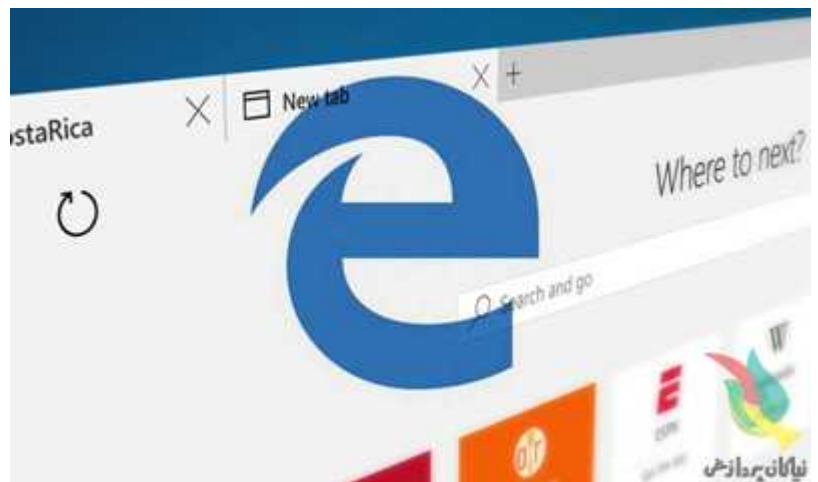


حذف خودکار تاریخچه مرورگر اِج



در ویندوز ۱۰ همچون دیگر مرورگرها، از قابلیت ذخیره‌سازی تاریخچه صفحات وب مرور شده پشتیبانی می‌کند و این قابلیت همان‌قدر که برای کاربران مفید است در مواردی نیز می‌تواند امنیت حریم خصوصی آنها را با مشکل مواجه کند.



در این شرایط اغلب کاربران برای حفظ امنیت اطلاعات خود از قابلیت مرور امن (خصوصی) کمک گرفته یا پیش از بستن مرورگر، تاریخچه ثبت شده در آن را تخلیه می‌کنند.

انجام این کار نسبتاً ساده است، اما تکرار آن به دفعات متعدد می‌تواند دشوار و خسته کننده باشد. اگر تمایل دارید با هر بار بستن مرورگر، تاریخچه ردپای ثبت‌شده از شما توسط مرورگر نیز به‌طور خودکار حذف شود کافی است این مراحل را دنبال کنید:

مرورگر اِج مایکروسافت را اجرا کرده و از بالا سمت راست روی آیکون منوی اصلی که به شکل سه نقطه عمودی به نمایش درآمده کلیک کنید.

روی گزینه Settings در انتهای منوی به نمایش درآمده کلیک کنید.

پنجره را به پایین اسکرول کرده تا بخش Clear browsing data را

مشاهده کنید.

در ادامه روی گزینه Choose what to clear کلیک کرده و در صفحه جدید ضمن فعال کردن موارد موردنظر برای حذف از تاریخچه مرورگر، کلید وضعیت موجود در کنار گزینه Always clear this when I close the browser را از حالت Off به On تغییر وضعیت دهید.

از حالا به بعد با هر بار بسته شدن مرورگر، تاریخچه آن نیز به طور خودکار پاک میشود و میتوانید بدون نگرانی صفحات وب را در مرورگر مرور کنید.

منبع: بیتوته

راهکارهایی برای کنترل حجم اینترنت همراه



زمانی اینترنت تلفن همراه سرعت چندانی نداشت و مصرف آن در بارگذاری چند صفحه وب و چک کردن ایمیل خلاصه میشد. آن زمان و با آن سرعت، نگرانی چندانی بابت مصرف بالا وجود نداشت، اما امروزه اوضاع متفاوت شده است.



نسل به نسل اینترنت‌های موبایل سریع‌تر شده‌اند و اکنون با اینترنت نسل چهارم و LTE تا چشم بر هم می‌گذارید، چند مگابایت از بسته اینترنت‌تان رفته است و احتمالاً هر بار با تمام شدن ناگافل حجم بسته‌تان با خودتان گفته‌اید باید مصرف اینترنتم را کنترل کنم تا دوباره این اتفاق پیش نیاید. پس اجازه دهید با هم تعدادی از راهکارهای کنترل مصرف اینترنت روی تلفن همراه را مرور کنیم.

۱- حواستان به مصرف باشد!

شاید با دیدن عنوان این بخش پیش خود فکر کنید «این که نشد راه‌حل!» ولی به شما اطمینان می‌دهم که در بسیاری از اوقات اصلاً حواسمان به این نیست که اینترنت موبایلمان با سرعت زیادی در حال مصرف شدن است. آن هم با اینترنت‌های سریع نسل سوم و چهارم. بنابراین مشخصاً نیاز به یک یادآور برای میزان مصرف اینترنت احساس می‌شود.

خوشبختانه در سیستم‌عامل اندروید، ساختار بسیار خوبی برای نمایش آمار میزان مصرف و هشدار مصرف بالا تعبیه شده است. با رفتن به تنظیمات اصلی گوشی یا تبلت‌تان و بخش مصرف داده (Data Usage) از قسمت اتصالات (Connections)، می‌توانید میزان مصرف داده کل یک ماه اخیر و همچنین فهرست برنامه‌های پرمصرف را مشاهده کنید.

اگر دقت کنید، روی نمودار مصرف، خطی افقی کشیده شده و در کنار آن عددی به گیگابایت نوشته شده است.

این خط عملاً سقف مصرفی ماهانه داده را مشخص می‌کند که شما می‌توانید آن را برای اندازه‌ای که می‌خواهید تنظیم کنید. هنگامی که مصرف‌تان به این حد برسد، سیستم از طریق اعلان‌ها به شما هشدار می‌دهد تا حواستان جمع شود!

