

اتصال گوشی اندروید به کامپیوتر با وایرلس (وای فای)



اکثر گوشی های اندروید دارای قابلیت ایجاد شبکه هستند اما ما در حدود صفر از آن استفاده می کنیم. یکی از این کاربردها که می توان از آن بهره برد اتصال گوشی اندروید به رایانه بدون استفاده از کابل است .

۱- نرم افزار wifi file explorer رو نصب کنید.

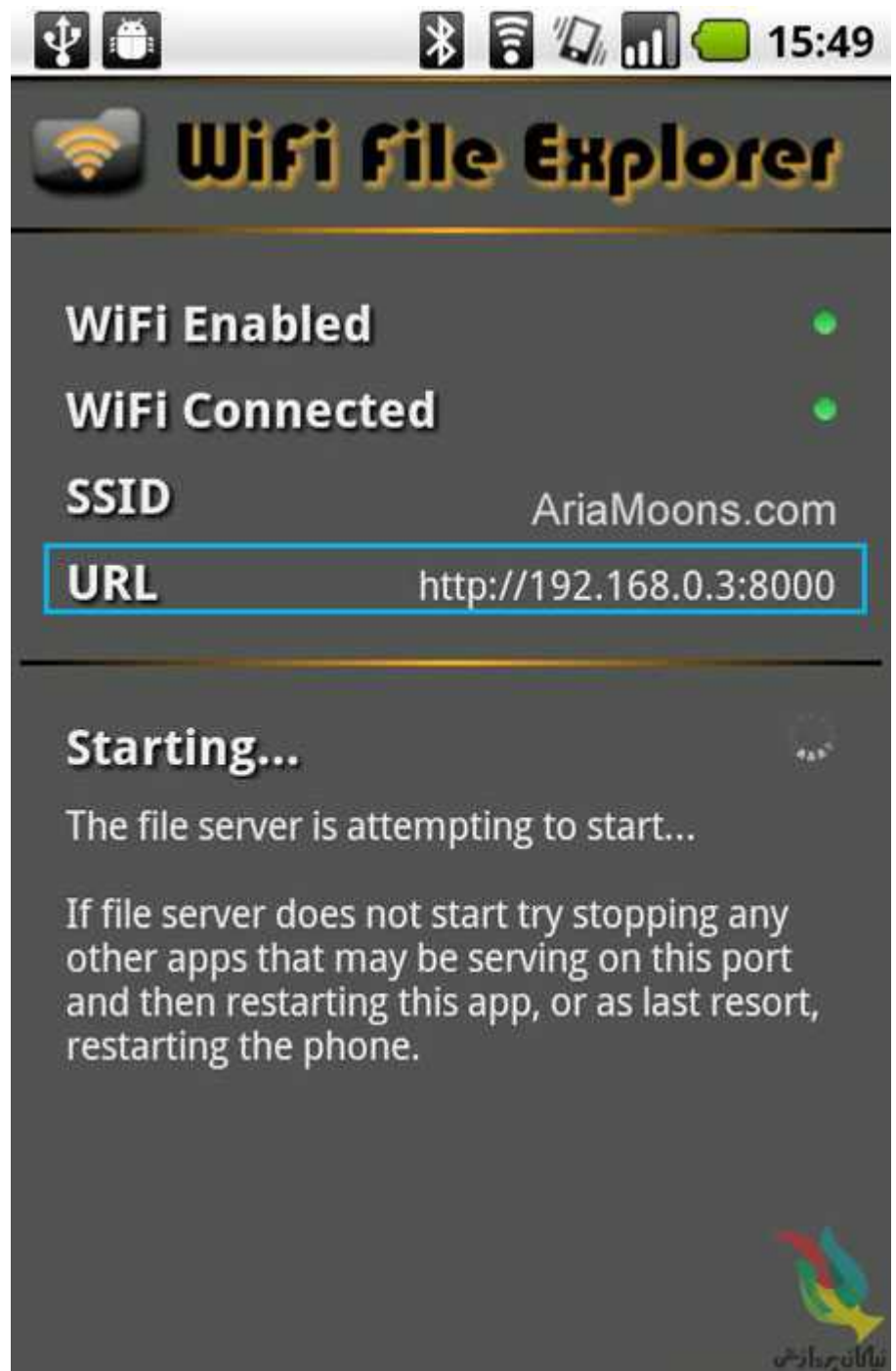
۲- hotspot گوشی خود را روشن کنید. (برای استفاده از این برنامه اول باید اونو نصب کنید بعد به قسمت "Wireless & network" بروید و "terthering & portable hot spot" را انتخاب کنید و تیک گزینه "portable Wi-Fi hotspote" را بزنید. در این بخش می توانید نام شبکه وایرلس ایجاد شده توسط گوشی را ببینید.)

