وای‌فای لذیذ

برای داشتن یک وای‌فای خانگی امن و سریع این ۹ مقاله را بخوانید

فهرست

ده روش ساده افزایش سرعت شبکه‌های وای‌فای خانگی

احتمال این‌که همین الان با وای‌فای به اینترنت متصل شده باشید و دارید این مقاله را می‌خوانید زیاد است. اگر همین‌طور است، شاید گاه‌گداری پیش آمده که شبکه وای‌فای‌تان آن‌طور که دوســـت دارید خوب کار نمی‌کند. راه‌های بسیار ســـاده‌ای وجود دارد که می‌توانید عملکرد شبکه وای‌فای‌تان را بهبود ببخشید. در این مقاله ما به ده تا از آن‌ها اشاره می‌کنیم.

ما اغلب به شبکه‌های وای‌فای به عنوان یک میدان یکنواخت فکر می‌کنیم که فضای زندگی ما را پر کرده اســـت. در حقیقت وای‌فای یک سیگنال فیزیکی است که می‌تواند توســـط دیوار و دیگر دستگاه‌های الکترونیکی و حتی خود

ما ســـد و یا پراکنده شود. برای اثبات این مســـئله به نقشه وای‌فای ای که جیسون کول، دانشجوی ارشد فیزیک از آپارتمان خود تهیه کرده است نگاهی بی‌اندازید.
واضح است که مکانی که روتر خود را قرار می‌دهید و چیزهایی که اطراف آن قرار دارد تاثیر زیادی روی قدرت شبکه دارند. در ادامه به چگونگی بهینه‌ترین چینش برای شبکه شما خواهیم پرداخت.

۱ . روتر را نزدیک مرکز خانه قرار دهید

روتر سیگنال را به تمام جهات انتشار می‌دهد، بنابراین قرار دادن آن در یک گوشه از خانه یا نزدیک پنجره به معنی هدر رفت بخش قابل توجه‌ای از سیگنال آن است. ممکن است نیاز باشد تا اتصال شبکه به یکی از دستگاه‌های‌تان را با کابل شبکه تامین کنید، اما کابل‌های شبکه طول و دراز قیمت چندانی ندارند و جابجا کردن روترتان می‌تواند تاثیر شگرفی در بهبود عملکرد آن داشته باشد.

۲ . روتر را از سطح زمین بالاتر قرار دهید

دو دلیل وجود دارد که بهتر است روتر را مستقیم روی زمین قرار ندهید. یکی این‌که اغلب آن‌ها طوری طراحی شـــده‌اند تا سیگنال را کمی به سمت پایین منتشر کنند. علاوه بر آن نمی‌توانند به سادگی در مصالحی مثل آهن و بتن و سیمان که احتمالا در ساخت کف خانه شما از آن‌ها استفاده شده نفوذ کنند. در نتیجه، متخصصان توصیه می‌کنند که روترتان را حداقل یک متر بالاتر از سطح زمین، مثلا بر روی یک میز یا قفسه کتاب‌خانه قرار دهید. به همین دلیل

شـــما نباید روتر را در زیر زمین قرار دهید. مخصوصا اگر خانه‌تان چند طبقه است و فندانسیون بتنی دارید.

۳ . روتر را در اتاقی قرار دهید که بیشتر از اینترنت استفاده می‌کنید

صرف نظر از محل قرارگیری روتر، سیگنال در اتاقی که روتر در آن قرار دارد از همه‌جا قوی‌تر اســـت. پس در حالت ایده‌آل شما می‌توانید آن را نسبتا در مرکز خانه و اتاقی که از دستگاه‌های متصل به وای‌فای استفاده می‌کنید قرار دهید.

۴ . روتر را در فضای باز قرار دهید

از آن‌جا که سیگنال روتر می‌تواند توسط خیلی از مواد جذب شود، باید آن را تا جای ممکن در فضای باز قرار دهید. به بیان دیگر، آن را در کمد قایم نکنید و یا بین مبلمان قرار ندهید. امواج رادیویی در هوای باز بهتر منتقل می‌شوند، بنابراین خط دید را در نظر داشته باشید. اگر می‌توانید روتر را از فاصله دور و از بسیاری جهات مختلف ببینید، آن را در جای درستی قرار داده‌اید.

۵ . روتر را از دیگر دستگاه‌های الکترونیکی دور نگه دارید

تمام دســـتگاه‌های الکترونیکی می‌توانند در سیگنال روتر تداخل ایجاد کنند: میکروفر، تلویزیون، تلفن‌های بی‌سیم و اساسا هرچیز که سیگنال الکترومغناطیس تولید می‌کند یا موتور دارد. به همین خاطر است که ساندویچ کردن آن بین تجهیزات سرگرمی‌های خانگی در زیر تلویزیون ایده خوبی نیست. به طور کلی

روتر را از دیگر دستگاه‌های الکترونیکی دور نگه دارید. اشیاء بزرگ فلزی (مثل آینه‌ها یا کابینت‌ها) و آب (مثلا آکواریوم) می‌توانند سیگنال را سد کنند و باید از آن‌ها پرهیز کنید.

۶ . یک آنتن را به صورت عمودی و دیگری را به شکل افقی تنظیم کنید

از آن‌جا که سیگنال روتر به شکل قائم بر آنتن منتشر می‌شود، عقل سلیم می‌گوید که آنتن‌های عمودی سیگنال را به شکل افقی پخش می‌کنند و فضای بیشتری از خانه را پوشش می‌دهند. صحیح، اما این مسئله در مورد تراز کردن آنتن‌های دستگاه‌ها در جهت یکسان با آنتن روتر برای به حداکثر رساندن دریافت سیگنال نیز صدق می‌کند. بیشتر لپ‌تاپ‌ها آنتن‌های داخلی افقی دارند اما یک تلفن یا تبلت بسته به شکلی که آن را نگه می‌دارید؛ احتمالا در موقعیت متفاوتی قرار می‌گیرد. تنظیم یک آنتن روتر به صورت عمودی و آنتن دیگر در جهت افقی می‌تواند تمام سطوح را پوشش دهد و در عین حال سیگنال را تا جای ممکن به شکل یکنواخت در خانه پخش کند.

۷ .قدرت سیگنال را اندازه بگیرید

تعدادی اپ مثل Cloud check یا Wi-Fi Analytics وجود دارد که به شما امکان می‌دهد تا نقشه‌ای از سیگنال وای‌فای در سرتاسر خانه‌تان رسم کنید و بفهمید سیگنال در کدام نقاط ضعیف است. این کار می‌تواند به شما برای قراردهی بهتر روتر سرنخ‌هایی بدهد.

۸. تنظیم نرم‌افزار روتر

در بعضی موارد تنظیمات و دست‌کاری‌های نرم‌افزاری وجود دارد که می‌تواند شبکه وای‌فای را بهبود ببخشد. برای تنظیم نرم‌افزاری روتر معمولا باید آدرس آی‌پی مشـــخصی را در مرورگر وب وارد کنید (برای فهمیدن آدرس آی‌پی، پنل پشتی روتر را نگاه کنید یا نام روتر را در اینترنت جستجو کنید). وقتی وارد تنظیمات شدید، دو چیز مهم را می‌توانید امتحان کنید.

یکی تغییر کانالی است که روتر روی آن کار می‌کند. این مورد برای روترهای جدید کمتر مشکل‌ساز است اما روترهای قدیمی‌تر اغلب با هم تداخل می‌کنند (مخصوصا در نواحی شلوغ شهری با شبکه‌های زیاد) و تغییر کانال فرکانس می‌تواند راه‌حلی برای آن باشـــد. روترهای قدیمی روی ۱۴ فرکانس مختلف کار می‌کنند و کانال‌های ۱، ۶ و ۱۱ عموما بهتر هســـتند، چرا که کمتر روی کانل‌های دیگر می‌افتند و تداخل کمتری ایجاد می‌کنند. کانال پیش‌فرض ۶ است اما اگر مشکل سیگنال دارید کانال‌های دیگر را امتحان کنید.

گزینه دیگر ارتقا نرم‌افزار روتر اســـت (که به آن فریم‌ویر گفته می‌شود). این کار برای تمام روترها ممکن نیست اما شرکت‌ها هر از چندگاهی فریم ویرهای رایگانی برای ارتقا روترهای قدیمی‌تر روی وب‌سایت‌های‌شان قرار می‌دهند که می‌تواند در بهبود عملکرد روتر موثر باشد. برای این‌که ببینید برای روتر شما هم فریم‌ویر جدیدی آمده باید به سایت شرکت سازنده مراجعه یا اینترنت را جستجو کنید.

۹. بررسی کنید اشکال از طرف شرکت سرویس‌دهنده اینترنت نباشد

یک راه ساده برای اطمینان از این‌که مشکل از روتر است و اشکال از سمت سرویس‌دهنده اینترنت نیست، اجرای تست سرعت تحت دو حالت متفاوت است: یک بار از طریق وای‌فای و بار دیگر از طریق کامپیوترتان که توسط یک کابل اترنت مستقیما به روتر متصل شده است. اگر هر دو با مشکل کندی سرعت مواجه‌اند، احتمالا برای رفع اشکال یا ارتقا نوع اینترنت باید با ISP خود صحبت کنید اما اگر سرعت وای‌فای خیلی کندتر است پس به احتمال زیاد اشکال از خود روتر است.

