگونه ردپای درایور هر کدام از سخت افزارهای موجود در لیست را دارید. آنگاه می توانید ابزار مورد نظر را جدا کرده و با اتصال دوباره آن به کامپیوتر، پنجره فرآیند نصب درایور را از ابتدا ببینید. این گونه شاید مشکل حل شود.

از پنجره Driver Manager می توانید اقدام به آپدیت، roll back یا حذف (uninstall) درایورها کنید.

۲۰- تست حافظه (رم)

واقعا نمی توان گفت چه زمانی حافظه یا رم دستگاه تان از کار خواهد افتاد و شما را تنها می گذارد. البته این اتفاق هم به ندرت می افتد و چندان متداول نیست. اما عدم ثبات دوره ای سیستم و قفل کردن های گاه و بیگاه اپلیکیشن ها می تواند نشانه هایی از این موضوع باشند. با کمک برنامه های عیب یابی رمی چون MemTest86+ می توانید به اسکن کامل ماژول های رم نصب شده بپردازید و هرگونه

مشکل در آنها را پیدا کنید.

۲۱- تست هارد درایو

هارد درایو های مدرن امروزی از سیستم درونی با نام SMART بهره می برند که سرواژه عبارت Self Monitoring And Reporting Technology یا «تکنولوژی خود-مانیتوری و گزارش دهی» است. با این تکنولوژی، دیسک ها وضعیت خود و سلامت عمومی شان را به ویندوز گزارش می کنند. ابزارهای رایگان فراوانی وجود دارند که می توانند داده های SMART را خوانده و برای تان تفسیر کنند. HDD Health یکی از این نمونه ها است که از درایو های SSD هم پشتیبانی می کند و اگر درایوهای شما نیاز به تعویض و جایگزینی داشته باشند، با نشان دادن اخطار شما را آگاه می کند.

۲۲- Windows disk checking

ویندوز هم برنامه کنترل دیسک درونی خود را دارد که به دنبال مشکلات احتمالی درون هارد دیسک های متصل به کامپیوتر می گردد. برای استفاده از آن، در ویندوز اکسپلور روی هارد درایو مورد نظر راست کلیک کرده و گزینه Properties را انتخاب کنید. آنگاه در پنجره باز شده به تب Tools بروید.

۲۳- ایراد های نمایشگر

مشکلات نمایشگر معمولا به دلیل ایراد در کارت گرافیک، خود مانیتور یا (در صورت عدم استفاده از لپ تاپ) کابل رابط رخ می دهند. در صورت امکان از یک کابل جداگانه استفاده کنید. یا اینکه سراغ گرافیک آن بورد سیستم بروید. این گونه شاید دریابید دقیقا کدام یک از حلقه های این زنجیر دچار نقص هستند. اگر مشکل از مانیتور باشد، احتمالا هیچ راهی به جز مراجعه به گارانتی، تعمیرکار یا خرید یک مانیتور جدید باقی نخواهد ماند.

۲۴- بازش کنید

حتما لازم نیست یک متخصص سخت افزار و فروشنده کامپیوتر باشید تا بتوانید نگاهی به درون کیس کامپیوترتان بیاندازید. اما قبل از هر کاری ابتدا مطمئن شوید بدن تان به زمین متصل است و الکتریسیته ساکن ندارد. همچنین کامپیوتر را از برق کشیده اید.

پس از باز کردن آن به دنبال اتصالات و پیچ های قطع شده یا شُل باشید. همچنین هرجا میزان زیادی گرد و خاک جمع شده، بهتر است تمیز شود. احتمالا یک قوطی هوای فشرده خیلی به کارتان بیاید. باز کردن لپ تاپ ها ممکن است بسیار مشکل تر باشد. اما در برخی مدل ها دست یابی به رم و هارد دیسک بسیار آسان است. لذا می توانید چک کنید تا اتصال آنها مشکلی نداشته باشد. احتمالا در سایت کارخانه سازنده و دفاتر راهنمای آنها کمک های بیشتری را هم می توانید بیابید.

۲۵- پشتیبان گیری

متاسفانه، زمان های بسیاری پیش می آید که شما دیگر هیچ کاری نمی توانید انجام دهید. و باید بپذیرید هارد دیسک یا کل سیستم تان به کلی نابود شده است. پس حیاتی است که نسخه های بک آپی از اطلاعات و فایل های مهم تان داشته باشید و آنها را در جای مطمئنی نگه داری کنید. احتمالا این مطلب نگهبان می تواند کمک خوبی بوده و اهمیت موضوع را دوباره گوشزد کند.

مشکلات نرم افزاری

۲۶- به روز رسانی ها

آیا برنامه ای که شما با آن درگیر هستید، آپدیت تازه ای نداده است؟ شاید برای پشتیبانی از سخت افزار جدید یا قابلیت های جدید سیستم عامل یک به روز رسانی آمده باشد؟ پس ضرری ندارد وب سایت سازنده آن را کنترل کنید. یا اینکه از ابزار آپدیت درونی که اغلب برنامه ها به آن مجهز هستند، استفاده کنید. البته در بسیاری از نرم افزارهای امروزی آپدیت ها به صورت خودکار نصب می شوند.

۲۷- نصب دوباره

اگر مشکل هنوز به قوت خود باقی است، تمام ردپاهای نرم افزار را از روی سیستم پاک کنید و سپس فرآیند نصب را از ابتدا و با نسخه تازه دانلود شده ای از برنامه یا دیسک اورجینال آن آغاز کنید. چرا؟ با این کار اطمینان می یابید هیچ فایل آسیب دیده یا خرابی روی سیستم نیست و تمام آنها را جایگزین خواهید کرد و تمامی تنظیمات نرم افزار ریست خواهند شد. برای حذف کامل تمامی ردپاهای نرم افزار می توانید از برنامه هایی همچون Revo Uninstaller استفاده کنید.