اگر بخواهید از این هم سخت‌گیرانه‌تر عمل کنید، در بسیاری از مدل‌های تلفن همراه، امکانی برای قطع اتصال داده در صورت رسیدن به حد تعیین‌شده وجود دارد تا کاملاً مطمئن شوید که از حد مجاز بالا نمی‌زنید. متأسفانه در سیستم‌عامل iOS این کارکرد به صورت سیستمی وجود ندارد و باید از نرم‌افزارهای جانبی برای تعیین حد مصرف و هشدار بهره بگیرید، اما در این سیستم‌عامل هم می‌توانید در قسمت Cellular میزان مصرف کلی و مصرف مربوط به هر برنامه را مشاهده کنید.

۲- اولویت را به وای‌فای بدهید

سرعت بالاتر اینترنت موبایل گاهی تشویق‌مان می‌کند که حتی در مکان‌هایی که به اینترنت وای‌فای دسترسی داریم هم از آن استفاده کنیم. این کار را نکنید! به این فکر کنید که هزینه‌ای که شما بابت هر کیلوبایت داده روی موبایل پرداخت می‌کنید بسیار بیشتر از اینترنت ADSL است.

علاوه بر سوئیچ دستی به وای‌فای تا حدی که امکان دارد، به نرم‌افزارهایی که گزینه‌اش را دارند، دستور استفاده از وای‌فای را بدهید. یکی از مهم‌ترین این نرم‌افزارها در اندروید، پلی‌استور است که در حالت پیش‌فرض، به‌روزرسانی نرم‌افزارها را به‌صورت خودکار و بدون در نظر گرفتن نوع اینترنت انجام می‌دهد. برای تغییر این حالت، از منوی کناری به تنظیمات آن بروید و در قسمت عمومی (General)، به‌روزرسانی خودکار برنامه‌ها را یا به طور کامل غیرفعال کنید یا به آن اجازه دهید این عمل را فقط هنگامی که به شبکه وای‌فای متصل هستید انجام دهد.

۳- ترمز داده را در شبکه‌های اجتماعی بکشید!

در کشور ما، یکی از اصلی‌ترین کاربردهای اینترنت موبایل، فعالیت در شبکه‌های اجتماعی است و بنابراین طبیعی است که هنگام مصرف بالای داده، این شبکه‌ها متهم ردیف اول باشند! اما چگونه می‌توان میزان مصرف داده در این‌گونه شبکه‌ها را کنترل کرد و کاهش داد؟

تلگرام از این نظر تنظیمات بسیار مناسبی را در اختیار کاربران قرار داده است. هنگامی که در تنظیمات آن به قسمت داده و مصرف (Data and Storage) بروید، علاوه بر مشاهده ریز مصرف داده موبایل در بخش مصرف داده موبایل (Mobile Data Usage)، با انجام تغییراتی در بخش دانلود خودکار، میزان مصرف‌تان را تا حد خوبی تحت کنترل

دربیاورید. با زدن روی بخشِ «هنگام مصرف داده موبایل» (When using mobile data) می‌توانید تعیین کنید که چه مواردی در زمان استفاده از داده موبایل به صورت خودکار دانلود شوند.

توصیه ما این است که در این فهرست تنها تیک تصاویر و حداکثر گیفها را بگذارید و از خیر دانلود خودکار بقیه بگذرید. دیگر موارد را در هر زمان که بخواهید می‌توانید با در نظر داشتن حجمشان به صورت دستی دانلود کنید.

شبکه‌های اجتماعی دیگر به اندازه تلگرام کاربران را تحویل نمی‌گیرند! اینستاگرام فقط یک گزینه برای مصرف کمتر داده (Use Less Data) در قسمت Cellular Data Use در اختیارتان می‌گذارد که تنها کاری که می‌کند این است که از پیش‌بارگذاری (Preloading) ویدئوها جلوگیری می‌کند، ولی ویدئوها کماکان به صورت خودکار پخش می‌شوند! البته فیسبوک کمی بهتر عمل کرده و در آن می‌توانید با رفتن به قسمت ویدئوها در تنظیمات، پخش خودکار کلیپها را به طور کامل غیرفعال یا به وای‌فای محدود کنید.

۴- کش دوست ماست!

کم نیستند کسانی که ساختار سیستم‌عاملها را به درستی نمی‌دانند و به شما توصیه می‌کنند در اندروید از نرم‌افزارهایی استفاده کنید که به طور متناوب برنامه‌های در پس‌زمینه را می‌بندند (task killer)، اما دوستانه از ما بپذیرید که ضرر استفاده از این برنامه‌ها بیشتر از سودشان است.

غیر از دخالت در سیستم مدیریت حافظه سیستم‌عامل که در دسرهای خودش را خواهد داشت، این نوع برنامه‌ها روی مصرف داده شما هم تاثیر منفی خواهند داشت. می‌پرسید چگونه؟ عموم این نرم‌افزارها هنگام بستن یک برنامه در حال اجرا در پس‌زمینه، داده‌های کش یا همان داده‌های موقت برنامه را هم پاک می‌کنند. این به آن معناست که وقتی شما دوباره آن برنامه را باز کنید، داده‌های حذف شده از حافظه موقت دوباره از اینترنت دریافت خواهند شد و این یعنی افزایش بی‌دلیل مصرف داده!

علاوه بر این، خودتان هم می‌توانید با کش کردن دستی برخی از انواع داده‌ها، در مصرف اینترنت موبایل‌تان صرفه‌جویی قابل توجهی داشته باشید. برای مثال، اگر از نرم‌افزارهای نقشه استفاده می‌کنید، می‌توانید با بهره‌گیری از امکان مناطق آفلاین (Offline areas) در

نقشه گوگل یا داندلود نقشه در نرم افزارهای دیگر با اینترنت وای فای خانه، از بارگذاری آنها به صورت مداوم جلوگیری کنید.

پیدا کردن مطلب در سایتهای فاقد فرم جستوجو



این روزها با دسترسی گسترده به اینترنت و سایتهای مختلفی که اطلاعاتی در زمینه های گوناگون منتشر میکنند، تقریباً میتوان به هر پرسشی پاسخ داد و هر چیزی را در اینترنت جستوجو کرد. با توجه به همین گستردگی اطلاعات، جستوجو در اینترنت و سایتهای مختلف از اهمیت زیادی برخوردار است، چرا که بدون این ابزار یافتن اطلاعات مورد نظر حتی در شرایطی که به سایت مربوطه نیز دسترسی داشته باشید، بسیار دشوار خواهد بود.