۱۰.اگر هیچ‌کدام از روش‌ها کارساز نبود، باید تجهیزات جدید خریداری کنید

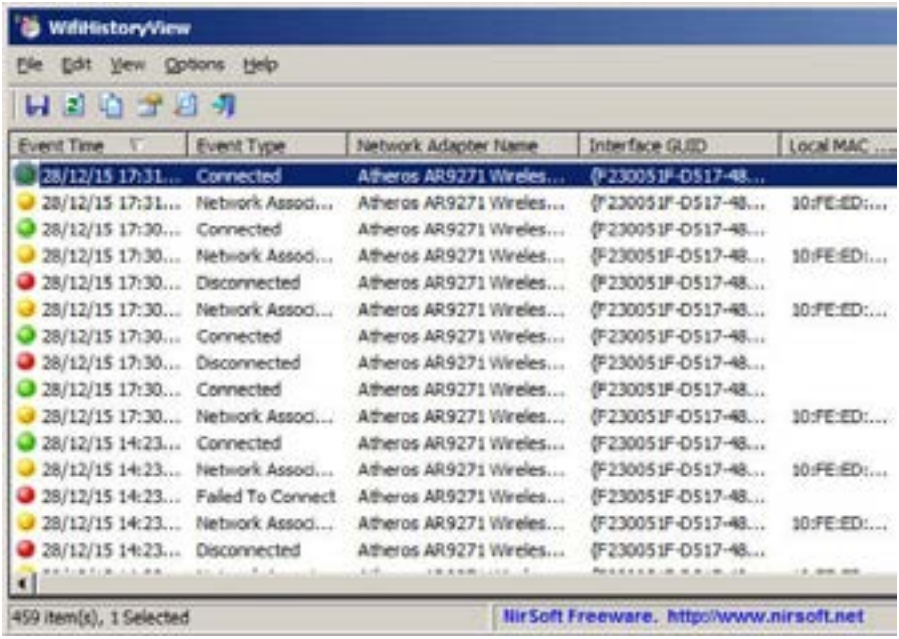
اگر هنوز هم با مشکلات شبکه مواجه هستید و هیچ‌کدام از این راه‌کارها کارساز نبود، ارتقا به یک روتر جدید می‌تواند تغییر چشم‌گیری ایجاد کند، چرا که فناوری استفاده شده در انتشار سیگنال در طی سال‌های اخیر تغییر بسیاری کرده است. شما همچنین می‌توانید روتر فعلی‌تان را با نصب یک آنتن قوی‌تر ارتقا دهید، اما فقط بعضی از روترها این اجازه را به شما می‌دهند. سرانجام، برای افزایش برد روتر خود می‌توانید یک تقویت‌کننده یا repeater خریداری کنید. تقویت‌کننده دستگاهی است که شبکه فعلی شما را می‌گیرد و مجدد منتشر می‌کند. این‌کار اصلا پهنای‌باند شما را افزایش نمی‌دهد اما شبکه را تا فاصله بیشتری پخش می‌کند

شبکه وای‌فای شما به این ۵ دلیل کند است + راه‌حل

برای دو دهه است که اینترنت با زندگی ما اجین شده است، صرف‌نظر از تمام تغییرات و پیشرفت‌هایی که در فناوری صورت گرفته، یک چیز همچنان ثابت باقی مانده است و آن هم نوع و شیوه اتصالات است. وقتی صفحات وب باز نمی‌شوند، ویدیوها به درستی بافر نشده و دائم قطع و وصل می‌شوند یا ایمیل‌ها قصد باز شدن ندارند، تازه مشکلات و فشار عصبی کاربران اینترنت شروع می‌شود. در ادامه پنج مشکل رایج و راه حل برطرف کردن آن را بررسی خواهیم کرد.

۱. سارقان اینترنت

یکی از بهترین مزیت‌های استفاده از یک شبکه وای‌فای امکان دسترسی سریع و آسان به اینترنت است. اما اگر کلمه عبور شبکه شما بیش از اندازه ساده باشد، این امکان را فراهم میکند تا افراد غریبه هم بتوانند به آن دسترسی داشته باشند و به این شکل هم امنیت و هم پهنای باند اینترنت شما دچار مشکل خواهد شد. مسلما این چیزی نیست که شما می‌خواهید. شبکه‌هایی که از کلمات عبور ضعیف استفاده می‌کنند و یا اصلا از آن استفاده نمی‌کنند در معرض خطر جدی دستبرد زدن توسط دیگران هستند. برای این که بدانید چه دستگاه‌هایی به شبکه شما متصل شده‌اند می‌توانید



از نرم افزار رایگان Wi-Fi History View استفاده کنید و آدرس‌های ای‌پی ناشناس را پیدا کنید.

برای پیشگیری از نفوذ بیگانگان به شبکه اختصاصی خود و جلوگیری از سرقت اینترنت و پهنای باند اولین قدم این است که کلمه عبور روتر خود را تغییر دهید. اگر نمی‌دانید کجا می‌توانید آن را پیدا کنید، سایتی به نام Router Passwords وجود دارد که می‌تواند در زمینه پیدا کردن کلمه عبور سازنده روتر به شما کمک کند. بعد از آن، یک کلمه عبور طولانی و پیچیده را انتخاب کنید که به راحتی نتوان آن را حدس زد.

۲. ازدحام

این مشکلی است که بیشتر برای محلات و آپارتمان‌های شلوغ از نظر تعداد شبکه‌های بی‌سیم رخ می‌دهد. وقتی تعداد زیادی کاربر قصد داشته باشند همزمان به یک کانال وای‌فای یکسان متصل شوند، سرعت اتصال به طرز قابل ملاحظه‌ای تحت تاثیر قرار خواهد گرفت.

وقتی سرعت اتصال شما به شبکه در ساعات خاصی از روز کند می‌شود، که معمولا این موضوع در عصر و زمانی که اکثرا از سر کار به خانه برگشته‌اند بیشتر اتفاق می‌افتد، این مشکل یک نشانه بزرگ از وجود تراکم و ازدحام در سیگنال‌های وای‌فای است. برای رفع این مشکل از یک کانال دیگر در روتر خود استفاده کنید.

اگر روتر شما از فرکانس ۲,۴ گیگاهرتز استفاده می‌کند، معمولا ۱۱ کانال برای انتخاب وجود دارد. بیشتر کانال‌های ۱، ۶ و ۱۱ توصیه شده است، اما برای پیدا کردن یک اتصال سریع‌تر بهتر است سایر کانال‌ها را نیز امتحان کنید. خرید یک روتر پشتیبانی کننده از باند جدیدتر ۵ گیگاهرتز هم کمک بزرگی به رفع این مشکل می‌کند.

۳. تجهیزات از رده خارج

همه روترهای وای‌فای یکسان ساخته نمی‌شوند. روترهای AC یک مرحله پیشرفته‌تر از مدل‌های قدیمی‌تر B و G و حتی مدل N هستند. این روترهای جدید قابلیت‌های بیشتری داشته و عملکرد بهتری از خود نشان می‌دهند. اگر قصد خرید یک روتر جدید را دارید بهتر است به دنبال نوع جدید AC باشید. روترهای AC داری حداکثر گستره پهنای باند در حدود ۸ در ۱۶۰ مگاهرتز هستند که در مقایسه با ۴ در ۴۰ استاندارد N گسترده‌تر است. به عبارت دیگر، هر چه پهنای باند گسترده‌تر باشد امکان تبادل داده بدون افت سرعت نیز بیشتر می‌شود.

۴. تنظیمات امنیتی روتر شما

گذشته از محافظت از شبکه شما در مقابل استفاده از پهنای باند توسط افراد غیر مجاز که می‌توانند بدون این که شما متوجه

باشید، سرعت شبکه شما را به میزان قابل ملاحظه‌ای کاهش دهد، آیا می‌دانستید که نوع امنیت بی‌سیمی که شما استفاده می‌کنید نیز می‌تواند روی عملکرد کلی سرعت شما نیز تاثیر گذار باشد؟ اگر شبکه شما به اصطلاح باز (بدون امنیت) است یا از استاندارد امنیتی WEP استفاده می‌کنید، فورا تنظیمات امنیتی خود را تغییر دهید. مسلما تلاش برای دسترسی به یک شبکه باز بسیار راحت‌تر به نتیجه می‌رسد و استاندارد امنیتی قدیمیWEP را آسان‌تر می‌توان هک کرد، بنابراین به هیچ وجه از آن استفاده نکنید.

گزینه‌های امنیتی دیگر پیش روی شما WPA, WPA2 with TKIP و WPA2 with AES هستند. WPA و TKIP نیز استانداردهای دیگری هستند که باید از آن پرهیز کرد. این دو پروتکل نه تنها قدیمی و ناامن هستند بلکه می‌توانند سرعت شبکه شما را هم کم کنند. بهترین گزینه استفاده از WPA2 with AES است. AES یک پروتکل جدیدتر و امن‌تری است که سرعت بیشتری را نیز در اختیار شما قرار می‌دهد.