۲۸- پلاگین ها

به خاطر داشته باشید برنامه شما ممکن است به خودی خود مشکلی نداشته باشد، اما یکی از افزونه ها یا پلاگین های آن دچار ایراد باشند. سعی کنید تمامی افزونه ها و اد-اون ها را غیر فعال کرده و با فعال کردن نوبتی آنها، مشکل را پیدا کنید.

پلاگین ها و اد-اون ها ریشه بسیاری از مشکلات نرم افزاری هستند.

۲۹- پاکسازی (Clean up)

بسیاری از برنامه ها فایل های موقتی و کش تولید می کنند که گاها می تواند باعث تداخل در روال کار عادی نرم افزار شود. پس بهتر است به دنبال راهی برای حذف این گونه فایل های جاگیر و مزاحم باشید. CCleaner یکی از برنامه های خوش دست رایگان برای انجام این کار است و می تواند فایل های موقتی یا تمپ اغلب نرم افزارها را به راحتی پاک کند.

۳۰- برنامه های ناسازگار

حتما شما هم اوقات پر دردسر و رنج آوری با برخی اپلیکیشن ها که سر ناسازگاری با برخی برنامه های دیگر سیستم داشته اند، گذرانده اید. این موضوع بیشتر در مورد ابزارهای امنیتی پیش می آید که سعی می کنند به طور همزمان کار یکسانی انجام دهند. سعی کنید به طور

موقت دیگر برنامه هایی را که ممکن است با نرم افزار مورد استفاده تان دچار اختلال گردند، غیر فعال کنید.

مشکلات اینترنت

۳۱- نقص را پیدا کنید
قدم اول: ببینید مشکل از کجا است. ببینید آیا توسط دیگر کامپیوتر و ابزارها می توانید به اینترنت وصل شوید. بهتر است لپ تاپ را مستقیما توسط کابل به روتر وصل کنید و برنامه درونی تست روتر را اجرا کنید. شرکت خدمات دهنده اینترنت تان (ISP) هم احتمالا در زمینه این ایرادها ورزیده و خبره است. اگر تنها یک کامپیوتر است که نمی تواند به اینترنت وصل شود، پس احتمالا مشکل از تنظیمات آن و یا کارت شبکه اش است.

۳۲- مشکلات کارت شبکه
اگر شما به آداپتور و کارت شبکه کامپیوترتان مشکوک شده اید (برای مثال دانگل یو اس بی وایرلس)، ابتدا بخش «مشکلات سخت افزاری» را (در بالا گفته شد) چک کنید. سعی کنید درایور آن را آپدیت کنید، آن را حذف و دوباره نصب کنید، یا اینکه از پورت یو اس بی دیگری استفاده کنید.

۳۳- به روز رسانی firmware
شاید به روز رسانی تازه ای برای firmware روتر و مودم مورد استفاده تان آمده باشد، اما شرکت های خدمات اینترنت معمولا دوست ندارند شما کنترل زیادی روی تنظیمات داشته باشید و چیزی نگفته اند. بهتر است به بخش پشتیبانی سایت ISP تان و همچنین کارخانه روتر نگاهی بیاندازید. گاهی مشکلات به سادگی آپدیت یک firmware حل می شوند.

۳۴- همه چیز را ریبوت کنید
شاید این موضوع تبدیل به یک طنز شده باشد، اما بسیار اوقات کارایی دارد. مودم یا روتر را ۳۰ تا ۶۰ ثانیه خاموش کنید و اجازه دهید ارتباط تان با شرکت از ابتدا بازسازی شود. آنگاه دوباره آن را روشن کنید. برای نتیجه بهتر، شاید مناسب باشد کامپیوتر تان را هم ریستارت کرده و دوباره سعی کنید به اینترنت وصل شوید.

۳۵- کانال ها را عوض کنید
روترها معمولا از فرکانسی همانند دیگر ابزارها (مایکروفرها، دستگاه های کنترل کودک و…) برای ارتباط بیسیم استفاده می کنند.

این می تواند باعث کندی ارتباط شما یا اخلال در آن شود. بهتر است دیگر ابزارها را از روتر دور کرده یا اینکه کانال مورد استفاده آن را تغییر دهید. برای انجام این کار به دفترچه راهنمای روتر و مودم تان مراجعه کنید.
استفاده از یک کانال دیگر روتر و مودم می تواند مشکل سرعت پایین اینترنت را حل کند.

۳۶- آیا سایت داون است؟
اگر با سایت خاصی مشکل دارید، بهتر است از طریق سرویسی مانند www.downforeveryoneorjustme.com آن را کنترل کنید، شاید مشکل از اینترنت و کامپیوتر شما نباشد. توجه داشته باشید اگر سرویس مهمی مانند S3 آمازون یا کلودفلر دچار مشکل شود، این می تواند به طور همزمان بر سایت های فراوانی تاثیر گذارده و آنها را از دسترس خارج کند.

۳۷- مدیریت شبکه
کمی در Network and Sharing Centre ویندوز به کاوش بپردازید تا مطمئن شوید چندین برنامه به طور همزمان سعی در مدیریت و اداره اتصال وایرلس شما ندارند. کارخانه های سازنده لپ تاپ معمولا برنامه مدیریت شبکه خودشان را روی دستگاه ها نصب می کنند. این برنامه ها تا زمانی سعی نکنند به صورت همزمان با ابزارهای درونی خود ویندوز به مدیریت شبکه بپردازند، کارشان را درست انجام می دهند.

۳۸- دردسرهای مرورگر
استفاده از یک مرورگر دیگر، بهترین راه است تا مطمئن شوید ایراد پیش آمده ربطی به مرورگر دوست داشتنی تان ندارد و از جایی دیگر آب می خورد. اگر لازم است مرورگر را سرزنش کنید، بهتر است بعد از ناسزا گفتن ها، نکات اشاره شده در بخش «مشکلات نرم افزاری» را هم نگاهی بیاندازید. به خصوص دقت کافی در کنترل بخش پلاگین و افزونه های مرورگرتان داشته باشید.