۳- بعد از رایانه خود به hotspot گوشی خود وصل شوید.

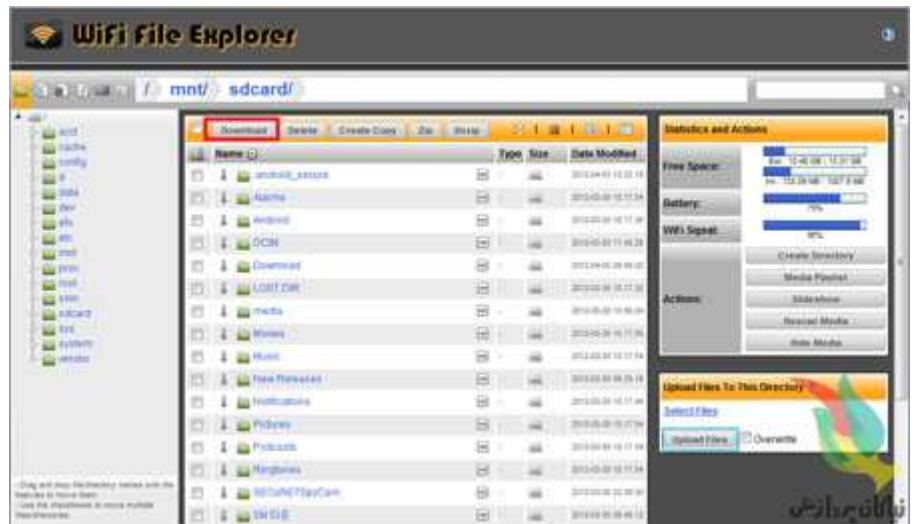
۴- نرم افزار را اجرا کنید .

۵- جلوی کلمه URL یه لینک داده شده است ان را در مرورگر رایانه

وارد کنید .



۶- حالا شما می توانید از روی کارت حافظه گوشی اطلاعات را روی رایانه خود دانلود کنید. (قرمز رنگ در عکس)



۷- برای فرستادن اطلاعات بر روی کارت حافظه گوشی پایین صفحه روی upload کلیک کنید. (ابی رنگ در عکس)

نکاتی مفید برای خرید مودم WiFi



داشتن یک مودم با کیفیت و قدرتمند می تواند به کاربر کمک کند مشکل کمتری در برقراری اتصال به شبکه داشته باشد. با توجه به این که امروزه بیشتر کاربران به جای رایانه های رومیزی و PC از لپ تاپ و تبلت استفاده می کنند و اغلب در هر خانه ای بیش از یک سیستم رایانه ای برای اتصال به اینترنت وجود دارد، مودم های بی سیم یا همان WiFi از محبوبیت بالاتری برخوردار شده اند.

با ما همراه شوید تا با نکاتی کاربردی برای انتخاب یک مودم WiFi مناسب آشنا شوید.

بیشتر مودم های WiFi دارای ۴ پورت LAN هستند، یعنی می توان ۴ سیستم PC یا لپ تاپ را به صورت مستقیم به آن ها وصل کرد. البته مودم های بی سیم تک پورت هم در بازار وجود دارد که نسبت به مدل های ۴ پورت ارزان تر است.

در ضمن برخی از مودم های بی سیم دارای ۲ یا ۳ آنتن هستند که عملکرد آن ها را بهتر می کند، این نوع مودم ها اگرچه کمی گران تر هستند اما برای محیط های بزرگ مانند شرکت ها یا خانه های بزرگ مناسب ترند.



همه مودم های بی سیم و روترها در محدوده فرکانسی ۲٫۴ گیگاهرتز کار می کنند. مودم های بی سیم به لحاظ برد و محدوده پوشش، سرعت انتقال اطلاعات و کیفیت ارسال سیگنال باهم فرق دارند؛ ما در زیر برای انتخاب بهتر، مشخصات این نوع مودم ها را شرح می دهیم:

مودم های بی سیم سری A و B: این مودم ها قدیمی ترین نوع مودم های بی سیم هستند که پوشش داخلی آن ها بسیار ضعیف تر از مودم های بی سیم سری N و G است و محدوده پوشش داخلی این مودم ها حدود ۱۵ متر و پوشش خارجی آن ها ۲۳ متر است.