۵. شما خیلی دورتر از محدوده سیگنال‌دهی هستید

بعضی اوقات آسان‌ترین راه برای رفع مشکل درست پیش چشم ما است. ساختار روترها به گونه‌ای طراحی نشده تا بتوانند سیگنال‌ها را تا مسافت‌های طولانی منتقل کنند، بنابراین در بخش‌هایی از

خانه شما ممکن است به اصطلاح نقطه کوری وجود داشته باشد که سیگنال وای‌فای به آنجا نمی‌رسد. برای تهیه یک نقشه جامع از مناطق تحت پوشش سیگنال شبکه خود از یک ابزار به نام HeatMapper استفاده کنید. این کار به شما کمک می‌کند ببینید کجای منزل یا محل کار شما سیگنال وای‌فای قویتری دارد. HeatMapper یک نرم افزار رایگان تحت ویندوز است که می‌توانید به راحتی آن را دانلود و استفاده کنید. اگر از کاربران مک هستید NetSpot جایگزین خوبی برای این کار است.

وقتی شما نواحی مشکل‌دار خانه را پیدا کردید، چند گزینه پیش روی شما است. یک گزینه خرید یک گسترش دهنده وای‌فای است که می‌تواند گستره انتشار سیگنال روتر شما را تقویت کند. گسترش دهنده‌های وای‌فای بر اساس مدل و قابلیت‌هایی که ارائه

می‌کنند قیمتی در حدود ۲۰ تا ۱۲۰ دلار دارند. معمولا یک گسترش دهنده سطح متوسط جوابگوی نیاز شما خواهد بود.

گزینه دوم خرید یک سیستم حرفه‌ای مخصوص ترکیبی است. برای مثال Eero Home Wi-Fi system پانصد دلاری تضمین می‌کند که دیگر نقطه کوری در خانه شما باقی نمی‌گذارد. یک سیستم ترکیبی و مخصوص شامل مجموعه‌ای از روترهای کوچک است که با هماهنگی بین یک دیگر محدوده تحت پوشش شبکه شما را گسترش می‌دهد. تنها کافی است این روترها را در بخش‌های مختلف خانه قرار دهید تا سیگنال به تمام نقاط خانه ارسال شود.

چگونه رمز وای فای خودمان را پیدا کنیم

گاهی پیش آمده که رمز عبور شبکه وای‌فای‌مان را فراموش کرده‌ایم یا در منزل یکی از آشنایان هستیم و نمی‌خواهیم رمز وای‌فای را مجددا سوال کنیم. در این مقاله به راه‌های بدست آوردن و بازیابی رمز عبور شبکه وای‌فای خواهیم پرداخت.

پیدا کردن رمزعبور پیش‌فرض ثبت شده بر روتر

روترهای وای‌فای مدرن و دستگاه‌های ترکیبی مودم و روتر که توسط خیلی از سرویس دهندگان اینترنت ارئه می‌شوند، یک نام شبکه وای‌فای و یک رمزعبور پیش فرض دارند. این رمز تصادفی است و هر روتر رمزعبور مختص خود را دارد. اگر هنوز این رمز پیش فرض را تغییر نداده‌اید، می‌توانید از طریق همان رمز اولیه به شبکه متصل شوید. برای یافتن رمز پیش فرض باید بر روی بدنه

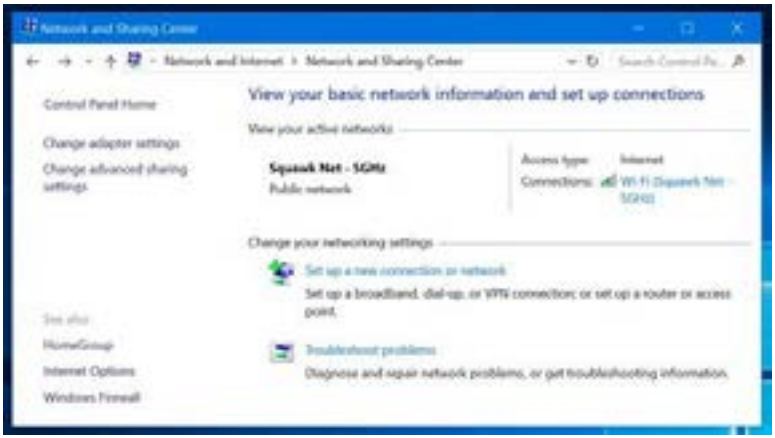
روترتـان بـه دنبـال برچسـبی بگردیـد کـه SSID (نـام شـبکه بی‌سـیم) و رمـز عبـور بـر روی آن ثبـت شـده اسـت.

اگـر رمـز بـر روی خـود روتـر نوشـته نشـده، در دفترچـه راهنمـای روتـر بـه دنبـال آن بگردیـد. اگـر دفترچـه در دسـترس‌تان نیسـت می‌توانیـد شـماره مـدل دسـتگاه را بـر روی اینترنـت جسـتجو کنیـد.

پیدا کردن رمز عبور در ویندوز

اگـر از یـک لپ‌تـاپ یـا کامپیوتـر دسـکتاپ ویـنـدوزی بـه شـبکه وای‌فای متصـل شـده باشـید، ویـنـدوز ایـن رمـز را بـه خاطـر می‌سـپارد و از همین طریـق قادریـد بـه رمـز عبـور دسترسـی پیـدا کنیـد. بـرای ایـن‌کار بـه کنتـرل پانـل برویـد و در ذیـل Network and Internet بـر روی View network status and tasks کلیـک کنیـد. سـپس در سـمت راسـت Connections (اتصـالات) روی نـام اتصـال فعلـی وای‌فـای کلیـک کنید.

اگـر قبـلا بـه شـبکه وای‌فـای متصـل بوده‌ایـد و در حـال حاضـر بـه آن وصـل نیسـتید، بایـد در سـمت چـپ پنجـره بـر روی Change adapter settings کلیـک کنیـد و سـپس در پنجـره جدیـد بـر روی نـام شـبکه راسـت کلیـک کنیـد و Status را انتخـاب کنیـد.



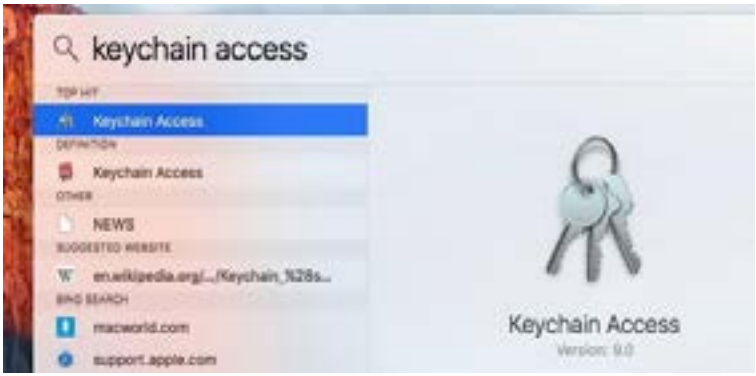
در پنجره Wi-Fi Status بر روی Wireless Properties کلیک کنید.

حـالا بـر روی سـربرگ Security کلیـک کنیـدو کادر Show charac-

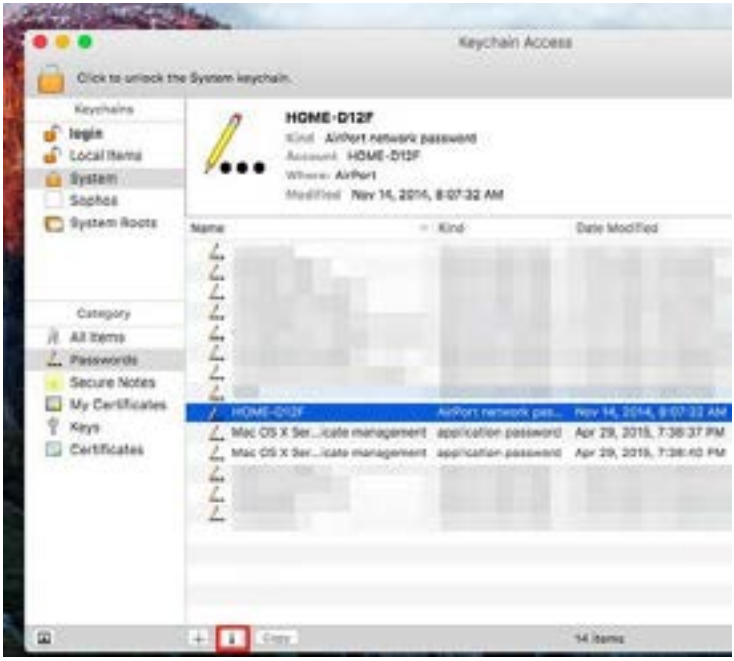
ters را تیک بزنید تا رمز عبور نمایان شود.

پیدا کردن رمزعبور روی مک

اگر یک کامپیوتر مک دارید که در حال حاضر به شبکه وای‌فای مورد نظر متصل است و یا قبلا به آن متصل بوده باز هم می‌توانید به رمز عبور دسترسی پیدا کنید. ویندوز و مک اجازه مشاهده این اطلاعات را می‌دهند اما دستگاه‌های سیار مثل تلفن‌های هوشمند آندرویدی و آی‌فون و آی‌پد امکان مشاهده رمز شبکه وای‌فای را در اختیارتان نمی‌گذارند. برای یافتن رمزعبور بر روی مک، کلیدهای Command+Space را برای باز شدن کادر جستجوی Spotlight بفشارید. عبارت Keychain Access را تایپ کنید و Enter بزنید تا اپ Keychain Access اجرا شود.