۳۹- تنظیمات فایروال
فایروال ها گاهی می توانند کج خُلقی کرده و برخی سایت ها، سرویس یا برنامه ها را مسدود کنند. به تنظیمات بخش ورودی و خروجی (incoming and outgoing) فایروال تان نگاهی بیاندازید و ابزارها و سایت های بیگناه بازداشت شده را نجات دهید. اگر برای اتصال ابزار شبکه یا بازی خاصی دچار مشکل شده اید، شاید لازم باشد به

دستورالعمل فایروال جهت صدور اجازه لازم برای دسترسی برنامه ها به اینترنت، نگاهی داشته باشید.
برخی ابزارهای شبکه و بازی ها به مجوزهای ویژه فایروال نیاز دارند.

۴۰- کانکشن ها را بررسی کنید.
به بخش Network and Sharing Centre ویندوز بروید و اطمینان یابید کامپیوتر شما برای اتصال به اینترنت از کانکشن صحیح استفاده می کنند. برای مثال کانکشن روشن و پیش فرض باید وایرلس، یا اتصال کابلی باشد. در حالی تمام این بخش ها باید خودشان به صورت خودکار پیکربندی و تنظیم شوند، برنامه های خرابکار یا ابزارهای امنیتی ممکن است آن را تغییر داده باشند. در این بخش همچنین یک ابزار رفع ایراد یا troubleshooter دارید که بسیار مفید و کاربردی است.

محافظت از حریم شخصی در کافی نت و کامپیوترهای عمومی

گاهی اوقات بنا به دلایلی مجبوریم به کافی‌نت و یا مکانی مشابه (مانند سایت کامپیوتری دانشگاه، مؤسسات و شرکت‌ها) که امکان استفاده از کامپیوترهای عمومی را فراهم می‌کنند، مراجعه کنیم. فرض کنید به مسافرت رفته‌اید و لپ‌تاپ همراه‌تان نیست، کامپیوترتان از کار افتاده و برای ارسال یا دریافت یک فایل عجله دارید؛ صرف‌نظر از هر دلیلی که برای مراجعه به کافی‌نت داشته باشید، باید بدانید که مراجعه به این گونه مکان‌ها احتمال به خطر افتادن اطلاعات شخصی‌تان را افزایش می‌دهد. در ادامه مقاله به ارایه و بررسی راهکارهایی مناسب به منظور محافظت از اطلاعات در این گونه مکان‌ها

پرداخته‌ایم.

پاکسازی تاریخچه گشت و گذار مرورگر

پاک کردن تاریخچه مرورگر اینترنت اولین قدمی است که باید برای محافظت از حریم شخصی و جلوگیری از فاش شدن اطلاعات بردارید. بعد از پایان وبگردی باید کوکی‌ها، اطلاعات وارد شده در فرم‌های ثبت‌نام، تاریخچه و حتی فایل‌های موقتی (Temp) اینترنتی مرورگر را حذف کنید.

اگرچه امکان حذف دستی این موارد وجود دارد، اما خوشبختانه با پیشرفت روزافزون مرورگرها و اضافه شدن ویژگی‌های متعدد برای بالا بردن امنیت کاربر، می‌توانید از ویژگی گشت و گذار محرمانه استفاده نمایید. با استفاده از ویژگی گشت و گذار محرمانه می‌توانید با خیال راحت وبگردی کنید، چون در این حالت اطلاعات وبگردی شما توسط مرورگر ذخیره نخواهند شد.

این ویژگی در فایرفاکس Private Browsing نام دارد و برای استفاده از آن می‌توانید به منوی Tools بروید و گزینه Start Private Browsing را کلیک کنید یا از کلیدهای میانبر Ctrl+Shift+P استفاده نمایید.

در مرورگر IE این ویژگی InPrivate Brwosing نام دارد و برای استفاده از آن باید از منوی Tools گزینه Inprivate Browsing را کلیک کنید. لازم به ذکر است که کلیدهای میانبر این ابزار در IE، مشابه فایرفاکس است.

این ویژگی در مرورگر Chrome شرکت گوگل با نام Incognito Mode شناخته شده و برای استفاده از آن باید روی دکمه آچار کلیک کنید و گزینه New incognito windows را انتخاب کنید، یا از کلیدهای میانبر Ctrl+Shift+N برای اجرای آن استفاده نمایید.

عدم ذخیره فایل روی کامپیوتر عمومی

اگر از کامپیوتر دوست‌تان استفاده می‌کنید، عدم ذخیره فایل‌های گوناگون و بی‌فایده روی سیستم وی نشانگر شخصیت شما و احترام متقابلی است که برای وی قایل هستید. اما زمانی که صحبت از کافی‌نت و مکان عمومی مشابه می‌شود واژه "احترام" محلی از اعراب نداشته و این امنیت و حریم شخصی شماست که در اولویت قرار می‌گیرد.

شاید برخی از فایل‌هایی که در کافی‌نت‌دانلود می‌کنید، اهمیت چندانی نداشته باشند (مثل فایل‌های صوتی، ویدیویی و یا تصویری)، اما زمانی که صحبت از دانلود فایلی می‌شود که در قالب ضمیمه به آدرس ایمیل شما ارسال شده، حساسیت امر چندین برابر می‌شود، چرا که گاهی چنین ضمیمه‌هایی حاوی اطلاعاتی بسیار مهم و محرمانه هستند.

فرض کنیم شخصی یک سند ساده Word را که حاوی متن چندان مهمی نیست، برای شما ارسال کرده است. صرف‌نظر از نوع سند، همه فایل‌ها اطلاعاتی تحت عنوان MetaData را همیشه یدک می‌کشند که این اطلاعات بسته به نوع فایل با یکدیگر فرق دارند.

برای مثال اطلاعات متادیتای اسناد Word شامل مواردی مثل عنوان فایل، موضوع آن، نام شخص نویسنده، تاریخ آخرین ویرایش، تعداد صفحات، تگ‌ها، کامنت‌ها و دیگر موارد مشابه است. یا اطلاعات متادیتای یک فایل MP3 شامل نام سازنده، آلبوم، مالک فایل و حتی نام کامپیوتر مالک و مواردی از این قبیل است.