به عنوان مثال فرض کنید به دنبال یک خبر در سایت هستید و ضمن آگاهی از عنوان خبر، این سایت به فرم جستوجو مجهز نباشد. به

نظرتان در چنین شرایطی می‌توانید خبر موردنظر را از میان ده‌ها هزار خبر موجود در سایت پیدا کنید؟ مطمئناً انجام این کار اگر غیرممکن نباشد بسیار دشوار و وقتگیر است. در وضعیت مشابه نیز چنانچه شما با سایتی مواجه شوید که فرم جستوجو ندارد یا جستوجوی آن عملکرد بسیار ضعیفی دارد ممکن است گمان کنید تنها راهکار باقی‌مانده همان صرف وقت طولانی برای پیدا کردن مطلب موردنظر است.

دوست دارید با روشی ساده‌تر آشنا شوید و بی‌نیاز از فرم جستوجوی سایت‌ها در هر سایتی که علاقه دارید جستوجو کنید؟ به کمک این روش می‌توانید با استفاده از انواع موتورهای جستوجوگر همچون گوگل، بینگ، جستوجوگر یاهو و... با استفاده از یک مرورگر ساده روی دستگاه‌های مختلف اعم از رایانه، تبلت و تلفن همراه عملیات جستوجو را اجرا کنید.

مرورگر اینترنتی موردنظر را اجرا و به یکی از موتورهای جستوجوگر مراجعه کنید. (به‌عنوان مثال سایت گوگل را باز کنید)

عبارت موردنظر را برای جستوجو وارد کرده و پیش یا پس از آن عبارت `site:Domain.com` را وارد کنید. (به‌جای عبارت `Domain.com` باید آدرس سایتی را که قصد دارید عملیات جستوجو در آن انجام شود، وارد کنید)

به‌عنوان مثال چنانچه به دنبال قیمت خودرو در سایت بیتوته هستید، کافی است یکی از عبارت‌های زیر را در کادر جستوجو وارد کنید: (در مورد اول، عبارت `site:beytoote.com` پیش از عبارت مورد جستوجو درج شده و در مورد دوم این عبارت پس از عبارت موردنظر برای جستوجو قرار گرفته است)

۱- قیمت خودرو `site:beytoote.com`

۲- `site:beytoote.com` قیمت خودرو

۱۳ میان‌بر کیبوردی که هر کاربر مایکروسافت ورد با یستی با آنها آشنا باشد



چه در حال حاضر خبره برنامه Word یا تازه‌کاری در دنیای پردازش متون و کلمات باشید، این ۱۳ میان‌بر کیبوردی برنامه Microsoft Word به شما در تسلط یافتن بر اسناد و افزایش بهره‌وری کمک می‌کند.

مجموعه نرم‌افزاری Microsoft Office شناخته‌شده‌ترین نرم‌افزار کاربردی در دنیا بوده و با توجه به آمار مایکروسافت، بیش از ۱٫۲ میلیارد نفر در ۱۴۰ کشور مختلف دنیا و با ۱۰۷ زبان متفاوت از آن استفاده می‌کنند.

همان‌طور که میدانید آفیس از برنامه‌های مختلف ساخته‌شده، اما احتمالاً Word پرکاربردترین آنها است. نرم‌افزار Word نیز به میان‌برهای کیبوردی ارزشمندی مجهز شده که به شما امکان صادر کردن دستوره‌ای متداول را تنها با فشردن چند کلید می‌دهد. اگر با نرم‌افزار Word کار می‌کنید اما از میان‌برهای آن استفاده نمی‌کنید، کار خود را سخت کرده‌اید.



به خاطر سپردن این ۱۳ میان‌بر بسیار ساده بوده و روش به خاطر سپردن هرکدام را هم به شما می‌گوییم.

از `Ctrl + S` برای ذخیره کردن سند فعلی استفاده کنید. S به Save اشاره دارد.

برای باز کردن سندی که در کامپیوترتان موجود است از `Ctrl + O` استفاده کنید. O به Open اشاره دارد.

برای بستن سند فعلی از `Ctrl + W` استفاده کنید.

برای ایجاد سند جدید از `Ctrl + N` استفاده کنید. N به New اشاره دارد.

برای خنثی کردن آخرین حرکتی که انجام داده‌اید از `Ctrl + Z` استفاده کنید.

اگر از نتیجه دستور قبل راضی نبودید و خواستید که حرکت دوباره تأثیر داده شود، از `Ctrl + Y` استفاده کنید.

برای توپر نشان دادن متن از `Ctrl + B` استفاده کنید. B نشانگر Bold است.

بعد از فشردن این کلید حروف بعدی که تایپ می‌کنید توپر نشان داده می‌شوند. اگر می‌خواهید بخشی از متنی که قبلاً نوشته شده توپر دیده

شود، آن را انتخاب کرده یا به عبارتی هایلایت کنید و بعد ترکیب `Ctrl + B` را فشار دهید. می‌توانید دوباره از همین ترکیب برای بازگرداندن متن به حالت عادی استفاده کنید.

برای کج یا *Italic* نشان دادن متن از ترکیب `Ctrl + i` استفاده کنید. *i* به *italic* اشاره دارد.

این میان‌بر بعد از اینکه از آن استفاده کردید بر متن اثر می‌گذارد. می‌توانید بخشی از متن را انتخاب کرده و بعد با استفاده از میان‌بر آن را *italic* کنید. می‌توانید از همین میان‌بر برای غیرفعال کردن آن استفاده کنید.

برای خط کشیدن زیر متن از ترکیب `Ctrl + U` استفاده کنید.

بعد از به کار گرفتن این میان‌بر زیر متن خط کشیده می‌شود. می‌توانید بخشی از متن را هم انتخاب کرده و با به کار گرفتن این میان‌بر زیر متن خط بکشید. می‌توانید از همین میان‌بر برای از بین بردن خط زیر متن نیز استفاده کنید.