نـام شـبکه وای‌فـای را از لیسـت پیـدا و بـر روی آن کلیـک کنیـد. حـالا بـر روی دکمـه "اطلاعـات" (دکمـه‌ای کـه بـا حـرف i مشـخص شـده اسـت) در پاییـن پنجـره کلیـک کنیـد.



در پنجره جدید بر روی کادر Show Password نمایش رمز عبور کلیک کنید. به خاطر داشته باشید که برای مشاهده رمز باید حساب کاربری‌تان دسترسی administrator (مدیر سیستم) داشته باشد. بعد از وارد کردن نام کاربری و رمز عبور حساب کاربری‌تان در مک، رمز وای‌فای نمایش داده می‌شود.

پیدا کردن رمز عبور در رابط کاربری تحت وب روتر

اگر نام کاربری و رمز روتر را می‌دانید، می‌توانید از طریق رابط کاربری وب روتر به رمز وای‌فای دسترسی پیدا کنید. اول وارد تنظیمات روتر شوید. برای این کار باید در نوار آدرس یک مرورگرِ وب عبارت "۱۹۱,۱۶۸,۱,۱" را تایپ کرده و پس از زدن دکمه Enter، در کادری که باز می‌شود نام کاربری و رمز روتر را وارد کنید. حالا در تنظیمات روتر به دنبال "Wi-Fi" یا چیزی مشابه آن بگردید. در پنجره مربوطه قادرید رمز وای‌فای را مشاهده کنید و همچنین

می‌توانید آن را به رمز دلخواه تغییر دهید.

ریست یا بازگرداندن روتر به رمز پیش فرض وای‌فای

اگر نتوانستید رمز را پیدا کنید و به رابط کاربری روتر نیز دسترسی ندارید می‌توانید روتر را ریست کرده و به تنظیمات

کارخانه بازگردانید تا رمز به حالت پیش فرضی که بر روی بدنه روتر ثبت شده باز گردد. برای انجام این کار باید در پشت روتر به دنبال یک حفره کوچک با عنوان reset بگردید و این دکمه را توسط یک سنجاق فشار داده و حدود ده ثانیه نگه دارید. توجه داشته باشید که با انجام این کار تمام تنظیمات روتر به طور کامل پاک شده و به حالت پیش فرض باز می‌گردد.

شبکه وای‌فای خودتان را هک کنید!

همیشه هم هک کردن شبکه‌های بی‌سیم غیرقانونی و غیراخلاقی نیست. شاید شما کلمه عبور شبکه شخصی خود را فراموش کرده باشید و نیاز به راهکاری دارید تا آن را بازیابی کنید. شاید می‌خواهید میزان امنیت شبکه خود را آزمایش کنید تا مطمئن شوید خرابکاران به این راحتی نمی‌توانند به شبکه شما نفوذ کنند. هر دلیلی که داشته باشید، چند روش وجود دارد که با استفاده از آن می‌توانید به یک شبکه وای‌فای نفوذ کنید. در ادامه سعی داریم چند نمونه از آن را به شما نشان دهیم. لطفا سعی نکنید از مهارت‌هایی که به آن دسترسی پیدا می‌کنید برای مقاصد نامشروع استفاده کنید.

Sneakernet

گاهی اوقات آسانترین راه برای نفوذ به یک ساختمان وارد شدن از در ورودی آن است. به این روش از حملات Sneakernet گفته می‌شود، زیرا به جای اینکه خودتان مستقیما روی یک شبکه کار کنید، اصطلاحا از کفش کتانی خود برای حرکت به مقصد استفاده می‌کنید.

اگر واقعا وسوسه شده‌اید که به یک شبکه وارد شوید و کسی هم دور و اطرافتان نیست که کار شما را زیر نظر داشته باشد، به راحتی می‌توانید لپتاپ خود را به پورت اترنت روتر مورد نظر متصل کنید. با این کار نه تنها به سرعت و بدون نیاز به کلمه عبور به این شبکه متصل خواهید شد، بلکه می‌توانید به تنظیمات روتر هم دسترسی پیدا کنید، چرا که معمولا خیلی از افراد از نام کاربری و کلمه عبور پیش‌فرض روتر استفاده می‌کنند. از این طریق می‌توانید کلمه عبور را مشاهده یا آن را تغییر دهید، اتصالات را مدیریت کنید و حتی مک آدرس دستگاه خود را به فهرست مجاز اضافه کنید تا بتوانید از این به بعد بدون دردسر به این شبکه متصل شوید.

خیلی از روترهای پیشرفته امروزی اغلب به قابلیتی به نام نصب محافظت شده وای‌فای یا به اختصار WPS مجهز هستند. اگر این قابلیت فعال باشد به شما اجازه خواهد داد به راحتی دستگاه خود را برای اتصال از طریق WPS آماده کرده و بعد با فشردن دکمه دسترسی روی روتر و نگه داشتن آن تا زمان شناسایی دستگاه،

اتصال را برقرار کرده و به شبکه بی‌سیم دسترسی داشته باشید. از اینجا به بعد، شما دیگر نیاز به وارد کردن کلمه عبور برای دسترسی به شبکه نخواهید داشت و خود روتر به طور خودکار کامپیوتر یا دستگاه شما را شناسایی خواهد کرد.

خرابکاری را شروع کنید

در اکثر موارد، شما نمی‌توانید با خیال راحت چند دقیقه با لپتاپ خود کنار روتر بنشینید و با آن خلوت کنید. اما همچنان گزینه‌های دیگری روی میز هست. اگر فقط نیاز به دسترسی به اینترنت دارید و برای شما مهم نیست که این دسترسی از طریق چه شبکه‌ای انجام می‌شود، می‌توانید از روشی به نام wardriving استفاده کنید و به راحتی یا سواره و یا پیاده به دنبال شبکه‌های بی‌سیم محافظت نشده در محیط پیرامون خود بگردید.

اگر چندان به نتیجه دادن این کار امیدوار نیستید، خبر خوب این است که خیلی از مردم همچنان از شیوه امنیتی WEP برای حفاظت از شبکه استفاده می‌کنند، و به راحتی می‌توان به این روش حفاظتی نفوذ کرد. نکته منفی در استفاده از این روش این است که ابزاری که برای اینگونه نفوذها مورد استفاده قرار می‌گیرد خودشان می‌توانند برای سیستم شما دردسرساز شوند، چرا که احتمالا شما مجبور هستید این ابزار را از منابع نامعتبر دانلود کنید.

یک روش برای جلوگیری از این مشکل استفاده از یک توزیع سبک و جمع و جور لینوکس است. PHLAK برای آزمایش پایداری یک شبکه طراحی شده است. شما به راحتی می‌توانید این توزیع از لینوکس را از روی CD یا درایو USB اجرا کنید. جلوگیری از دسترسی به هارد درایو شما این امکان را به وجود می‌آورد که شما از یک نرم‌افزار بدون بر جا گذاشتن هیچ‌گونه اثری روی سیستم خود استفاده کنید. با این روش از اطلاعات شخصی خود نیز محافظت خواهید کرد.

بعد از اینکه PHLAK را روی CD یا درایو USB قرار دادید، تنها کافی است کامپیوتر خود را از نو بارگذاری کنید تا به یک سیستم‌عامل موقتی بوت شود. شما بعد از ورود به این سیستم‌عامل تعدادی ابزار و اسکریپت را مشاهده خواهید کرد که به شما کمک می‌کنند تا میزان امنیت شبکه خود را آزمایش کنید.

درها را باز کنید

اگر هیچ‌کدام از روش‌های گفته شده برای نفوذ به یک شبکه بی‌سیم برای شما کارساز نیست، همیشه می‌توانید از روشی که هکرها نام آن را brute force گذاشته‌اند، استفاده کنید. این شیوه مثل زمانی است که دوست شما از شما می‌خواهد عددی را که او به آن فکر می‌کند را حدس بزنید و شما به ترتیب شروع می‌کنید از ۱، بعد ۲ و بعد ۳ و همینطور به حدس زدن ادامه می‌دهید تا

بالاخره عدد درست را پیدا کنید.