مسئله این است که اطلاعات متادیتا می‌تواند اطلاعات بسیار جامع و البته محرمانه‌ای از شما را در اختیار دیگران قرار دهد؛ اطلاعاتی مثل نام شما، نام سازمان، نام کامپیوتر، نام هارددیسک و یا سرور شبکه‌ای که فایل را در آن ذخیره کرده‌اید، نام و نوع چاپگر، مولف‌های قبلی سند، و نسخه‌های مختلف سند.

فرد خرابکار به راحتی می‌تواند از این اطلاعات سوءاستفاده کرده و شما و حتی سازمان یا شرکتی که در آن مشغول به کار هستید را به خطر بیندازد.

برای حذف اطلاعات متادیتا در ویندوز ابتدا روی فایل کلیک راست کرده، از منوی ظاهر شده گزینه Properties را کلیک کرده و در پنجره ظاهر شده به برگه details بروید. حال در انتهای این پنجره گزینه Remove Properties and Personal Information را مشاهده می‌کنید که باید آن را کلیک نمایید.

در پنجره بعدی دو گزینه در اختیار دارید؛ گزینه اول یعنی Create a copy with all possible properties removed که به صورت پیش‌فرض در حالت انتخاب شده قرار دارد، تمامی اطلاعات شخصی قابل حذف را پاک می‌کند. با استفاده از گزینه دوم یعنی Remove the following properties from this file هم می‌توانید به صورت دستی اطلاعات متادیتای مورد نظر خود را پاک نمایید.

البته راه دیگر برای حذف این‌گونه اطلاعات، استفاده از نرم‌افزارهای ثالث مانند Document Trace Remover است که حتی امکان پاکسازی گروهی (Batch) اسناد را فراهم می‌کند.

در هر صورت اگر در چنین شرایطی مجبور به دانلود فایل هستید، بهتر است یک حافظه فلش همراه داشته و فایل مورد نظر را مستقیم روی آن ذخیره نمایید. دقت داشته باشید اگر ابتدا فایل را روی کامپیوتر دانلود کنید، امکان بازیابی آن برای دیگران وجود خواهد داشت. مگر اینکه از برنامه‌هایی مثل File Shredder استفاده کنید. اگر چنین نرم‌افزاری روی کامپیوتر عمومی نصب نشده بود بهتر است ابزار پرتابل مشابه همراه خود داشته باشید.

عدم ذخیره رمز عبور

یکی از نکات بسیار مهم که متأسفانه تازه‌کارها اطلاعی در مورد آن نداشته و هرگز توجهی به آن نمی‌کنند امکان ذخیره سازی رمز عبورها توسط مرورگرهاست. البته این نکته در مورد کاربران حواس‌پرت و بی‌حوصله‌ای که وقتی برای خواندن پیام‌ها نگذاشته و تنها به زدن گزینه Yes و Next بسنده می‌کنند هم صادق است.

این عادت بد کلیک سریع روی پیام باعث شده که کاربران هیچ‌گونه احساس خطری نسبت به کلیک روی پیام‌های سیستم‌عامل و یا دیگر نرم‌افزارها، به خصوص مرورگرها نکنند. بعضی از کاربران کافی‌نت حین چک ایمیل، پیام مربوط به ذخیره‌سازی رمز عبور که از سوی مرورگر نشان داده می‌شود را تایید می‌کنند. به این ترتیب کاربر بعدی به راحتی می‌تواند وارد حساب ایمیل شخص قبلی شده و حتی رمز عبور آن را از طریق مرورگر مشاهده نموده و تغییر دهد.

در چنین شرایطی بهتر است قبل از انجام هر کاری ویژگی ذخیره‌سازی رمز عبور را غیرفعال نمایید. برای این منظور در محیط فایرفاکس از منوی Tools گزینه Options و سپس Security را کلیک کرده و در قسمت Passwords گزینه Remember passwords for site را غیرفعال کنید.

در مرورگر IE هم بعد از باز کردن پنجره تنظیمات (Options)، به برگه Content رفته و در قسمت AutoComplete دکمه Settings را کلیک نمایید. در پنجره باز شده گزینه Usernames and passwords on forms را غیرفعال کنید.

عدم انجام کارهای بانکی

نت به هیچ عنوان مکانی مناسب برای انجام امور بانکی نیست؛ از این رو اکیداً توصیه می‌کنیم هرگز برای انجام امور مرتبط با تراکنش مالی به آن جا مراجعه نکنید. اگر به کامپیوتر شخصی خود دسترسی ندارید، برای کنترل حساب بانکی‌تان بهتر است از دستگاه‌های خودپرداز و یا سرویس‌های تلفنی بانک‌ها استفاده کرده و یا به نزدیک‌ترین شعبه بانکی مراجعه نمایید.