برای کوچک کردن فونت ابتدا `Ctrl` را نگه‌داشته و پیوسته کلید `]` را فشار دهید.

این میان‌بر بعد از به کار گرفتن آن بر متن جدیدی که تایپ می‌کنید تأثیر می‌گذارد. می‌توانید بخشی از متن را انتخاب کرده و به کمک میان‌برها فونت آن را کوچک کنید.

برای بزرگ کردن متن نیز مشابه روش قبل کلید `Ctrl` را نگه‌داشته و از کلید `[` استفاده کنید.

این میان‌بر بعد از به کار گرفتن آن بر متن جدیدی که تایپ می‌کنید تأثیر می‌گذارد. می‌توانید بخشی از متن را انتخاب کرده و به کمک میان‌برها فونت آن را کوچک کنید.

برای پرینت گرفتن سند از ترکیب `Ctrl + P` استفاده کنید. `P` به `Print` اشاره دارد.

این میان‌بر صفحه گزینه‌های پرینت `Word` را برایتان نمایش می‌دهد.

برای پیدا کردن کلمه یا عبارتی خاص از میان‌بر `Ctrl + F` استفاده کنید.

این میانبر نشانگر را مستقیماً به نوار هدایت در سمت چپ صفحه می‌برد، در اینجا می‌توانید کلمه یا عبارت موردنظر خود را تایپ کرده تا آن را در صفحه پیدا کنید. برای رفتن به نمونه‌های بعدی که در متن پیدا شده است، کلید Enter را فشار دهید.

بد نیست بدانید که بسیاری از این میانبرها در دیگر برنامه‌های مایکروسافت نظیر Excel، Edge و غیره نیز کار می‌کند. از امتحان کردن نهراسید.

منبع: beytoote

آموزش تبدیل گوشی به اکسس پوینت و شیر کردن اینترنت



ابتدا به قسمت تنظیمات گوشی خود بروید و گزینه more را انتخاب کنید.

سپس گزینه tethering and portable hotspot را انتخاب کنید.

در این مرحله Portable wi-fi hotspot را روشن کنید.

حالا برای انتخاب پسورد و نام شبکه خود باید به قسمت تنظیمات hotspot بروید که در گوشی‌های مختلف متفاوت است یا قسمت تنظیمات جداگانه زیر همان دکمه فعال کردن هات اسپات وجود دارد یا با رفتن به همان قسمت فعال سازی می‌توانید پسورد و نام انتخاب کنید.

تنظیمات شبکه ساخته شده

در مرحله آخر هم کافی است تا از طریق کامپیوتر و یا دستگاه دیگر به شبکه ساخته شده که اینجا androidzoom است وصل شوید و با وارد کردن پسورد از اینترنت اشتراکی استفاده کنید.



چگونه از ابزار یادداشت برداری قدرتمند Evernote □ استفاده کنیم؟



در دنیای دیجیتال دو نوع کاربر وجود دارد: آنهایی که از Evernote استفاده نمیکنند و آنهایی که نمیکند! دسته اول اگر این ابزار

فوق‌العاده را از آنها بگیرید، زندگی‌شان مختل می‌شود و دسته دوم هم مرتب از دسته اول خواهند شنید که «اورنوت» چقدر فوق‌العاده است و چقدر می‌تواند خیالشان را بابت نگهداری اطلاعات راحت کند!

این مطلب هم تقریباً از همین نوع است و بگذارید به‌عنوان کسی که از بی‌علاقه بودن به اورنوت به کاربر پروپاقرص آن تبدیل شده است، بگویم اورنوت این ظرفیت را دارد که خیلی زود جای خودش را به‌عنوان جزئی لاینفک در زندگی دیجیتال‌تان باز کند!



نصب و شروع

Evernote در حالت پایه، رایگان است و روی هر پلتفرمی که فکرش را بکنید عرضه می‌شود: ویندوز، مک، اندروید، iOS و حتی بلک‌بری. برای شروع کار با اورنوت از دو طریق می‌توانید عمل کنید: از طریق وب، با رفتن به نشانی evernote.com گزینه ثبت‌نام را بزنید و مراحل آن را دنبال کنید.

راه دیگر، ایجاد حساب کاربری اورنوت با استفاده از نرم‌افزار آن، چه روی رایانه و چه روی موبایل است که تفاوتی با حالت آنلاین ندارد. برای حساب اورنوت به یک ایمیل و رمز عبور نیاز دارید و البته این امکان را هم دارید که با اکانت گوگل‌تان در سرویس ثبت‌نام کنید.

پس از ایجاد حساب کاربری، روی هر دستگاه دیگری که بخواهید از اورنوت استفاده کنید، کافی است با ایمیل و رمز عبور وارد حساب‌تان شوید. البته در مورد نصب و بهره‌گیری از اورنوت روی دستگاه‌های مختلف توجه کنید که این سرویس بتازگی برای حالت رایگان محدودیت

دو دستگاه را اعمال کرده است. یعنی غیر از فضای آنلاینش که به عنوان دستگاه محاسبه نمیشود، تنها دو دستگاه دیگر را میتوانید به حسابتان متصل کنید.