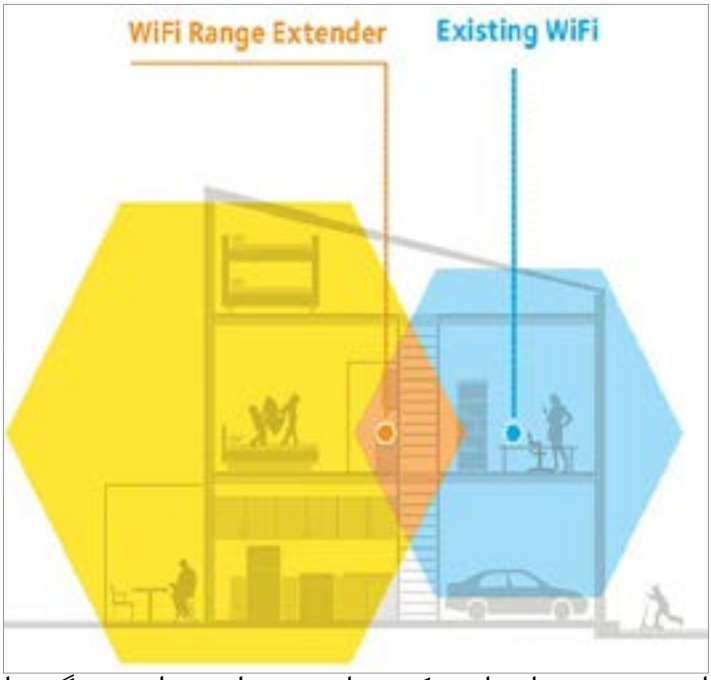
اشکالاتی نیز در این روش برای هک یک شبکه وجود دارد. اشکال اول این است که این کار نیاز به مقدار زیادی توان پردازشی و صرف زمان بسیار زیاد دارد. کامپیوتر شما باید بین کلمات و عبارات موجود در یک دایره لغت عبور کرده و هر یک از ترکیبات احتمالی را امتحان کند تا به نتیجه درست برسد.

هر چه ساختار کلمه عبور پیچیده‌تر باشد، زمان و توان پردازش جستجو در ترکیبات احتمالی بیشتر بوده و رسیدن به نتیجه دشوارتر می‌شود. از آنجا که استفاده از حروف به تنهایی برای انتخاب کلمه عبور بیشتر رایج است، رسیدن به نتیجه را برای هکرها راحت‌تر می‌کند زیرا تعداد کاراکترهای احتمالی کمتر می‌شوند. استفاده از یک کلمه عبور پیچیده که از ترکیبی از حروف و اعداد و کاراکترهای علامتگذاری تشکیل شده باشد می‌تواند تقریبا روش استفاده از brute force را غیرممکن کند.

همچنین لازم است به این نکته توجه داشته باشید که این روش از حمله به راحتی قابل شناسایی است. اغلب روترهای پیشرفته وقتی تعداد زیادی کلمه عبور اشتباه از یک منبع خاص را دریافت می‌کنند، به طور خودکار جلوی ورود این اطلاعات را برای مدت طولانی سد می‌کنند. اگر قصد نفوذ به یک دفتر کار یا شبکه حرفه ای در کار باشد، این احتمال نیز وجود دارد که مدیر شبکه نیز از این حمله احتمالی مطلع شود.

روتر قدیمی خود را دور نیاندازید!

چگونه با روتر دوم شبکه وای‌فای قوی‌تری بسازیم؟



روترهای بی‌سیم تا زمانی که خانه شما چندان بزرگ نباشد به خوبی وظیفه خود را انجام می‌دهد، اما اگر خانه شما بزرگ باشد شعاع تحت پوشش امواج بی‌سیم روترها نمی‌تواند اینترنت را به تمام نقاط خانه برساند و ممکن است افرادی که با فاصله زیاد از روتر به شبکه متصل هستند ارتباط آنها دائما قطع و وصل شود. شما با استفاده از یک روتر دوم به عنوان افزایش‌دهنده برد سیگنال می‌توانید شعاع تحت پوشش شبکه خود را به دو برابر افزایش د هید .

مراحل اصلی انجام کار

ابتـدا روتـری را کـه می‌خواهیـد از آن بـه عنـوان افزایشـدهنده قـدرت سـیگنال اسـتفاده کنیـد بـه وسـیله یـک کابـل اترنـت Cat5 بـه یکـی از پورت‌هـای LAN روتـر و طـرف دیگـر آن را بـه پـورت اترنـت موجود در کنـار لپ‌تـاپ خـود متصـل کنیـد. سـپس یـک سـنجاق قفلـی یـا گیـره کاغـذ را بـه داخـل حفـره reset روتـر وارد کنیـد. معمـولاً حفـره reset

Router Brand	Common Default IP Addresses
2Wire	192.168.1.1 192.168.0.1 192.168.1.254 10.0.0.138
3Com	192.168.1.1 192.168.1.10.1
Actiontec	192.168.1.1 192.168.0.1 192.168.2.1 192.168.254.254
Airlink	192.168.1.1 192.168.2.1
Airlive	192.168.2.1
Airties	192.168.2.1
Apple	10.0.1.1
Amped Wireless	192.168.3.1
Asus	192.168.1.1 192.168.2.1 10.10.1.1

در پشـت روتـر و در کنـار محـل اتصـال آداپتـور برق قـرار دارد. ریسـت کـردن روتـر تنظیمـات آن را بـه حالـت کارخانـه‌ای بـاز می‌گردانـد و این کار باعـث می‌شـود شـما بتوانیـد بـه آسـانی بـه رابـط گرافیکـی روتـر دسترسـی داشـته باشـید و تنظیمـات آن را از ابتـدا انجـام دهیـد.

برای دسترسی به رابط گرافیکی روتر آدرس آی‌پی پیشفرض آن را در نوار آدرس مرورگر خود وارد کنید. اگر شما آدرس آی‌پی پیشفرض را نمی‌دانید، به سایت TechSpot.com مراجعه کرده و از فهرست موجود آدرس‌های رایج مربوط به روترها را مشاهده کنید.

برای مثال اگر شما از یک روتر دی لینک استفاده می‌کنید، آی‌پی ۱۹۲,۱۶۸,۱,۱ را در نوار آدرس وارد کرده و بعد کلید اینتر را فشار دهید تا به صفحه ورود تنظیمات روتر خود وارد شوید.

شما برای وارد شدن به صفحه اصلی تنظیمات روتر باید اطلاعات پیش فرض ورود را نیز وارد کنید.

اگر اطلاعات پیش فرض ورود مربوط به روتر خود را نمی‌دانید به سایت RouterPasswords.com مراجعه کرده و نام‌های کاربری و کلمات عبور متداول را مشاهده کنید.

بعد از ورود به صفحه تنظیمات روتر گزینه DHCP server را پیدا کرده و با انتخاب گزینه Disabled آن را غیرفعال کنید. مکان قرارگیری تنظیمات DHCP server در مدل‌های مختلف روتر متفاوت است، اما اغلب تولیدکنندگان معروف این تنظیمات را در صفحه Basic Settings قرار می‌دهند. گزینه SSID (نام شبکه روتر) را پیدا کرده و آن را به نام روتر اصلی شبکه خود تغییر دهید. از آنجا که SSID تنها روی کامپیوترهایی که به صورت بی‌سیم به شبکه متصل می‌شوند تاثیر گذار است، معمولاً تنظیماتSSID در صفحه Wireless Setup رابط کاربری قرار دارد.

بخش گذرواژه مربوط به امنیت روتر را پیدا کرده و آن را به گذرواژه روتر اصلی خود تغییر دهید. به‌روزرسانی SSID و گذرواژه به کامپیوترها اجازه می‌دهد بدون مشکل از روتر اصلی به گسترش دهنده متصل شوند. در نهایت روی گزینه Save Settings کلیک کنید تا تنظیمات روتر شما به‌روزرسانی شود.

حالا کابل اترنت را از روتر و کامپیوتر جدا کنید. سپس یک سر کابل اترنت را به پورت LAN روتر اصلی و سر دیگر کابل اترنت را به پورت WAN روتر گسترش‌دهنده سیگنال متصل کنید. گسترش‌دهنده سیگنال را با فاصله تقریبی ۱۰ متری نسبت به روتر اصلی قرار دهید تا اطمینان حاصل کنید که امواج شبکه به تمام نقاط خانه شما ارسال می‌شود.

نکاتی که باید در نظر داشته باشید

معمولاً متداول است که کاربران از یک برند روتر یا حتی از یک مدل مشابه استفاده می‌کنند. سازندگانی مثل لینک‌سیس، ایسوس و دی لینک معمولاً از یک آدرس آی‌پی یکسان برای تمام روترهای خود استفاده می‌کنند. اگر شما روترهای خود را با یک آی‌پی یکسان تنظیم کرده‌اید، باید به طور دستی آدرس آی‌پی روتری که به عنوان گسترش‌دهنده سیگنال از آن استفاده می‌کنید، را تغییر دهید. برای انجام این کار به رابط گرافیکی صفحه تنظیمات وارد شده و گزینه Local IP address را پیدا کنید، سپس آخرین عدد آن را به یک شماره دیگر تغییر دهید. به خاطر داشته باشید که شما نمی‌توانید از دو آدرس آی‌پی یکسان در یک شبکه استفاده کنید.

با دقت از دارایی خود محافظت کنید!

چگونه بفهمیم یکی از همسایه‌ها به وای‌فای ما وصل شده است

آیا سرعت اینترنت شما کم شده است؟ آیا در زمان پخش ویدیو سرعت بافر شدن به کندی صورت می‌گیرند؟ آیا برای دانلود کردن یک فایل کوچک هم به مدت زمان زیادی نیاز دارید؟ اگر این‌گونه است ممکن است خبرهای بدی در انتظار شما باشد. احتمالاً یکی از همسایگان شما بدون اطلاع در حال استفاده از شبکه وای‌فای شما است.