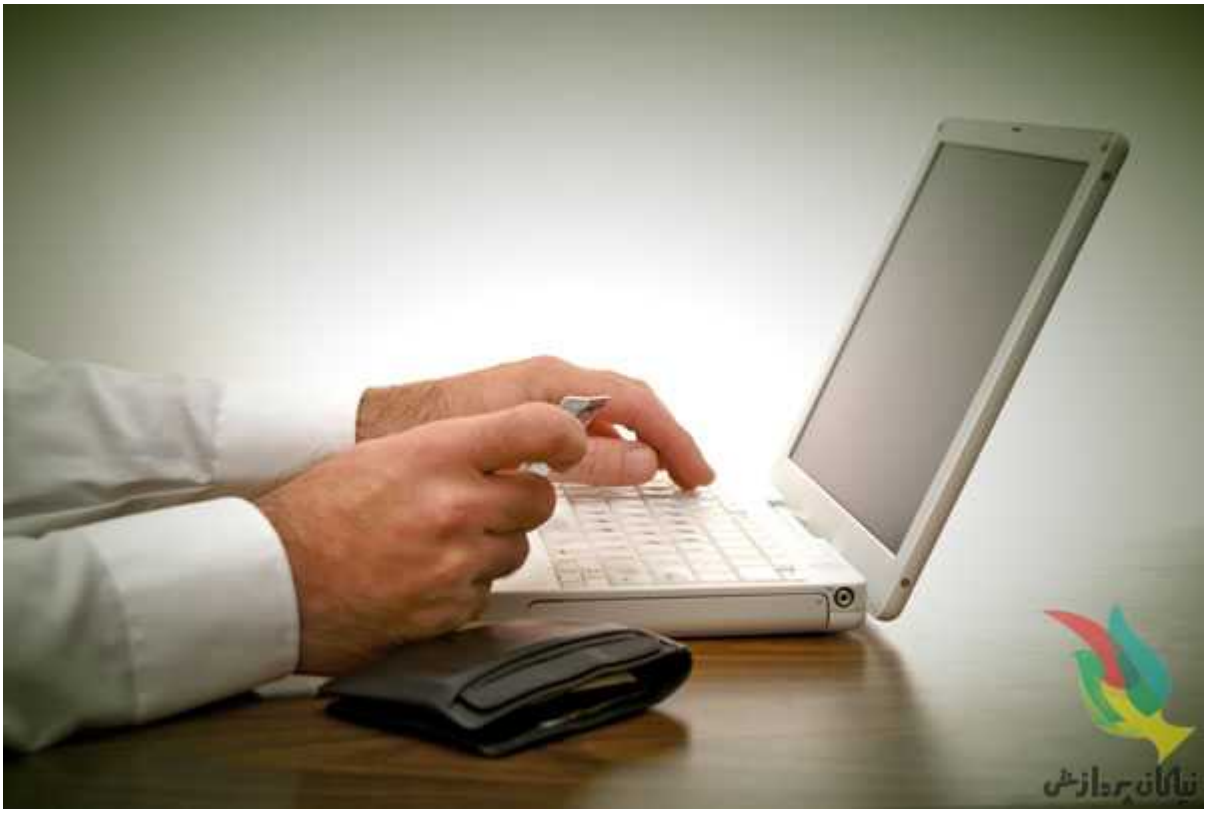
البته از نظر سرقت اطلاعات شخصی مربوط به حساب‌های بانکی جای نگرانی زیادی وجود ندارد. زیرا می‌توان موجودی حساب و تراکنش‌های مالی حساب در دوره‌های زمانی مختلف را مشاهده کرد.

عدم استفاده از کارت‌های اعتباری

این روزها استفاده از کارت‌های اعتباری رواج بسیاری در میان مردم پیدا کرده و فروشگاه‌ها نیز برای جذب مشتریان، امکان خرید از طریق کارت‌های الکترونیکی را به وب‌سایت‌های خود اضافه کرده‌اند. فقط باید مراقب باشید که از صفحه کلید مجازی درگاه‌های پرداخت الکترونیکی بانک‌ها و مؤسسات مالی استفاده نمایید.

این امر به دلیل وجود نرم‌افزارهایی مخربی موسوم به Keylogger است. این نرم‌افزارها هر کلیدی که شما فشار دهید را ثبت می‌کنند و می‌توانند امور دیگری مثل کلیک‌های ماوس، عکس گرفتن از صفحه نمایش، ارسال اطلاعات در تاریخی خاص به یک ایمیل مشخص و … را نیز انجام دهند.

توصیه ما در خصوص محافظت از اطلاعات کارت‌های الکترونیکی، انجام فرایند خرید تنها از طریق کامپیوتر شخصی‌تان است.



حذف فایل‌های موقتی

های موقتی یا همان Temporary Files در مقابل فایل‌های موقتی اینترنت یا Temporary Internet Files قرار می‌گیرند. این گونه فایل‌ها هنگام کار با نرم‌افزارها ساخته می‌شوند. معمولاً این فایل‌ها بعد از بسته شدن نرم‌افزار مربوطه یا راه‌اندازی مجدد سیستم، به طور خودکار حذف می‌شوند که متأسفانه در بیشتر موارد این کار انجام نمی‌شود.

برای مشاهده این گونه فایل‌ها می‌توانید فایل‌های *.tmp یا *.chk و یا *.*~ را در سیستم جستجو کنید. با این کار تمامی فایل‌هایی که

با این کاراکترها آغاز شده و یا دارای پسوندهای .tmp و .chk هستند، ظاهر خواهند شد. سپس همه آنها را با هم انتخاب کرده و برای حذف کلید Shift را نگه داشته و سپس کلید Delete را فشار دهید تا به این ترتیب این فایل‌ها مستقیماً پاک شده و به سطل بازیافت نروند.

هر چند امکان برگرداندن آن‌ها توسط نرم‌افزارهای بازیابی فایل مثل Recover My Files وجود دارد.
افزارهایی همچون CCleaner نیز برای حذف چنین فایل‌هایی طراحی شده‌اند. این نرم‌افزار تمهیدات لازم برای حذف فایل‌های موقتی بدون امکان بازیابی آنها (Shred) را برای کاربر فراهم می‌کند.

در صورت تمایل به پاک کردن دستی، ۲ مسیر اصلی این گونه فایل عبارتند از:

برای دسترسی آسان به این دو مکان می‌توانید عبارت‌های %temp% برای مسیر اول و همچنین Tempبرای مسیر دوم را در قسمت Run تایپ کرده و اینتر نمایید.

حذف Pagefile

در ویندوز حکم حافظه مجازی را دارد. هدف Pagefile دریافت اطلاعات از RAM و ذخیره موقت آن روی هارددیسک است؛ به این ترتیب برنامه‌ها تصور می‌کنند مقدار زیادی RAM روی کامپیوتر نصب شده و از این رو

از آن به عنوان حافظه مجازی استفاده می‌کنند. بهتر است بعد از اتمام کار با کامپیوتر عمومی، Pagefile ویندوز را به صورت دستی پاک نمایید. برای این کار باید به قسمت Local Security Policy مراجعه نمایید.