یادداشت برداری

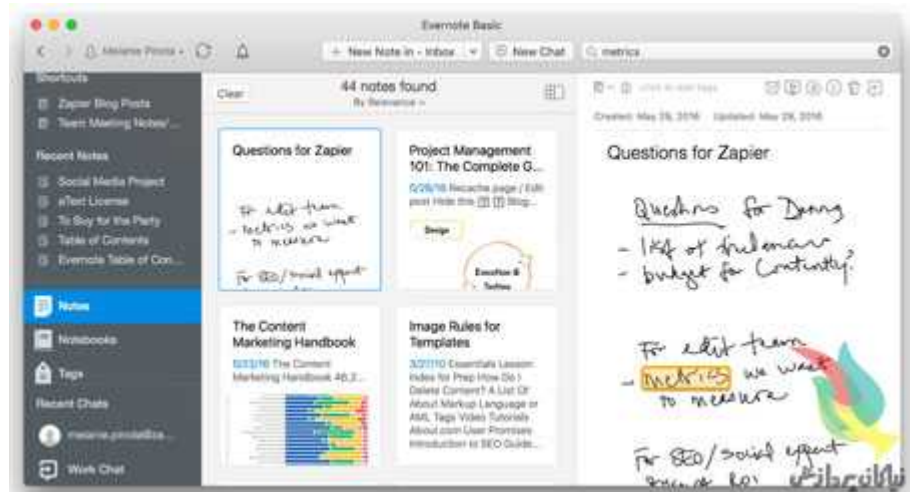
هرچه باشد، Evernote یک ابزار یادداشت برداری است و قاعدتا همه چیز حول این یادداشتها میچرخد. ولی بگذارید یک چیز را از همین ابتدا روشن کنیم: اگر میخواهید واقعا به قدرت این سرویس پی ببرید، آن را به صورت یک مخزن یادداشت در کنار بقیه نبینید، بلکه سعی کنید به طور کامل از آن استفاده کنید! اورنوت سرویسی است که هر چه یادداشت بیشتری در آن بگذارید، بیشتر به مفید بودن آن پی میبرید.

اورنوت برای یادداشتها کم نگذاشته و اینجا دیگر بحث یادداشتهای متنی نیست. شما میتوانید در یادداشتها علاوه بر متن، دستنوشته (با ماوس، انگشت یا قلم)، صدا، تصویر و حتی مکان بگذارید! در یادداشت متنی هم میتوانید مواردی مختلف مانند پررنگ بودن یا ایتالیک یا حتی های لایت را داشته باشید. یعنی تقریبا اطلاعاتی نیست که نتوانید آن را در اورنوت ذخیره کنید؛ میتوانید به آن به چشم مخزن اطلاعاتی نگاه کنید، نه فقط یک نرم افزار یادداشت برداری.

همچنین، به تجربه میگویم یادداشتهای تصویری اورنوت را دستکم نگیرید! دفعه بعدی که کسی به شما کارتش را داد، کافی است تصویر آن را در یادداشتهایتان ذخیره کنید تا دیگر نگران از دست رفتن اطلاعات تماس نباشید. با این قابلیت براحتی میتوانید از شر یادداشتهای کاغذی یا کارتهای اضافی خلاص شوید.

یادداشتها در اورنوت به صورت خودکار همگام سازی میشود و نیازی نیست این کار را به صورت دستی انجام دهید. هر یادداشتی که ایجاد میشود یا تغییر میکند، در کنار آن علامتی به نشانه در حال همگام سازی نمایش داده میشود که با اتمام این عمل، علامت هم حذف میشود. البته اگر بخواهید، گزینه ای هم برای درخواست همگام سازی به صورت دستی در منوی اصلی برنامه وجود دارد.

Evernote یک ابزار یادداشت برداری است و قاعدتا همه چیز حول این یادداشتها میچرخد.



ساختر Evernote

یادداشت‌برداری و ذخیره اطلاعات در اورتوت به آسانی صورت می‌گیرد، اما یادداشت‌ها بدون دسته‌بندی و نظم چه فایده‌ای دارد؟ بگذارید نگاهی به ساختار اورتوت برای دسته‌بندی اطلاعات بیندازیم.

در اورتوت همه‌چیز در «دفترچه»ها قرار می‌گیرد. یعنی شما می‌توانید دفترچه‌های مختلفی ایجاد کنید تا یادداشت‌هایتان را در آنها ذخیره کنید. مثلاً دفترچه‌ای به نام «یادداشت‌های شخصی» درست کنید و یادداشت‌های شخصی‌تان را در آن بنویسید. نگران این هم نباشید که یادداشتی را در دفترچه درستش بگذارید، دفترچه یک یادداشت را می‌توانید راحتی تغییر دهید. تعداد دفترچه‌ها هم در حالت رایگان حداکثر ۲۵۰ عدد است. در وهله دوم، خود دفترچه‌ها هم می‌تواند در چیزی به نام «پشته» یا Stack قرار گیرد. یعنی دفترچه‌هایی را که به هم مربوط یا در مورد یک موضوع است، می‌توان در یک پشته گذاشت که نظم بهتری داشته باشد.

علاوه بر این موارد، اورتوت ابزار دیگری هم برای دسترسی سریع به یادداشت‌ها در اختیار شما می‌گذارد: «تگ». هر یادداشت می‌تواند تا صد تگ داشته باشد و از فهرست تگ‌ها می‌توانید به تمام یادداشت‌هایی که یک تگ خاص دارد دسترسی داشته باشید.

از جست‌وجوی پر قدرت اورتوت هم غافل نشوید که بدون آن در دریای یادداشت‌ها غرق می‌شوید! هنگامی که شما عبارتی را در فیلد جست‌وجو تایپ می‌کنید، اورتوت عبارت ورودی شما را در همه‌جا از جمله متن خود یادداشت‌ها جست‌وجو می‌کند. بنابراین تنها با دانستن قسمتی از متن یک یادداشت می‌توانید آن را راحتی پیدا کنید.

Evernote برای حرفه‌ای‌ها

اورنوت شاید در نگاه اول سرویس ساده و سراسری به نظر برسد، اما آن قدر جزئیات و ترفند دارد که کسانی که سال‌ها مشتری آن بوده‌اند هم می‌توانند کاربردهای جدیدی کشف کنند.