مودم سری G: حرف G در مودم های بی سیم مخفف کلمه Good است. مودم های بی سیم سری G در حال حاضر در بسیاری از موارد قابل استفاده هستند و می توانند گزینه مناسبی برای استفاده خانگی باشند.

پوشش داخلی مودم های بی سیم این سری حدود ۴۶ متر و پوشش خارجی

این نوع مودم ها حدود ۹۱ متر است که تقریبا ۲ برابر محدوده ای است که مودم های سری A و B می توانند پوشش دهند. مودم های بی سیم سری G همچنین می توانند اطلاعات را با حداکثر سرعت ۱۲۸ مگابایت در ثانیه انتقال دهند و از نظر قیمت نسبت به سری A و B گران تر اما نسبت به سری N ارزان تر ند.

مودم های سری N: حرف N در مودم های بی سیم مخفف Newest Generation به معنی جدیدترین نسل است. این مودم ها بهترین گزینه برای استفاده کاربران خانگی و تجاری و شرکت ها و محیط های بزرگ تر هستند. پوشش داخلی مودم های بی سیم سری G حدود ۷۶ متر و پوشش خارجی ۸۲ متر است که در مقایسه با سری های دیگر بهتر و با کیفیت تر ند.

چطور رایانه خود را خانه تکانی کنیم؟



روش اصولی تمیز کردن قطعات سیستم

در این مطلب آموزشی به شما روش اصولی تمیز کردن قطعات سیستم مانند cd-drive، هارد دیسک و مانیتور را آموزش می دهیم. برای تمیز کردن داخل cd-drive توصیه می کنم از ابزار مخصوص این کار استفاده کنید که در مغازه های کامپیوتری بفروش می رسد. کیت های مخصوص تمیزکردن cd-drive را تهیه و مصرف کنید.

اگر تجربه بیشتری با کامپیوتر و امور فنی آن دارید می توانید این درایو را باز کرده و با گوش پاک کن آغشته به الکل سفید داخل آنرا

تمیز کنید اما برای افراد کم تجربه این عمل به هیچ عنوان توصیه نمیشود برای تمیز کردن cd می توانید از پارچه نرم آغشته به آب استفاده کنید و سطح زیر آنرا بصورت دورانی از مرکز بسمت خارج تمیز کنید. اگر آلودگی بخصوصی در سی دی دیده می شود که با آب تمیز نمی شود می توانید برای آن قسمت از کمی الکل سفید استفاده کنید.



تمیز کردن هارد دیسک

عملا تمیز کردن فیزیکی ندارد زیرا تکنولوژی آن بسیار بالاست و نباید آنرا باز کرد. تمیز کردن آن در واقع عمل دیفراگ است که از طریق برنامه انجام می شود. قبلا در آموزش برخی نرم افزارها به آن پرداخته ایم.

هارد درایوها نسبت به درجه حرارت درون کیس بسیار حساسند. تمیز کردن درون کیس یقیناً هارد درایو را خنک نگاه خواهد داشت. برای این کار شما باید یکی از پانلهای پهلوی کیس را باز کرده و بیرون آورید و گرد و خاک را با یک پارچه خشک پاک کنید.

در اغلب کیس ها تعدادی پیچ در قسمت پشت کیس وجود دارد. این پیچ ها را باز کنید تا به راحتی صفحه پهلویی کیس را بیرون آورید قبل از اینکه شروع به پاک کردن گرد و غبار روی قطعات کامپیوتر خود کنید، یک قطعه فلزی را لمس کنید تا از الکتریسته ساکن در امان بمانید. این کار راحت تر از آن است که هارد درایو یا مادربرد کامپیوتر شما بسوزد و ناچار به تعویض آنها شوید. پس از اینکه این کار را انجام دادید، به آرامی با پارچه ای خشک، گرد و غبار روی هارد درایو خود را پاک کنید؛ همچنین هارد درایوهای

بیرونی (external) نیاز به مقداری مراقبت ویژه دارند. این درایوها هم مانند درایوهای داخلی بیش از اندازه داغ میشوند به ویژه وقتی که کتاب هایتان را در اطراف این درایوهای بیرونی بچینید و یا کاغذ یا موارد دیگری از این قبیل را در پیرامون آنها قرار دهید.