برای دسترسی به این قسمت در ویندوز ایکس‌پی ابتدا به کنترل پانل رفته، گزینه Administrative Tools را باز کرده و سپس روی گزینه Local Security Policy دوبار کلیک کنید. سپس روی گزینه Security Options در سمت راست صفحه کلیک کرده و گزینه Shutdown: Clear Virtual Memory Pagefile را که در قسمت پایین صفحه قرار دارد را پیدا کرده، آن را باز نموده و فعال کنید.

نکته: اگر به هر دلیلی به قسمت Local Security Policy دسترسی ندارید، می‌توانید Pagefile را به صورت دستی پاک کنید. برای این کار ابتدا باید قابلیت نشان دادن فایل‌های مخفی و سیستمی ویندوز را فعال کنید. برای این منظور Folder Options را در کنترل پانل باز کرده و گزینه Show Hidden Files and Folders را فعال کرده و تیک گزینه Hide Protected Operating System Files را هم بردارید.

بعد از این فایلی با نام pagefile.sys را پیدا کرده و آن را پاک کنید. این فایل معمولاً در درایو C: یعنی درایوی که ویندوز در آن نصب شده قرار دارد. دفعه بعد که کامپیوتر از نو راه‌اندازی می‌شود Pagefile جدیدی ساخته خواهد شد.

راه‌اندازی مجدد کامپیوتر

بعد از اتمام کار با کامپیوتر، آخرین کاری که باید انجام دهید راه‌اندازی مجدد سیستم با استفاده از دکمه Restart تعبیه شده روی کیس است. این کار نه تنها Pagefile را پاک می‌کند (البته در صورت فعال بودن) بلکه تمامی اطلاعات موجود در RAM را هم از بین می‌برد.

زیر نظر گرفتن محیط

نهایتاً باید گفت جدای از محیط مجازی کامپیوتر بهتر است به اتفاقاتی که دور و بر می‌افتد هم توجه کرده و همه چیز را زیر نظر داشته باشید. به خاطر داشته باشید در مکانی عمومی نشسته‌اید. هرگز

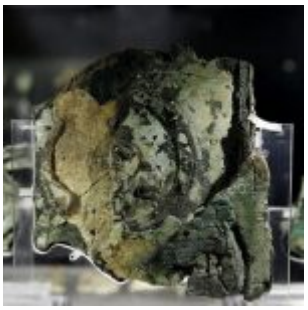
اقدام به باز کردن و مشاهده سند محرمانه در این مکان‌ها نکنید؛ چه بسا Keylogger نصب شده در کامپیوتر که شما از وجود آن بی‌خبرید، اقدام به عکس برداری از محتویات سند کند.

در صورت وجود دوربین مداربسته بهتر است دقت بیشتری کنید. برای مثال هنگامی که در حال تایپ اطلاعات مرتبط با ورود به حساب کاربری هستید، بهتر است کیبورد را با دست به خوبی بپوشانید، چه بسا برخی بتوانند کلیدخوانی (در مقابل لب‌خوانی) کنند! به یاد داشته باشید که به هیچ عنوان امکان ایمن‌سازی کامل کامپیوترهای عمومی وجود ندارد.

توصیه نهایی: از کامپیوترهای عمومی تنها برای وبگردی ساده استفاده کنید.

منبع:computernews

قدیمی‌ترین کامپیوتر دنیا رمزگشایی شد



بیش از صد سال پیش بود که در بقایای یک کشتی یونانی، ماشینی کشف شد که نامش را آنتیکیترا گذاشتند. از آن هنگام تاکنون عملکرد این ماشین – که آن را اولین کامپیوتر دنیا لقب داده‌اند – نامشخص بوده است. البته از روی کلماتی که روی این ماشین حک شده بود تشخیص داده شد که باید ابزاری نجومی باشد.

اکنون و با یک دهه تلاش در زمینه اسکن کردن این دستگاه، محققان توانسته‌اند ۳۵۰۰ کاراکتر از متنی که در این دستگاه حک شده را

بخوانند؛ یعنی یک‌چهارم متن این دستگاه ۲۱۰۰ساله را. این متن نشان می‌دهد که از این دستگاه برای پیشگویی آینده استفاده می‌شده است. الکساندر جونز، از تیم محققان می‌گوید: «این دستگاهی است که از آن برای آموزش درباره کهکشان‌ها و جایگاه ما در کیهان استفاده می‌شده است. این مانند کتاب درسی نجوم است که حرکات ستارگان و سیارات در آسمان را با زندگی یونانی‌های باستان پیوند می‌داده است.» این دستگاه برای نشان دادن موقعیت خورشید و ماه در آسمان هم به کار می‌رفته است و البته از آن برای پیشگویی بخت و اقبال هم استفاده می‌شده است.

HDMI چیست؟

یکی از فناوری‌هایی که به تازگی محبوبیت فراوانی یافته، HDMI است. این فناوری به کاربر امکان می‌دهد صدا و تصویر با کیفیت بسیار بالا از دستگاه پخش به تلویزیون و بلندگو منتقل شوند. در این مقاله، این فناوری را بررسی خواهیم کرد.

HDMI که اختصار عبارت High Definition Multimedia Interface (رابط چندرسانه‌ای با کیفیت بالا) است، یکی از نوآوری‌های برتر در صنعت لوازم الکترونیکی خانگی است. این رابط امکاناتی مانند انتقال ویدیوی دیجیتال با کیفیت بالا، تا هشت کانال صدای دیجیتال، رمزگذاری HDCP و پروتکل CEC (کنترل لوازم الکترونیکی خانگی) را به همراه پنج ولت برق، تنها در یک کابل فراهم می‌آورد.