اینها برخی از ترفندهایی است که کارکرد این سرویس را توربوشارژ می‌کند:

Web Clipper: مطلبی جالب در وب پیدا کرده‌اید و می‌خواهید آن را ذخیره کنید، رویش یادداشت بگذارید یا به مطالب دیگر ارتباطش دهید. کدام سرویس بوک‌مارک می‌تواند از پس اینها برآید؟ اینجا افزونه Evernote Web Clipper (برای فایرفاکس و کروم) به کار می‌آید که همه اینها را در خود دارد. کافی است آن را نصب کنید و با یک کلیک، صفحاتی را که می‌خواهید به دفترچه‌هایتان بفرستید. یک نکته جالب این افزونه هم آن است که به جستجوی گوگل هم مرتبط می‌شود. یعنی هنگامی که صفحه‌ای را ذخیره کرده باشید و این صفحه در فهرست نتایج جستجوی گوگل‌تان باشد، افزونه آن صفحه را در کنار نتایج نمایش می‌دهد.

ارتباط میان یادداشتی: در حالت عادی Evernote را می‌توان در فهرستی از یادداشت‌ها خلاصه کرد، اما یک ترفند ساده می‌تواند یادداشت‌هایتان را از این حالت خشک دربیآورد و به آن ارتباط هدیه کند! برای این کار از منوی یک یادداشت، گزینه Copy Note Link را انتخاب کنید سپس این لینک را در هر یادداشت دیگری که می‌خواهید قرار دهید. با این کار، به آسانی می‌توانید از یک یادداشت به یادداشت دیگر بروید و فهرست یا زنجیره یادداشتی تشکیل دهید. این ترفند برای استفاده از Evernote در تحقیق و جمع‌آوری منابع بسیار مفید

خواهد بود.

جستجو با قدرت: وقتی تعداد یادداشت‌ها، دفترچه‌ها و تگ‌ها زیاد می‌شود، دیگر جستجوی عادی جوابگو نیست و باید کمی حرفه‌ای‌تر عمل کنید. Evernote غیر از جستجو، به شما امکان فیلتر کردن نتایج را هم براساس مواردی مانند زمان، دفترچه و حتی حجم یادداشت می‌دهد. با بهره‌گیری از این امکان و ترکیب موارد آن، می‌توانید مثلاً به دنبال یادداشتی حاوی عبارت خاصی با تگ‌های مشخص بگردید که هفته پیش ذخیره کرده بودید.

۵ راه حل اضطراری برای حل مشکلات رایانه



شاید رایانه شخصی برای بعضی‌ها به اندازه موبایل ضروری نباشد، اما برای همان آدم‌ها نیز در رتبه دوم اهمیت قرار دارد. بنابراین اگر به هر دلیل دچار مشکل شوید؛ در این مطلب پنج راه حل برای حل مشکلات رایانه شما پیشنهاد شده که در مواقع ضروری بسیار کارآمد است.

شاید رایانه شخصی برای بعضی‌ها به اندازه موبایل ضروری نباشد

۱- شکستن صفحه نمایش رایانه

فرض کنید صفحه نمایش لپ‌تاپ شما با لیوانی که به سویتان پرتاپ شده، شکسته است! چه باید کرد؟ در صورتی که فقط صفحه نمایش آسیب دیده باشد، با این‌که کمی غیرعادی است، اما هنوز می‌شود از لپ‌تاپ استفاده کرد. در این مرحله از حل مشکلات رایانه اگر مانیتور دیگری دارید، می‌توانید به صورت موقت به لپ‌تاپ وصل کنید.

از تلویزیون نیز می‌شود استفاده کرد؛ فقط باید یک پورت خروجی مناسب (VGA یا HDMI, mini-HDMI, DisplayPort, mini-Display, DVI) داشته باشید تا به دستگاه خود وصل کنید. بعضی لپ‌تاپ‌ها نیز حالت صفحه نمایش اضافی دارند که در این صورت باید آن را فعال کنید که این کار معمولاً از طریق کلیدهای Function انجام می‌شود. اگر خروجی لپ‌تاپ شما در صفحه نمایش دیگر بدون مشکل بود، احتمالاً فقط مشکل رایانه شما صفحه نمایش دارید آن است و دچار مساله دیگری نشده‌اید.

اگر صفحه نمایش ترک مویی در کنار لبه برداشته باشد، باید حواستان باشد رایانه خود را بدقت حرکت دهید؛ چون ممکن است با هر فشاری که به آن وارد شود، ترک آن به شکستگی بزرگتری تبدیل شود. خیلی با احتیاط آن را به مرکزی منتقل کنید تا یک کارشناس آن را تعمیر کند.



۲- پاک شدن تصادفی اطلاعات مهم

دو نوع فایل مهم داریم؛ یکی فایل‌هایی که برای کاربر مهم است، مانند عکس‌ها و آرشیو موسیقی، دسته دیگر فایل‌هایی است که برای رایانه اهمیت دارد مثل فایل‌های سیستم. خوشبختانه در این مرحله از مشکلات رایانه فایل‌های اصلی به گونه‌ای نیست که به صورت تصادفی پاک شود، اما گاهی برخی فایل‌های مهم آن پاک می‌شود که خرابی سیستم را در پی دارد.

در این مرحله از حل مشکلات رایانه اگر به صورت تصادفی عکس یا سند مهمی پاک شد، ابتدا ویندوز اکسپلورر را باز کرده و نام فایل را در باکس جستجو تایپ کنید. ممکن است آن را پاک نکرده و فقط اشتباهی به پوشه دیگری منتقل کرده باشید که در این صورت با این جستجو پیدا می‌شود. اگر آن را پیدا نکردید، سطل آشغال را باز کنید شاید به‌طور کلی هنوز پاک نشده باشد، اگر هم فایل‌های زیادی درون آن بود با کلیک راست کردن داخل این پنجره، Sort by را انتخاب کرده و روی Date Deleted کلیک کنید. فایل‌هایی که اخیراً پاک شده‌اند، در بالای پنجره ظاهر خواهند شد.