برای اینکه یک درایو بیرونی سرد شود، بایستی هوا به خوبی در آن جریان داشته باشد و در صورتی که شما فضای اطراف درایو را محصور کنید، این کار صورت نخواهد گرفت. همچنین هارددرایو بیرونی خود را با استفاده از اسپری هوای فشرده پاک کنید تا گرد و غباری که بر روی آن نشسته است و سبب افزایش درجه حرارت آن میشود را پاک کنید.

صفحه کلید

یکی از این راه‌ها تمیز کردن صفحه کلید با دستمال آغشته به الکل است. راه دیگر، تمیز کردن صفحه کلید با دستگاه فشار هواست.



مانیتور

برای تمیز کردن شیشه مانیتور می‌توانید از تمیزکننده شیشه معمولی که در خانه استفاده می‌کنید کمک بگیرید. فقط باید مطمئن شوید که مانیتور حتماً خاموش باشد و آنرا از برق بکشید. این مایع تمیزکننده را ابتدا به یک پارچه بدون پرز اسپری کنید و پارچه را بروی شیشه بکشید. با جاروبرقی تمام راههای عبوری هوا را بخوبی تمیز کنید.

توصیه اکید می‌کنم از قرار دادن هر نوع کاغذ و کتاب بروی مانیتور مخصوصاً بخشهای تهویه مانیتور هنگام کار بشدت اجتناب کنید که نه تنها می‌تواند باعث خرابی مانیتور شود بلکه احتمال آتش گرفتن آنرا افزایش می‌دهد. بدنه مانیتور را میتوانید با پارچه

آغشته به آب و مایع ظرفشویی بخوبی تمیز کنید اما اگر مانیتورتان lcd است روش کار اندکی فرق می کند.

این مانیتورها از شیشه ساخته نشده اند لذا هیچوقت هیچ مایعی را مستقیماً بروی آن اسپری نکنید و از دستمال کاغذی از هر نوع برای تمیز کردن آن استفاده نکنید که باعث خش افتادن بروی صفحه آن می شود. اگر میخواهید صفحه مانیتور lcd را تمیز کنید پیشنهاد می کنم از یک پارچه کتان نرم خشک استفاده کنید. اگر صفحه مانیتور بخوبی تمیز نشد میتوانید کمی الکل به پارچه بزنید و صفحه مانیتور را با آن تمیز کنید.