اجازه دادن به دستگاه‌های غیر مجاز برای استفاده از اینترنت شما ایده خوبی نیست، به ویژه این که انجام چنین کاری علاوه بر

کاهش سرعت اتصال شما و بار مالی ناشی از مصرف پهنای باند اینترنت، وضعیت امنیتی شبکه شما را نیز به مخاطره می‌اندازد.

خطرات پیش‌رو

بزرگترین خسارتی که به یک شبکه وای‌فای سرقت شده وارد می‌شود، کند شدن سرعت اتصال به آن است. هر شبکه کامپیوتری میزان مشخص و محدودی از پهنای باند را در اختیار دارد و با تقسیم آن بین چند کامپیوتر، یک تلویزیون هوشمند و چند تلفن همراه شما به مرور متوجه خواهید شد که سرعت اتصال دستگاه‌ها به شبکه در حال کم شدن است، به ویژه اگر پهنای باند مصرفی یکی از این دستگاه‌ها زیاد بوده و مثلا در حال پخش یک ویدئو از اینترنت باشد. همچنین این روزها خیلی از خدمات دهندگان اینترنت هزینه مصرف اینترنت را بر اساس میزان پهنای باند مصرفی محاسبه می‌کنند و دیگر خبری از اینترنت نامحدود نیست. با این اوصاف اگر یکی از همسایگان شما بدون اطلاع و اجازه شما از این پهنای باند استفاده کند شما در انتهای ماه مجبور به پرداخت یک هزینه سرسام آور برای استفاده از اینترنت هستید. علاوه بر مشکل کند شدن اتصال به شبکه، یک روتر بی‌سیم غیر امن نیز می‌تواند مشکلات امنیتی بزرگی را برای شما فراهم کند. هر چند ممکن است همسایه شما تنها بخواهد از اینترنت شما برای چک کردن رایگان ای‌میل‌هایش استفاده کند، اما یک روتر

ناامـن می‌توانـد بـرای دسترسـی بـه اطلاعاتـی کـه شـما بـا وب‌سـایت هـا در میـان می‌گذاریـد (مثـلا اطلاعـات حسـاب بانکی شـما)، دسترسـی بـه سـایر دسـتگاه‌های متصـل بـه ایـن شـبکه یـا آلـوده کـردن کامپیوتـر شـما بـه ویـروس مـورد اسـتفاده قـرار بگیـرد. ایـن همسـایگان مزاحـم همچنیـن می‌تواننـد از اتصـال اینترنـت شـما بـرای مقاصـد و فعالیت‌هـای غیرقانونـی خـود اسـتفاده کننـد. تصـور کنیـد اگـر چنیـن اتفاقـی بیفتد چه کسـی مسـئول عواقـب ناشـی از اسـتفاده غیرقانونـی از اینترنـت خواهـد بـود؟ مسـلما خـود شـما.

چگونه تشخیص دهیم که آیا کسی در حال سرقت از شبکه وای‌فای ما است

اگـر شـما بـه ایـن موضـوع مشـکوک شـده‌اید کـه ممکـن اسـت کسـی در حـال سـرقت از شـبکه وای‌فـای شـما باشـد، لازم اسـت ابتـدا بـه

صفحه مدیریت روتر خود وارد شوید. متداول‌ترین روش برای انجام این کار در خیلی از برندهای روتر، تایپ کردن آدرس آی‌پی ۱۹۲,۱۶۸,۱,۱ و یا ۱۹۲,۱۶۸,۲,۱ در نوار آدرس مرورگر شما است. اگر این دو آدرس کار نکرد، برای بدست آوردن آن به دفترچه راهنمای روتر خود مراجعه کنید.

بعد از این که به صفحه مدیریت روتر خود دسترسی پیدا کردید، باید به صفحه‌ای که در آن فهرستی از MAC آدرس‌هایی که به روتر شما متصل شده‌اند وجود دارد مراجعه کنید. محل قرارگیری این صفحه با توجه به مدل روتر شما ممکن است متفاوت باشد، اما اغلب اوقات این صفحه در زیر مجموعه‌ای از بخش‌های wire-less configuration، wireless status یا DHCP client قرار دارد. شما با بررسی دقیق این فهرست می‌توانید متوجه شوید چه تعداد دستگاه به شبکه شما متصل شده است. برای مثال اگر شش آدرس MAC در این فهرست وجود دارد (توجه داشته باشید که هر دستگاهی که به یک شبکه متصل می‌شود آدرس MAC اختصاصی خود را دارد) اما شما تنها ۴ دستگاه در خانه دارید احتمالاً یک مزاحم مشغول استفاده از اینترنت شما است.

نکته: هر دستگاهی اعم از تلفن‌های هوشمند قدیمی، کنسول‌های بازی، دوربین‌های دارای قابلیت وای‌فای و هر دستگاه دیگری که قابلیت اتصال به شبکه بی‌سیم را داشته باشد ممکن است در فهرست آدرس MAC قرار داشته باشد. به همین دلیل ممکن است

شما در تشخیص دستگاه‌هایی که به شبکه متصل هستند دچار سردرگمی شوید. برای مدیریت بهتر آدرس‌های MAC و این که کدام آدرس مربوط به کدام دستگاه است می‌توانید از وب سایت macvendors.com استفاده کنید.

چطور جلوی سارق اینترنت را بگیریم؟

اگر به این نتیجه رسیدید که کسی مشغول سرقت از وای‌فای شما است، بهترین کار این است که تدابیر امنیتی را افزایش دهید. اگر شبکه شما بدون کلمه عبور کار می‌کند، هر چه سریع‌تر آن را فعال کنید. اگر شما همچنان از نام و کلمه عبور پیش‌فرض روتر استفاده می‌کنید، آن را تغییر دهید. برای انجام این کار به صفحه مدیریت روتر خود مراجعه کنید. برای تغییر کلمه عبور در بخش تنظیمات امنیتی روتر به دنبال عبارت PSK یا Pre Shared Key بگردید. تغییر دادن کلمه عبور شبکه وای‌فای باعث می‌شود تا ارتباط تمام دستگاه‌هایی که قبلا به آن متصل بودند قطع شود، بنابراین شما باید بعد از تعیین یک کلمه عبور جدید یک بار دیگر دستگاه‌های خود را به شبکه معرفی کنید.

برای تغییر نام روتر عبارت Service Set identifier م(SSID) را پیدا کنید. معمولا این گزینه در بخش تنظیمات بی‌سیم روتر قرار دارد. در پایان انتخاب یک سیستم کدگذاری قدرتمند برای شبکه بی‌سیم ضروری خواهد بود. معمولاً بهترین انتخاب در روترهای

رایـج اسـتفاده از اسـتاندارد WPA2 اسـت.اگر تاریـخ تولیـد روتـر شـما بـه قبـل از سـال ۲۰۰۶ بـاز می‌گـردد، احتمـالا بـا سیسـتم کدگـذاری WPA2 سـازگار نخواهـد بـود. در ایـن شـرایط بهتـر اسـت بـه فکـر خرید یـک روتـر جدیـد باشـید.

هکرها را ناکام بگذارید

۱۲ کاری که باید برای بهبود امنیت روتر بی‌سیم خانگی انجام دهید

با اخباری که این روزها از میزان آسیب‌پذیری روترها به گوش می‌رسد، بد نیست که با رعایت یک سری از نکات سطح امنیت روتر خود را بالا ببریم. شما می‌توانید با رعایت چند نکته نسبتا ساده خود را از دسترس هکرها پنهان کنید.

نکات ارائه شده در این مقاله به ترتیب از اصول ابتدایی تا سطوح فنی‌تر طبقه‌بندی شده‌اند:

۱. این مرحله ممکن است برای خیلی‌ها ابتدایی و بی اهمیت به نظر برسد، اما اکثر روترها برای ورود به بخش تنظیمات خود از نام‌های کاربری پیش فرض یکسان مثل admin و برای کلمه

عبور خود از کلمات ساده پیش فرضی مثل password استفاده می‌کنند. اولین کاری که شما باید بعد از راه اندازی روتر انجام دهید تغییر نام کاربری و استفاده از یک کلمه عبور پیچیده است. لطفا توجه داشته باشید که این کار متفاوت از تغییر نام و پسورد وای‌فای شما است.

۲. بعد از اینکه اطلاعات لاگین به تنظیمات روتر را تغییر دادید، حالا نوبت انتخاب یک نام و کلمه عبور مناسب برای اتصال به روتر است. توصیه می‌شود این اطلاعات را نیز از حالت پیش فرض خارج و آن را به چیزی که بیانگر اطلاعات شخصی نباشد تغییر دهید. در حالت ایده‌ال بهتر است نام سازنده روتر مثل Netgear یا Linksys یا اطلاعات شخصی را به عنوان نام وای‌فای انتخاب نکنید. برای افزایش این سطح از امنیت پیشنهاد می‌شود روش کدگذاری تبادل اطلاعات را به جای WPA یا WEP به WPA2 تغییر دهید. در این مرحله انتخاب یک گذر واژه (passphrase) طولانی از اهمیت زیادی برخوردار است و پیشنهاد می‌شود تعداد کاراکترهای انتخابی بیشتر از ۲۰ حرف باشد.