اگر در این مرحله از حل مشکلات رایانه به نتیجه نرسیدید، باید از ابزار ریکاوری فایل‌های پاک شده مانند نرم‌افزار Recuva استفاده

کنید تا اطلاعات پاک شده شما بازیابی شود. اگر فایل‌های شما باز هم پیدا نشد احتمالا می‌توانید از بک‌آپ آنها را بازیابی کنید. برای حل مشکل رایانه شما ویندوز ۷ نسخه‌های قبلی فایل‌ها را به‌طور خودکار ایجاد می‌کند، به این صورت که باید روی ویندوز اکسپلورر کلیک راست و بعد از انتخاب properties، پوشه‌ای را که شامل فایل است پیدا کنید، سپس روی پوشه کلیک راست کرده و Restore previous را انتخاب کنید. در اینجا فهرستی از بک‌آپ‌های پوشه را که براساس تاریخ فهرست شده‌اند، مشاهده خواهید کرد و این مشکل رایانه به راحتی حل می‌شود.

اما برای حل مشکلات رایانه در ویندوز ۸ باید به‌طور دستی ویژگی File History را روشن کنید. بعد منوی File History را باز و روی Restore personal files کلیک کنید. توجه داشته باشید اگر نتوانستید فایل پاک شده خود را بیابید یا از هیستوری فایل ویندوز بازیابی کنید، هنوز هم نباید ناامید شوید.

در این مرحله از حل مشکلات رایانه اگر پیش از این از سیستم خود بک‌آپ گرفته باشید، می‌توانید در درایو بک‌آپ به دنبال آن بگردید و اگر درایو بک‌آپ، سرویس کلود مانند دراپ باکس یا وان درایو باشد، احتمالا می‌توانید فایل خود را از وبسایت سرویس کلود بازیابی کنید. اما در غیر این صورت، رایانه شما به مشکل برمی‌خورد و باید از نرم‌افزارهای حرفه‌ای ریکاوری مانند DriveSavers استفاده کنید که درایوهای شما را با دقت اسکن می‌کنند تا فایل پاک شده پیدا شود. اگر فایل پاک شده، فایل مهمی از سیستم بود، باید با System Restore آن را تعمیر کنید. شاید هم مجبور شوید برای رفع مشکل رایانه، ویندوز را دوباره نصب کنید.

برای پیشگیری از ریختن مایعات روی سیستم از محافظ استفاده کنید

۳ - ریختن مایع روی سیستم

برای همه پیش می‌آید که فنجان چای یا آب روی کیبورد سیستم‌شان ریخته شود. باید بدانید مایعات به دلیل داشتن نمک و کانی موجب خرابی وسایل الکترونیکی می‌شود. برای حل این مشکل اگر دستگاه شما روشن بود و این اتفاق افتاد، اول آن را خاموش کنید، از برق بکشید و باتری آن را دربیاورید. بعد از آن تمام کابل‌ها، کارتهای رسانه و درایوهای قابل جابه‌جایی را بیرون بکشید و روبه پایین بگیرید تا مایع ریخته شده از آن بیرون بیاید. اگر رایانه شما لپ‌تاپ بود، نذارید مایع نزدیک صفحه نمایش شود. اگر دستگاه‌تان دسکتاپ بود

باید تمام کلیدهای کیبورد سیستم خود را به‌زور هم شده در بیاورید تا مایع درون آن بیرون بریزد، اجزای درون کیس مانند کارت گرافیک را هم خارج کنید. بعد یک هفته صبر کنید و دوباره آن را روشن کنید. امیدواریم رایانه شما مثل سابق کار کند!



۴ - دسترسی نداشتن به اینترنت

شاید هیچ چیز بدتر از این نباشد که بخواهید وبگردی کنید، اما اینترنت قطع شود. در این صورت اول از همه با سرویس‌دهنده خود تماس بگیرید، به جرات می‌توان گفت ۸۰ درصد مواقع مشکل از آی.اس.پی‌هاست. اگر تمام آنچه اپراتور سرویس‌دهنده گفت که مثل همیشه با روشن و خاموش شدن مودم شروع می‌شود، انجام دادید و اینترنت شما وصل نشد، ممکن است مشکل از روتر وایرلس یا از رایانه شما باشد.

از دیگر حل مشکلات رایانه در این مرحله این است که روتر و مودم خود را یک بار از پریز برق بکشید، ۳۰ ثانیه صبر و دوباره مودم را وصل کنید. بعد دوباره ۳۰ ثانیه صبر و روتر را وصل کنید. رایانه خود را ری‌استارت کنید. باید مشکل برطرف شده باشد اما اگر نشد، چک کنید که آیا مشکل از روتر است یا نه، به این صورت که مستقیماً رایانه خود را با استفاده از کابل اترنت به مودم وصل کنید. اگر بعد از این مرحله اینترنت وصل شد، روتر شما مشکل دارد. اما در غیر این صورت، مودم یا کابل اترنت دچار مشکل شده، کابل اترنت دیگری امتحان کنید.

اگر تمام این موارد را چک کردید و هنوز نتیجه نگرفتید، پس مشکل از رایانه است، آسان‌ترین روش امتحان، اتصال به اینترنت از طریق تبلت یا گوشی موبایل است، اگر به‌وسیله آنها به اینترنت وصل شدید دیگر صددرصد مشکل از رایانه است. در این مرحله از حل مشکلات رایانه

برای اینکه مطمئن شوید آداپتور شبکه شما وصل است، به کنترل پنل بروید، وارد Device Manager شوید و Network adapters را انتخاب کنید. روی آن کلیک راست کنید، اگر فعال نبود، Enable را بزنید وگرنه Properties را کلیک کرده و وضعیت دیوایس را چک کنید، اگر کار نمی‌کرد، شاید مجبور شوید درایور آن را به‌روزرسانی کنید. روی تب Driver کلیک کرده و Update Driver را انتخاب کنید.

اگر از وای فای استفاده می‌کنید، اول چک کنید وای فای‌تان روشن باشد، بعضی لپ‌تاپ‌ها دکمه سوئیچ یا Function دارند تا وای - وای روشن یا خاموش شود.