نسخه ۱ فناوری HDMI اواخر سال ۲۰۰۲ معرفی شد و تمام امکانات بالا را داشت. نسخه ۱٫۳c این فناوری قابلیت‌های بسیار بیشتری مانند پشتیبانی از رنگ عمیق (نمایش بیش از یک میلیارد رنگ)، تصحیح همزمانی صدا و تصویر، و پشتیبانی از دو فرمت صوتی با کیفیت بالای دیسک‌های بلو-ری را دارد. در این مقاله خواهیم دید که HDMI چطور قابلیت‌های جدید را عرضه می‌کند و در عین حال، با استاندارد قدیمی‌تر DVI نیز سازگار است.

تصویر

HDMI مانند DVI از روش TMDS برای کدگذاری و انتقال ویدیوی دیجیتال استفاده می‌کند. البته HDMI از این روش برای انتقال صدا هم سود می‌برد. روش TMDS به گونه‌ای است که باعث می‌شود اثر تداخل‌های الکترومغناطیسی روی کابل‌ها کم شود و سیگنال‌ها بتوانند با سرعت بالاتر و خطای کمتر از کابل عبور کنند.

دستگاه پخش، سیگنال دیجیتال را کدگذاری کرده و آن را به همراه یک کپی معکوس، از طریق دو سیم مسی به نمایشگر می‌فرستد. اگر دستگاه‌های مجاور باعث ایجاد نویز روی کابل شوند، اثر این نویز روی دو سیم برعکس هم خواهد بود و نمایشگر با استفاده از تفاوت بین داده‌های دو سیم، سیگنال‌های خراب‌شده را بازسازی می‌کند.

تمامی نسخه‌های HDMI از کابل‌های یکسان و ۱۹ پین استفاده می‌کنند، اما در هر نسخه پهنای باند افزایش یافته و ویژگی‌های جدیدی به این استاندارد افزوده شده که برخی از آنها انتخابی است. برای مثال HDMI 1.0 از حداکثر نرخ ساعت پیکسل ۱۶۵ مگاهرتز (پهنای باند ۴٫۹۵ گیگابیت در ثانیه) پشتیبانی می‌کرد که با آن می‌شد تصویر HDTV با ابعاد 1920) ۱۰۸۰p در ۱۰۸۰ پیکسل) را با نرخ نوسازی (Refresh Rate) 60 هرتز منتقل کرد. همچنین تصاویر WUXGA به ابعاد ۱۹۲۰ در ۱۲۰۰ پیکسل با نرخ نوسازی ۶۰ هرتز نیز قابل انتقال بود.

نسخه ۱٫۱ فناوری HDMI از DVD Audio نیز پشتیبانی می‌کرد. در نسخه ۱٫۲، پشتیبانی از Super Audio CD نیز اضافه شد. در نسخه ۱٫۳، نرخ ساعت پیکسل به ۳۴۰ مگاهرتز (پهنای باند ۱۰٫۲ گیگابیت در ثانیه) افزایش یافت و با آن می‌شد تصاویر WQXGA به ابعاد ۲۵۶۰ در ۱۶۰۰ پیکسل را با یک کابل انتقال داد.

در نسخه ۱٫۳ پشتیبانی از رنگ عمیق (Deep Color) و فضای رنگی xvYCC نیز اضافه شد. در فناوری رنگ عمیق تعداد سایه‌زنی‌ها، رنگ‌ها و شدت نورهای بسیار زیادی وجود دارد و رنگ‌ها می‌توانند از چند میلیون تا چند میلیارد باشند. در فناوری رنگ عمیق، از ۳۰، ۳۶ یا ۴۸ بیت برای ذخیره یک رنگ استفاده می‌شود، در حالی که در HDMI 1.0 عمق رنگ تنها ۲۴ بیت بود. فضای رنگ xvYCC که به آن x.v.Color نیز می‌گویند، برای ذخیره‌سازی رنگ از فضای ۸ بیتی (اعداد ۰ تا ۲۵۶) استفاده می‌کند.

صدا

HDMI نسخه ۱٫۰ از هشت کانال LPCM (مدولاسیون کد پالس خطی) با وضوح ۲۴ بیت و نرخ نمونه‌برداری تا ۱۹۲ کیلوهرتز پشتیبانی می‌کند.

نسخه ۱٫۳ از هشت کانال صدای فراگیر با روش‌های فشرده‌سازی بدون افت کیفیت (Dolby TrueHD (Lossless و DTS-HD Master Audio پشتیبانی به عمل می‌آورد. همچنین در تمامی نسخه‌ها می‌توان از روش‌های با افت کیفیت (Lossy) دالبی دیجیتال و DTS استفاده کرد.

پیچیدگی پردازش تصویری ممکن است باعث تأخیر شود، یعنی شاید صدا زودتر از تصویر به مقصد برسد. در این حالت، صدا همزمان با تصویر نخواهد بود. در نسخه HDMI 1.3 یک ویژگی به نام Auto Lip Sync افزوده شده که به صورت خودکار، مانع بروز چنین اتفاقی می‌شود.

تمامی نسخه‌های HDMI مجموعه فرمان‌های مشترکی به نام CEC دارند که این دستورها در نسخه ۱٫۲ به صورت کامل مدون شده‌اند. به کمک این فرمان‌ها، می‌توان با یک کنترل از راه دور مشترک، دستگاه‌هایی را که به کابل HDMI متصلند، کنترل کرد. برای مثال، اگر دکمه Play روی این کنترل فشار داده شود، تمامی دستگاه‌های متصل روشن شده و دیسک شروع به پخش می‌کند. تفاوت اصلی بین نسخه‌های ۱٫۳b ،۱٫۳a و ۱٫۳c با نسخه ۱٫۳ دستورهای جدید CEC است.

نسخه‌های ۱٫۳b ،۱٫۳a و ۱٫۳c با نسخه ۱٫۳ دستورهای جدید CEC است.

DVI چیست؟

یکی دیگر از استانداردهای انتقال ویدیو با کیفیت بسیار بالا، DVI نام دارد که سرنام Digital Visual Interface است.