۳. در ادامه افزایش سطح امنیت مطرح شده در مرحله قبل، شما می‌توانید به طور کامل از انتشار SSID جلوگیری کنید، بنابراین تنها کاربرانی که از نام شبکه شما مطلع هستند می‌توانند به آن متصل شو ند .

۴. اگر قصد دارید برای کاربران مهمان خود نیز اجازه دسترسی

به شبکه را صادر کنید، یک شبکه Guest کاملا مستقل و جداگانه ایجاد کنید. هرگز توصیه نمی‌شود که اطلاعات اتصال اصلی خود را در اختیار همه بگذارید.

۵. متاسفانه تنبلی همیشه باعث به خطر افتادن سطح امنیت ما می‌شود. اگر چه ممکن است استفاده از دکمه WPS و Wi-fi Pro-tected Setup کار را تا اندازه زیادی راحت کند، اما بنا به دلایل امنیتی معمولا توصیه نمی‌شود که از این قابلیت استفاده کنید. این امکان ممکن است به یک حمله کننده اجازه دهد با آزمایش PIN های مختلف که به حمله brute-forced معروف است سعی کند به شبکه شما متصل شود.

۶. همیشه اطمینان حاصل کنید که فایروال روتر شما به‌روز باشد. توصیه می‌شود که هر چند مدت یک بار به تنظیمات روتر وارد شده و به‌روزرسانی‌های لازم را انجام دهید. این وظیفه‌ای است که خیلی از اوقات نادیده گرفته می‌شود و نباید این گونه باشد.

۷. قابلیت دسترسی مدیریتی از دور یا Remote Administrative Ac-cess را در روتر خود غیرفعال کنید و دسترسی در سطح مدیریت از طریق وای‌فای را نیز غیرفعال کنید. با این کار کاربر Admin تنها می‌تواند از طریق کابل اترنت به روتر متصل شود.

۸. مرحله بعدی که معمولا برای افزایش سطح امنیت توصیه می‌شود تغییر رنج IP پیش فرض روتر است. تقریبا تمام روترها از IP مشابه ۱۹۲,۱۶۸,۱,۱ استفاده می‌کنند و تغییر آن می‌تواند از

حمـلات CSRF وCross-Site Request Forgery جلوگیـری کنـد.

۹.بـه وسـیله آدرس MAC از دسترسـی بـه روتـر جلوگیـری کنیـد. شـما می‌توانیـد مشـخص کنیـد کـه دقیقـا کـدام دسـتگاه‌ها اجـازه دسترسـی بـه شـبکه را دارنـد. بـرای انجـام ایـن کار بایـد وارد بخـش وای‌فـای تنظیمـات روتـر خـود شـده و آدرس MAC دسـتگاه‌های مـورد نظـر خـود را وارد کنیـد.

۱۰. اگـر دسـتگاه‌هایی کـه از آنهـا اسـتفاده می‌کنیـد بـا ایـن فنـاوری سـازگار اسـت، معمـولا پیشـنهاد می‌شـود بانـد اسـتاندارد ۲,۴ گیگاهرتـز را بـه بانـد ۵ گیگاهرتـز تغییـر دهید. ایـن کار برد سـیگنال را کاهـش داده و امـکان دسترسـی حمـلات از راه دور را بـه روتـر شـما محـدود می‌کنـد.

۱۱. در صـورت امـکان قابلیت‌هـای Telnet, PING, UPNP, SSH و HNAP را غیرفعـال کنیـد. شـما می‌توانیـد تمـام آنهـا را یک جـا غیرفعال کنیـد، امـا معمـولا توصیـه می‌شـود آنهـا را در وضعیتـی بـه نـام Stealth قـرار دهیـد. ایـن کار باعـث می‌شـود تـا از پاسـخگویی روتـر شـما بـه ارتباطـات خارجـی جلوگیـری شـود.

۱۲. بعـد از اینکـه ایـن مراحـل را انجـام دادیـد، مطمئـن شـوید کـه از تنظیمـات روتـر لاگ اوت کـرده باشـید. انجـام ایـن کار تنهـا مختـص بـه روتـر نیسـت. شـما بایـد بعـد از اتمـام کار بـا وب‌سـایت‌ها، برنامه‌هـا یـا کنسـول‌ها از آنهـا نیـز لاگ اوت کنیـد.

در نهایـت توصیـه می‌شـود کـه تمـام مراحـل گفتـه شـده در بـالا را انجـام دهیـد، امـا اگـر قـادر بـه انجـام همـه آنهـا نیسـتید تـا هـر کجـا

که ممکن است این موارد را رعایت کنید. از قدیم گفته‌اند «کار از محکم کاری عیب نمی‌کند.»

بهتر است سبک زندگی دیجیتالی خود را تغییر دهید!

چرا باید وای‌فای را آخر شب خاموش کنیم؟

مودم‌ها و روترها طوری ساخته شده‌اند که برای همیشه و مدت زمان طولانی روشن باشند اما تا کنون با خود فکر کردید آخر شب و هنگامی که دیگر نیازی به اینترنت یا وای‌فای ندارید؛ چرا باید این دستگاه‌ها روشن باشند و چه خطراتی را متوجه شما می‌کنند؟

شاید اولین دلیلی که به ذهن برسد؛ خطرات امواج رادیویی و وای‌فای برای سلامتی بدن باشد اما دلایل قانع‌کننده دیگری هم هست که شاید هیچ‌گاه به‌شان فکر نکردید و برایتان اهمیت نداشتند. در ادامه می‌خواهم به ۵ دلیل اصلی اشاره کنم که نشان

می‌دهند بهتر است در مواقعی که نیازی به وای‌فای ندارید یا اینکه آخرشب مودم یا روتر را خاموش کنید.

۱- امواج رادیویی برای انسان به‌خصوص کودکان خطرناک هستند

درست است که هنوز این موضوع به طور کامل و علمی ثابت نشده است اما تقریبا تمام کارشناسان محیط‌زیست و پزشکی موافق این موضوع هستند که امواج مایکروویو تاثیراتی روی بدن و ذهن انسان می‌گذارند. هر ساله تحقیقات زیادی صورت می‌گیرد که نتایج‌شان نشان می‌دهد افرادی که کمتر در معرض امواج رادیویی حتا موبایل و نوت‌بوک و تلویزیون هستند؛ سلامت جسمی و روانی بهتر دارند. این موضوع به‌خصوص برای نوزادان و کودکان تشدید می‌شود؛ چون ساختار بدنی و مغزی آن‌ها آسیب‌پذیرتر است و دارد تکامل پیدا می‌کند.

شاید سوال کنید پس بهتر است از موبایل هم استفاده نکنیم؟ جواب این است که بله؛ گوشی‌های تلفن همراه را هم بهتر است در آخر شب و مواقعی که نیاز ندارید توی بغل خودتان نگذارید و کمی دور نگه‌دارید. در این مورد تحقیقات زیادی صورت گرفته و ثابت شده افرادی که در آخر شب مدت زمان نسبتا طولانی با گوشی‌های موبایل کار می‌کنند؛ مشکلات بی‌خوابی بیشتری دارند.

۲- نزدیک بودن به امواج رادیویی بی‌خوابی می‌آورد

کارشناسان توصیه می‌کنند بهتر است در اتاقی بخوابید که هیچ‌گونه دستگاه بی‌سیم یا وای‌فای وجود نداشته باشد. به معنی دیگر، بهتر است روتر یا مودم در اتاق خواب نباشد. خطرات امواج رادیویی و وای‌فای در فاصله نزدیک زیر ۵ متر و ۱۰ متر بسیار بیشتر است و در فاصله‌های بالاتر از ۵۰ متر کم می‌شود. بهتر است با یک روتر روشن ۱۰۰ متر فاصله داشته باشید. در خانه‌های آپارتمانی جدید که بسیار کوچک هستند؛ معمولا فاصله ۱۰۰ متری غیرممکن است؛ پس بهتر است که روتر را خاموش کنید. اگر دوست دارید با خیال آسوده بخوابید، بهتر است مودم یا روتر را خاموش کنید تا به این صورت ذهن شما هم خاموش شود و کم‌کم برای رفتن به ضمیر ناخودآگاه آماده شوید. ذهن انسان در شب و هنگام خواب فرآیندها و واکنش‌های بیولوژیکی دارد که امواج وای‌فای مزاحم‌اش هستند.

۳- مصرف انرژی در دنیایی که مشکل کمبود انرژی دارد

مودم و روتر مودهایی برای کاهش مصرف انرژی دارند و در مواقعی که هیچ دستگاهی بدان‌ها وصل نباشد، به طور محسوسی مصرف انرژی را کاهش می‌دهند اما باز چندین چراغ LED روشن است و دستگاه دارد برق مصرف می‌کند. چرا باید این‌طور باشد؟ هم هزینه‌های قبض برق شما افزایش پیدا می‌کند و هم به یک

دشمن محیط‌زیست و انرژی تبدیل می‌شوید. روشن بودن مودم و روتر هیچ فایده‌ای برای شما جز افزایش هزینه ندارد.