برای حل مشکلات رایانه ابتدا اینترنت را قطع کنید

۵ - ویروسی شدن سیستم

اگر رایانه شما به دلیل منقضی شدن آنتی‌ویروس یا دانلود فایل ویروسی آلوده شود، تبلیغات pop up های ناخواسته‌ای می‌بینید یا سیستم شما کند کار می‌کند یا شاید کرش کند. ابتدا در برای حل مشکلات رایانه خود اینترنت دستگاه را قطع کنید، سیستم را پس از ری‌استارت کردن، در حالت Safe Mode بوت کنید، بعد کلید F8 را چند بار بزنید تا منوی Advanced Boot Options را ببینید، سپس از کلیدهای فلش روبه بالا و پایین استفاده کنید و روی حالت Safe Mode with Networking قرار دهید و دکمه اینترنت را بزنید.



راه های حل مشکلات رایانه

در این مرحله از حل مشکلات رایانه از برنامه ضدویروس و ضدبدافزار استفاده کنید تا چند اسکن انجام شود. حتی اگر برنامه آنتی‌ویروس دارید، باید برنامه جدیدی نصب کنید،

چون برنامه قدیمی به درستی کار نکرده که رایانه شما آلوده شده است. فلش درایور حاوی آنتی ویروس جدید را به سیستم وصل کنید تا برنامه جدید نصب شود، ضمن این که نیازی نیست برای نصب آن به اینترنت وصل باشید. اگر آنتی ویروس نتوانست ویروس را پیدا و پاک کند، باید ویندوز را دوباره نصب کنید.

اگر هم ویروسی بود که با این روشها پیدا و حذف نشد، باید تمام سرویسهای سینک سازی کلود خودکار خود را غیرفعال کنید تا فایل های ذخیره شده شما و دیگر دستگاه هایتان آلوده نشود.

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 معمولاً 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. معمولاً 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 احیاناً با تغییر در دی ان اس مواجه شدید، باید به تنظیمات مودم رفته، ابتدا آن را روی حالت اتوماتیک 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) UPnP را 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 می آید؟



آیا از خود پرسیده اید هنگامی که فردی می میرد، چه اتفاقی برای حساب های بانکی، حساب ای میل و پروفایل های او در شبکه های اجتماعی می افتد؟

دیوید ایگلمن، نویسنده و عصب شنای مشهور یک داستان کوتاه به نام «کلید مرگ» دارد که در مجموعه داستان های او به نام «مجموع» منتشر شده است. او در این داستان به زندگی آنلاین افراد پس از مرگ آنها می پردازد. در بخشی از این داستان آمده است: «در ابتدای دوران کامپیوتر، افراد در حالی می مردند که پسوردهایشان را فقط خودشان می دانستند و پس از مرگشان هیچ کسی نمیتوانست به فایل هایشان دسترسی داشته باشد. گاهی ممکن بود این فایل ها برای یک شرکت ارزشی حیاتی داشته باشند؛ در این حالت شرکت به بحران برمی خورد. به همین دلیل بود که برنامه نویسان کلید مرگ را اختراع کردند.»

ایگلمن سپس درباره این کلید خیالی توضیح می دهد: «کلید مرگ به این نحو کار می کند که کامپیوتر هر هفته یک بار به کاربر می گوید 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 می دهد 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 بازماندگان نشان 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 بخواند 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. تقریباً 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، یا هو 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 مادر بزرگ 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 دیجیتالی 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. مثلاً 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 کاملاً مستقل منتقل می‌کنیم تا مطمئن شویم که به مشکل مالی برخوردیم 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 در گذشته 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. مثلاً، 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 Alphataalk 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 مثلاً 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.» اخیراً 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



۱- عدم نصب ابزارهای امنیتی

تصور داشتن یک زندگی مجازی آرام بدون استفاده از ابزارهای امنیتی به منظور شناسایی و حذف انواع بدافزارها عملاً 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 عملاً 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.

ضمناً 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!

۲- 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. ضمناً از کار افتادگی‌های هارددیسک امری اجتناب‌ناپذیر است! بهتر است با شیوه‌های گوناگون پشتیبان‌گیری 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.

۳- عدم پشتیبان‌گیری آنلاین

یکی از بهترین و امن‌ترین روش‌های موجود برای ذخیره‌سازی کاملاً امن اطلاعات، ارسال آنها به فضای ابرهاست. سرویس Live شرکت مایکروسافت ۲۵ گیگابایت فضای کاملاً مجانی در اختیار کاربران قرار داده و امکان آپلود انواع فایل‌های حجیم را میسر کرده است. البته در Gmail گوگل هم تقریباً 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!

۴- پاسخ به هرنامه‌های تبلیغاتی

یکی از دلایل مهمی که اسپمرها را تشویق به ادامه کار می‌کند، کلیک کاربران روی لینک‌های موجود در هرنامه‌های 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 هرنامه‌ها 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.

۵- حمل دستگاه‌های روشن

حمل نوت‌بوک روشن از اتاق خواب تا نشیمن ایرادی ندارد، اما جابه‌جایی آن مثلاً 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. ضمناً 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.

۶- 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.

۷- 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. ضمناً چاپ کمتر، برابر با قطع کمتر درختان و ایفای نقشی هر چند جزیی در نجات کره زمین است.



۸- اظهار نظرهای آنلاین

در آغاز یک روز کاری بعد از نشستن 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) قدیمی‌ شما 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 شدن تان 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.

۹- 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.

ضمناً 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 صدای ناهنجار و بسیار بلند پخش می‌کند. ضمناً در ویندوز ۷ و ویستا نیز با استفاده از ویژگی Bitlocker می‌توان کار رمزنگاری اطلاعات روی هارددیسک را به منظور عدم دسترسی دیگران به آنها انجام داد.

۱۰- عدم داشتن آدرس ایمیل اضافه

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

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 سرویس‌های ایمیل‌ها را نگهداری کرده و بعضاً 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.

۱۱- 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.

۱۲- نصب نرم‌افزارهای غیرضروری

“چرا ویندوزم کند شده؟” این سوالی است که به شنیدن آن عادت داریم و عوامل گوناگونی در بروز آن نقش دارند؛ احتمالاً 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.

ضمناً بسیاری از برنامه‌های ناشناخته مثل نوار ابزارها 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.

۱۳- 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 فضاهاى 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.

۱۴- 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.

ضمناً 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