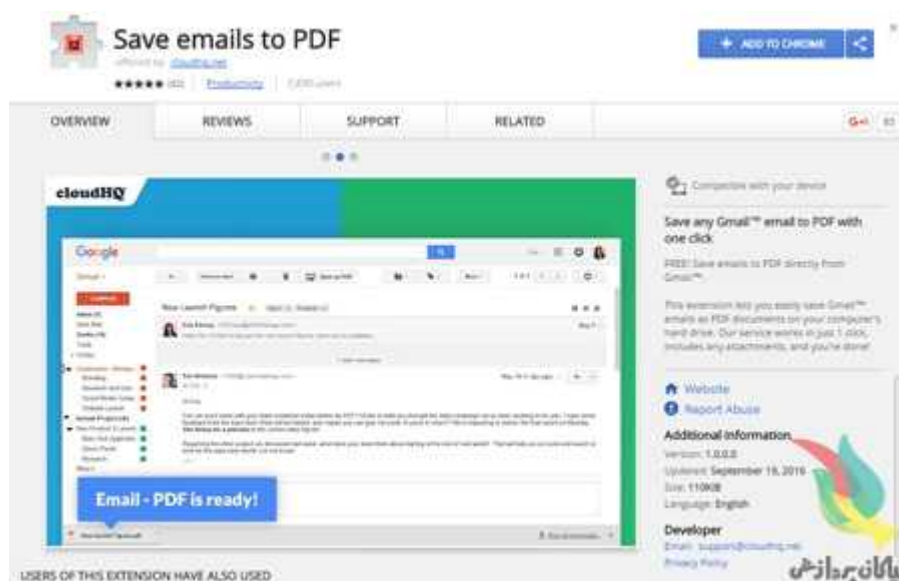
منبع: beytoote

چگونه یک ایمیل را با فرمت PDF ذخیره کنیم؟

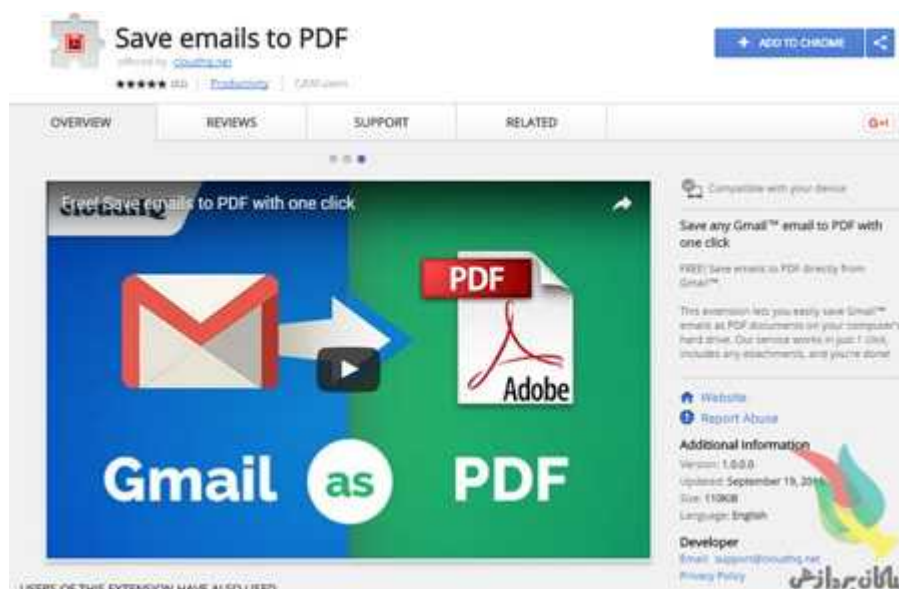
برخی از کاربران فضای مجازی همیشه برای ذخیره کردن ایمیل خود دچار مشکل هستند. با تبدیل ایمیل به یک فایل pdf می توانید آن را همیشه به عنوان یک سند به همراه داشته باشید. برای اینکه بتوانید از این راهکار برای ذخیره ایمیل خود استفاده کنید طبق روش زیر عمل کنید.

برای این کار می‌توانید با بازکردن مرورگر کروم افزونه ای کم حجم

اما کاربردی به نام Save emails to PDF را مورد استفاده قرار دهید.



افزونه برای ذخیره ایمیل‌ها به عنوان pdf در مرورگر کروم Save emails to PDF یک افزونه رایگان است که با دانلود آن گزینه ای به نوار ابزار جیمیل شما اضافه می‌شود. شما می‌توانید با استفاده از این افزونه ایمیل‌های دلخواه خود را به فرمت PDF تبدیل کنید.



تبدیل ایمیل به یک فایل pdf

در این روش ساده تنها باید از طریق لینکی که در انتهای همین خبر برای شما آماده شده است به صفحه مربوط به افزونه در مرورگر گوگل

کروم بروید و با انتخاب گزینه add to chrome افزونه را به نوار بالایی موتور جستجوگر کروم اضافه کنید و در نهایت به سادگی بعد از هر بار باز کردن ایمیل، در نوار بالایی صفحه گزینه save as PDF برای شما ظاهر میشود.

چگونه از ابزار یادداشت برداری قدرتمند Evernote □ استفاده کنیم؟



در دنیای دیجیتال دو نوع کاربر وجود دارد: آنهایی که از Evernote استفاده میکنند و آنهایی که نمیکند! دسته اول اگر این ابزار فوقالعاده را از آنها بگیرد، 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 به‌عنوان دستگاه محاسبه نمی‌شود، تنها دو دستگاه دیگر را می‌توانید به حساب‌تان متصل کنید.

یادداشت‌برداری

هرچه باشد، Evernote یک ابزار یادداشت‌برداری است و قاعدتا همه‌چیز حول این یادداشت‌ها می‌چرخد. ولی بگذارید یک چیز را از همین ابتدا روشن کنیم: اگر می‌خواهید واقعا به قدرت این سرویس پی ببرید، آن