DVI که در سال ۱۹۹۹ معرفی شد، برای انتقال داده‌های ویدیویی فشرده نشده و با وضوح بالا به کار می‌رود. استاندارد DVI با استانداردهای دیگر، مانند VGA سازگاری دارد، هر چند که بیش از همه با HDMI سازگار است و تصاویر این دو را می‌توان به هم تبدیل کرد. البته یک تفاوت مهم بین این دو استاندارد وجود دارد: DVI در کانال TMDS خود صدا را منتقل نمی‌کند و تنها به انتقال تصاویر ویدیویی می‌پردازد.

برای تبدیل خروجی DVI کامپیوترها به HDMI، باید از یک تبدیل‌کننده استفاده کرد تا صدا هم در داده‌های ارسالی قرار گیرد.

کیفیت تصاویر انتقالی با DVI بسیار بالاست و با یک کابل، می‌توان تا ۲٫۷۵ مگاپیکسل را با فرکانس ۶۰ هرتز منتقل کرد که معادل تصاویر با ابعاد ۱۹۱۵ در ۱۴۳۶ پیکسل در استاندارد ۴:۳ و ۲۰۹۸ در ۱۳۱۱ پیکسل در استاندارد صفحه عریض ۱۶:۹ می‌شود. همچنین می‌توان از دو کابل DVI برای انتقال استفاده کرد که در این صورت، کیفیت تصاویر در فرکانس ۶۰ هرتز تا ۴ مگاپیکسل هم بالاتر می‌رود. با هر کابل DVI فرکانس حداکثر ۱۶۵ مگاهرتز قابل انتقال است که در صورت نیاز به فرکانسی بالاتر باید از دو کابل استفاده کرد.

حداکثر طول کابل در استاندارد DVI برای انتقال بهینه تصاویر ۱۹۲۰ در ۱۲۰۰ پیکسل ۴٫۵ متر است و در صورتی که از کابل‌های ویژه استفاده شود این طول می‌تواند تا ۱۰ متر هم افزایش یابد. برای انتقال بهینه تصاویر با وضوح ۱۲۸۰ در ۱۰۲۴ پیکسل، طول کابل حداکثر باید ۱۵ متر باشد. در صورتی که کاربر نیاز داشت تصویر را در فاصله بیشتری منتقل کند، باید از یک دستگاه DVI Booster استفاده کند.

گزینه‌های خرید

هنگام خرید دستگاه‌های HDMI، به این نکته توجه داشته باشید که بعضی از ویژگی‌ها مانند رنگ عمیق، فضای رنگی xvYCC و حتی Dolby TruHD یا DTS-HD انتخابی هستند و به صورت پیش‌فرض روی دستگاه‌ها قرار ندارند. همچنین هر چند در استاندارد HDMI حداکثر طول کابل ذکر نشده، اما دو نوع کابل HDMI 1.3 وجود دارد:

- استاندارد یا نوع ۱
- سرعت بالا یا نوع ۲

کابل نوع ۱ قابلیت انتقال اطلاعات با سرعت ۷۵ مگاهرتز را دارد که با این سرعت می‌توان سیگنال ۱۰۸۰i (تصویر با وضوح ۱۹۲۰ در ۱۰۸۰) را منتقل کرد. چنین کابل‌هایی می‌توانند حداکثر ۵ متر کارایی داشته باشند.

نوع ۲ کابل‌ها می‌تواند سرعت ۳۴۰ مگاهرتز داشته باشد و می‌تواند سیگنال ۱۰۸۰p و عمق رنگ بیشتری را انتقال دهد. با این کابل‌ها می‌توان تصاویر با ابعاد بزرگ‌تر، حتی در حد ۲۵۶۰ در ۱۶۰۰ پیکسل را نیز منتقل کرد. این کابل‌ها برخلاف کابل‌های نوع ۱ که مسی با استاندارد AWG ۲۸ هستند، از استانداردهای AWG ۲۶ یا حتی AWG ۲۴ بهره می‌برند و به همین دلیل سنگین‌تر هستند. حداکثر طول آنها نیز بیشتر از کابل‌های نوع ۱ است.

اگر نیاز به طول کابل بیشتری داشته باشید، باید از تکرارکننده (Repeater) استفاده کنید. این تکرارکننده‌ها که با برق کار می‌کنند، سیگنال ورودی را تقویت کرده و باعث می‌شوند تصویر در مسافت بیشتری منتقل شود. همچنین می‌توانید از کابل‌های Active استفاده کنید که کارکردی مشابه دارند. همچنین می‌توانید از توسعه‌دهنده‌هایی (Extender) که با فیبر نوری یا کابل Cat5 کار می‌کنند نیز بهره بگیرید.

در جدول ۱ مشخصات نسخه‌های مختلف HDMI با هم مقایسه شده است.

SUPPORTED FEATURES	HDMI VERSION				
	1.0	1.1	1.2, 1.2a	1.3	1.3a, 1.3b, 1.3b1, 1.3c
Standard RGB Color Space	Yes	Yes	Yes	Yes	Yes
YCbCr Color Space	Yes	Yes	Yes	Yes	Yes
36–bit Deep Color	No	No	No	Yes	Yes
48–bit Deep Color	No	No	No	Optional	Optional
xvYCC (aKa x.v.Color) Color Space	No	No	No	Optional	Optional
1920 x 1200 resolution at 60Hz using a single Link	Yes	Yes	Yes	Yes	Yes
2560 x 1600 resolution at 60Hz using a single Link	No	No	No	Yes	Yes
Auto Lip Sync	No	No	No	Yes	Yes
DVD_Audio CD (DVD-A)	No	Yes	Yes	Yes	Yes
Super Audio CD (SACD)	No	No	Yes	Yes	Yes
Eight–channel LPCM Audio (192KHz/24 bit)	Yes	Yes	Yes	Yes	Yes
Dolby True HD/DTS- HD Master Audio	No	No	No	Optional	Optional

نیاکان پرداز

منبع:computernews.ir