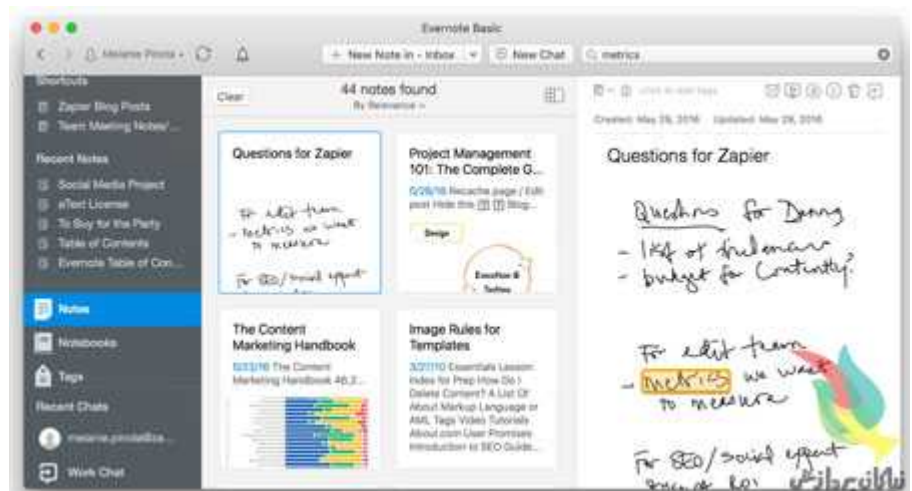
را به صورت یک مخزن یادداشت در کنار بقیه نبینید، بلکه سعی کنید به طور کامل از آن استفاده کنید! اورنوت سرویسی است که هر چه یادداشت بیشتری در آن بگذارید، بیشتر به مفید بودن آن پی می‌برید.

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 های‌لایت را داشته باشید. یعنی تقریباً اطلاعاتی نیست که نتوانید آن را در اورنوت ذخیره کنید؛ می‌توانید به آن به چشم مخزن اطلاعاتی نگاه کنید، نه فقط یک نرم‌افزار یادداشت‌برداری.

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 همگام‌سازی 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 همگام‌سازی نمایش داده می‌شود که با اتمام این عمل، علامت هم حذف می‌شود. البته اگر بخواهید، گزینه‌ای هم برای درخواست همگام‌سازی به صورت دستی در منوی اصلی برنامه وجود دارد.

Evernote یک ابزار یادداشت‌برداری است و قاعدتاً همه چیز حول این یادداشت‌ها می‌چرخد.



ساختار 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 براحتی 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 براحتی پیدا کنید.

Evernote برای حرفه‌ای‌ها

اورتوت 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) به‌کار 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 میان‌یادداشتی: در حالت عادی Evernote را می‌توان در فهرستی از یادداشت‌ها خلاصه کرد، اما یک ترفند ساده می‌تواند یادداشت‌هایتان را از این حالت خشک دریاورد 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.

منبع: beytoote

چگونه در گروه‌های وایبر ادمین

شویم؟



وایبر یکی از محبوب‌ترین اپلیکیشن‌های پیام‌رسان در سراسر دنیا است که در ایران نیز به عنوان محبوب‌ترین اپلیکیشن در این حوزه به شمار می‌رود.

در جدیدترین بروزرسانی این اپلیکیشن امکانی به آن اضافه شده است که می‌توانید برای گروه‌های خود یک ادمین (مدیر) انتخاب کنید. اگرچه با شروع سال ۹۴، تعداد بسیاری از کاربران ایرانی با افت سرعت شدید این اپلیکیشن، به حدی که استفاده از آن را غیر ممکن می‌کند مواجه شده‌اند، اما با این حال هنوز کاربران در حال استفاده از آن هستند و همین موضوع نشان از محبوبیت بالای این اپلیکیشن در داخل کشور دارد.

بخش بزرگی از این محبوبیت وایبر، به گروه‌ها، چه از نوع فامیلی، چه دوستانه اختصاص دارد و به احتمال زیاد شما هم حداقل یک گروه وایبری را در لیست گفتگوهای خود دارید. تا پیش از جدیدترین بروزرسانی وایبر، این گروه‌ها به طور کامل یک مکان عمومی به حساب می‌آمدند به طوری که اگر شخصی را به آن دعوت می‌کردید، دیگر هیچ راهی برای برگشت از این تصمیم و خارج کردن آن فرد از گروه نداشتید.

در واقع امکانات تاسیس‌کننده‌ی گروه با اشخاصی که بعد از آن اضافه می‌شوند یکسان بود که این موضوع در مواقعی موجب مشکلاتی می‌شد. اما با امکان جدیدی که وایبر در اختیار شما قرار می‌دهد می‌توانید یک ادمین برای گروه خود انتخاب کنید تا در صورت نیاز، بتوانید فردی را از گروه خود خارج کنید. امکانات ادمین گروه تنها در حد حذف افراد از گروه خلاصه خواهد شد و همچنان افراد دیگر نیز می‌توانند عضوهای جدید به گروه دعوت کنند.



این امکان به صورت پیش‌فرض در گروه‌های جدید قرار خواهد گرفت به این صورت که، شخصی که گروه را تاسیس می‌کند، به طور پیش‌فرض ادمین گروه نیز خواهد بود. اما برای گروه‌هایی که پیش از این ساخته شده‌اند و البته به آخرین نسخه وایبر به روزرسانی کرده‌اند، گزینه‌ای در منوی کناری با عنوان Add Me As Admin اضافه می‌شود که با کلیک روی آن می‌توانید ادمین گروه شوید.

نکته‌ی جالب و شاید حاشیه‌سازی که در این بخش قرار دارد این است که شخصی که زودتر این گزینه را ببیند و روی آن کلیک کند به ادمین گروه تبدیل می‌شود حتی اگر جدیدترین عضو گروه باشد و بعد از آن نیز شخص دیگری قادر به انتخاب این گزینه نخواهد بود و تنها در صورتی امکان وجود ادمین دوم وجود دارد که ادمین اصلی او را تایید کند. این موضوع مورد انتقاد جدی برخی از کاربران قرار گرفته است بخصوص در گروه‌های عمومی که افراد داخل گروه شناخت چندانی از هم ندارند. در این گروه‌ها شخصی که به طور اتفاقی ادمین می‌شود به طور سلیقه‌ای می‌تواند افراد دیگر را از گروه حذف کند.

اگر شما هم علاقه‌مند به ادمین شدن در گروه‌های دوستانه و فامیلی خود هستید، کافی است تا جدیدترین نسخه وایبر را دانلود، و بعد از آن مانند تصویر بالا، خود را به عنوان ادمین گروه انتخاب کنید.

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، 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 احتمالاً 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، احتمالاً 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 دریاورید. 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، نگذارید 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 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 و گرنه 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 – فای 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 به‌درستی کار نکرده که رایانه شما آلوده شده است. فلش درایور حاوی آنتی‌ویروس جدید را به سیستم وصل کنید تا برنامه جدید نصب شود، ضمن این‌که نیازی نیست برای نصب آن به اینترنت وصل باشید. اگر آنتی‌ویروس 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 سینکسازی کلود خودکار خود را غیرفعال کنید تا فایل‌های ذخیره شده شما و دیگر دستگاه‌هایتان آلوده نشود.

چگونه به icloud دسترسی پیدا کنیم؟



iCloud

کاربران اپل می‌توانند به این سرویس ابری، بدون مراجعه به سایت icloud و استفاده از مرورگر، به اطلاعات ذخیره شده در icloud خود دسترسی داشته باشند.

فضای ابری محیطی است که کاربران می‌توانند فایل‌ها و اطلاعات خود را در آن نگهداری کنند و در هر کجای دنیا که به اینترنت متصل شوند به اطلاعات خود دسترسی خواهند داشت.

شرکت‌های زیادی این سرویس را به کاربران ارائه می‌دهند. شرکت اپل هم این سرویس را با نام iCloud در اختیار مشترکین خود قرار می‌دهد. کاربران محصولات شرکت اپل می‌توانند با ثبت نام در این فضای ابری، به ۵ گیگا بایت فضای رایگان دسترسی داشته باشند که در صورت نیاز به فضای بیشتر می‌توانند آن را خریداری کنند.

برای دسترسی به فضای ابری شرکت اپل، کاربران باید وارد سایت icloud شوند. اپل این امکان را طوری در اختیار مشترکین خود قرار داده است که بتوانند از رایانه خود به صورت مستقیم به iCloud دسترسی پیدا کنند.

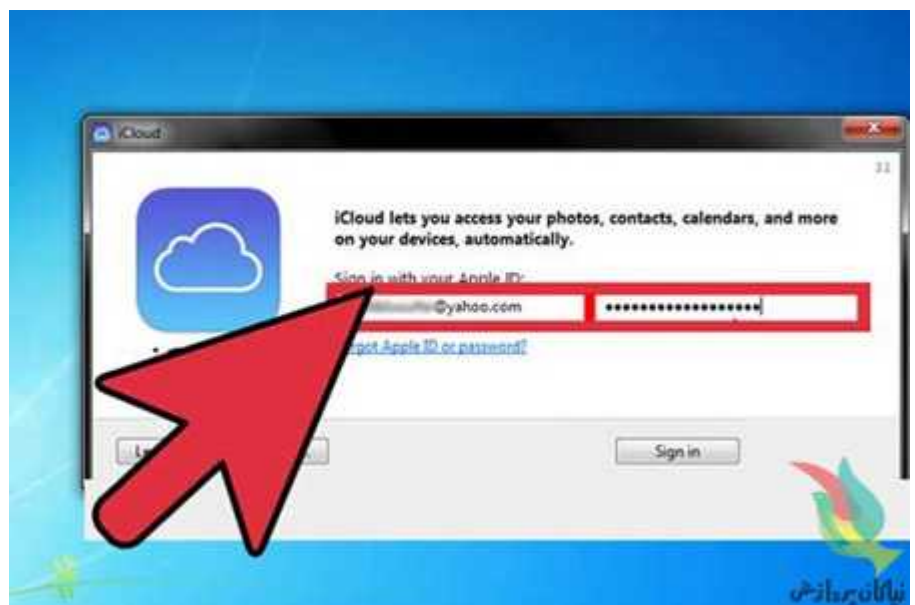
۱- به صفحه کنترل پنل iCloud



آموزش استفاده از سرویس icloud

مرور گر خود را باز کنید و به آدرس www.icloud.com/icloudcontrolpanel مراجعه کنید که برنامه icloud را دانلود کنید.

۲- کنترل پنل iCloud را نصب کنید

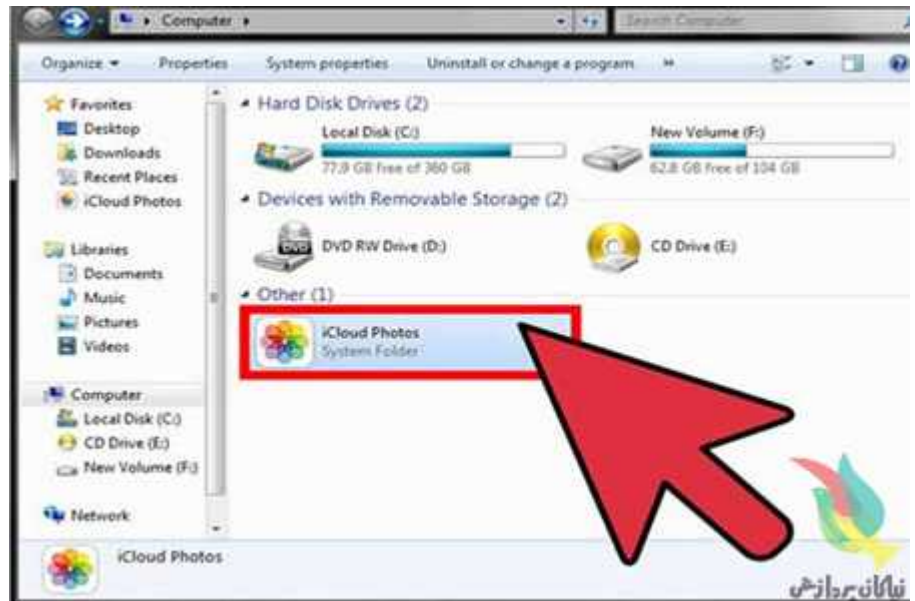


فضای ابری محیطی است که کاربران می توانند اطلاعات خود را در آن نگهداری کنند.

بر روی فایل دانلود شده کلیک کنید و مراحل نصب شروع شود. مرحله به مرحله نصب را پیش ببرید و در پایان Shortcut برنامه را در

Desktop خود خواهید دید.

۳- iCloud را فعال کنید



بر روی آیکون برنامه در Start Menu یا Desktop رایانه خود کلیک کرده و آن را باز کنید. در پنجره نمایان شده، نام کاربری و کلمه عبور خود را وارد کنید.

پس از اینکه در iCloud نام کاربری و رمز عبور خود را وارد کردید، می توانید به اطلاعات ذخیره شده در iCloud خود دسترسی داشته باشید. کافست برنامه نصب شده را اجرا کنید تا عکس ها، شماره های تماس و دیگر اطلاعات خود را که در سرویس ابر اپل ذخیره کرده اید را ببینید.

منبع: beytoote

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 زیر 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 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، دارای‌های 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، پسردهای افراد درگذشته هم به دست افرادی برسد که خود فرد تعیین کرده بود.

اگر فردی بمیرد، سایت‌های شبکه‌های اجتماعی به راحتی پسرود 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 وکلای 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.

Google



!Yahoo

ياهو 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 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 مرتباً 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. مثلاً 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 مرتباً 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 برنخواهیم خورد. همچنین از فناوری‌های ساده و استانداردهای باز استفاده می‌کنیم تا با انقضای 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. 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 فرزندان‌شان 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 طفر 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 پسوندهای 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؟