۴- احتمال خرابی دستگاه افزایش پیدا می‌کند

اجازه بدهید یک راز درباره مودم‌ها و روترها برایتان فاش کنم. این دستگاه‌ها طوری ساخته شده‌اند که تا دو الی سه سال به طور همیشه روشن باشند و کار کنند اما بعد از این مدت استاندارد که معمولا در دفترچه راهنما و مستندات دستگاه از طرف کارخانه اعلام می‌شود، مادربورد، خازن‌ها و چیپ‌ست‌ها شروع به اصطهلاک و فرسایش می‌کنند و عمر مفید خود را از دست می‌دهند. بنابراین، هرچه بیشتر روشن باشند، زودتر خراب می‌شوند و احتمال از کار افتاده‌گی یا سوخته‌گی بالاتر می‌رود. همین‌طور ممکن است روی کیفیت و کارایی دستگاه تاثیر بگذارد و وای‌فای با سرعت پایین‌تری داشته باشید. اگر یک دستگاه روتر با قدمت بالا دارید، بهتر است مانند انسان‌های سن بالا کمی به او استراحت بدهید تا بیشتر عمر کند.

۵- هکرها و دزدان وای‌فای شب‌ها بیدارند

دوستی برایم تعریف می‌کرد روتر بی‌سیم خود را شب‌ها خاموش نکرده و روشن می‌گذاشت. یک مدتی به مصرف اینترنت شک می‌کند و با نصب چند ابزار مشاهده ترافیک و تحلیل وای‌فای،

سعی می‌کند بفهمد چرا این قدر زود به زود حجم اینترنت‌اش تمام می‌شود. با این ابزارها می‌فهمد که هر شب نزدیک به یک گیگابایت اینترنت مصرف می‌شود. ندانسته پیش خودش تصور می‌کند موبایل یا تلویزیون به‌روزرسانی می‌شوند. چند شبی مسافرت می‌رود و برمی‌گردد می‌بیند باز هم هر شب اینترنت مصرف شده است. خلاصه با کلی کارآگاه‌بازی متوجه می‌شود یکی از همسایه‌های بلوک کناری شب‌بیداری دارد و از اینترنت او استفاده می‌کند. هکرها هم از سکوت و خلوت شب‌ها برای حمله به دستگاه‌ها و سیستم‌ها و هک وای‌فای کاربران استفاده می‌کنند. خاموش کردن دستگاه روتر در آخر شب یا مواقعی که برای چند روز خانه نیستید از این جهت هم فوایدی دارد.

باور عمومی اشتباه

یک باور اشتباه وجود دارد که روشن/خاموش کردن زیاد یک روتر باعث خرابی آن می‌شود! اگر این‌طور بود سازنده روتر کلید خاموش/روشن را برای راحتی شما نصب نمی‌کرد. ما هم موافق این نظر هستیم که نباید در یک شبانه‌روز چندین بار روتر را خاموش/روشن کرد ولی وقتی طولانی مدت کاری به اینترنت و وای‌فای ندارید؛ بهتر است با کلید خاموش/روشن این دستگاه‌ها را خاموش کنید یا برق سراسری دستگاه را قطع کنید.

راه‌حل رفع مشکل روترهای وای‌فای از برق کشیدن آنها نیست!

قبل از دور انداختن روتر؛ این ترفندها را برای بهبود وای‌فای امتحان کنید!

معمولا کمتر اتفاق می‌افتد که کسی کاملا از وضعیت شبکه وای‌فای خود رضایت داشته باشد. ممکن است مشکلات متعددی برای شبکه‌های بی‌سیم وای‌فای رخ دهد، اما شایع‌ترین آن نرسیدن سیگنال به برخی از نقاط خانه و یا کم شدن سطح قدرت آن در هنگام فاصله گرفتن از روتر است. با افزایش تعداد دستگاه‌های متصل به یک شبکه نیز علاوه بر حادتر شدن این مشکل، کم شدن پهنای باند و کاهش سرعت اینترنت هم به مشکلات اضافه خواهد شد. یکی از عادات بد استفاده از یک شبکه وای‌فای این

است ما تصور می‌کنیم تا زمانی که مشکلی پیش نیامده نباید کاری به روتر و تنظیمات آن داشته باشیم و اگر بخواهیم کمی صادق باشیم مهمترین راه حلی که در زمان بروز یک مشکل به ذهن اکثر کاربران می‌رسد این است که دستگاه را از برق بکشند، به این امید که شاید با یک بار روشن و خاموش شدن دستگاه مشکل برطرف شود. در ادامه به برخی از نکات پر اهمیتی که ممکن است وضعیت شبکه شما را بهبود بخشد اشاره خواهیم کرد.

روش صحیح استفاده از دستگاه

اولین سوالی که باید به آن پاسخ دهید این است که چند سال از کار مودم یا روتر شما می‌گذرد؟ اگر چند سال است که از آن استفاده می‌کنید و همان مودمی است که شرکت خدمات دهنده اینترنت به شما داده است باید به فکر تهیه یک دستگاه جدید باشید. اما اگر روتر شما هنوز نسبتا جدید است و از لحاظ فنی اصطلاحا هنوز منسوخ نشده است، چند گزینه پیش روی شما است.

یکی از مواردی که می‌تواند به افزایش کیفیت دستگاه شما کمک کند به‌روزرسانی میان افزار (firmware) آن است. روش بعدی تغییر فرکانس یا کانال سیگنال ارسالی از روتر است. یکی از موارد ناخوشایندی که کاربران اصلا تمایلی به درگیر شدن با آن را ندارند استفاده از نرم افزار تنظیمات روتر است، هر چند در خیلی از

موارد آشنایی با این تنظیمات می‌تواند به رفع مشکلات احتمالی کمک کند.

یکی دیگر از روش‌های حل مشکلات به وجود آمده، کمک گرفتن از بخش فنی شرکت خدمات دهنده اینترنت شما است. در برخی موارد مشکلات ناشی از عدم امکان دسترسی به اینترنت ممکن است از طرف خدمات دهنده باشد و یا با مطرح کردن آن متخصصان شرکت آنها بتوانند شما را راهنمایی کنند.

دستگاه در کجا قرار گرفته است؟

بعضی اوقات اندکی جابه‌جایی در موقعیت مکانی روتر می‌تواند افزایش چشمگیری در سطح گیرندگی آن ایجاد کند. خیلی از ما به این دلیل که روترها ظاهر زیبایی ندارند یا باعث شلوغی میز ما می‌شوند آنها را در کشوی میز و یا یک گوشه از خانه پنهان می‌کنیم که باعث افت شدید در قدرت سیگنال رسانی آن می‌شود. از آنجا که این روزها معمولا در همه جای خانه از اینترنت و شبکه استفاده می‌شود؛ بهترین مکان برای قرار دادن روتر در مرکز خانه است تا شعاع تحت پوشش سیگنال تمام محیط خانه را در بر بگیرد. خوشبختانه این روزها روترها ظاهر زیباتری پیدا کرده‌اند و حتی در برخی موارد می‌توان از آنها به عنوان وسایل تزئینی استفاده کرد.

یکی دیگر از مواردی که به افزایش سطح سیگنال‌رسانی روتر

کمک می‌کند قرار دادن آن در ارتفاع است. بنابراین به جای متصل کردن مودم به سیم سیار و قرار دادن آن روی زمین بهتر است آن را مستقیما به دیوار متصل کنید.

از فناوری برای رفع مشکل کمک بگیرید

یک روش سریع و مطمئن برای افزایش محدوده تحت پوشش سیگنال یک شبکه وای‌فای خرید یک دستگاه گسترش دهنده وای‌فای (Wi-Fi extender) یا ساخت یک اکسس پوینت جدید است. وظیفه گسترش دهنده‌ها تقویت و افزایش محیط تحت پوشش امواج بی‌سیم است. هر چند ممکن است در برخی از موارد این افزایش محدوده به قیمت کاهش سرعت ارتباط تمام شود. محدوده قیمت خرید یکی از این دستگاه‌ها بین ۱۲۰ تا ۴۰۰ هزار تومان است و خوشبختانه طریقه استفاده از اغلب آنها بسیار ساده است. یک روش ارزان‌تر برای تقویت محدوده تحت پوشش سیگنال استفاده از یک روتر قدیمی و تنظیم آن به عنوان یک اکسس پوینت برای تقویت سیگنال‌رسانی است.

چند محصول جدید دیگر نیز وجود دارند که می‌توانند به رفع برخی از مشکلات شما کمک کنند. روتر OnHub گوگل محصولی است که در سال ۲۰۱۴ توسط این شرکت ارائه شد و از زمان عرضه تا به حال پیشرفت‌های زیادی داشته است. این دستگاه با طراحی زیبای خود این امکان را فراهم می‌کند که بتوان آن را

بـه جـان پنهـان کـردن زیـر میـز در اتـاق نشـیمن قـرار داد. بـه لطـف فناوری‌هـای پیشـرفته بـه کار گرفتـه شـده در این محصول، سیگنال‌رسـانی توسـط آن نیـز بهتـر انجـام می‌شـود. یکـی از بهتریـن مزایـای اسـتفاده از OnHub داشـتن یـک اپلیکیشـن کارآمـد برای انجـام تنظیمات آن اسـت کـه بـه تشـخیص ایـرادات احتمالـی نیـز کمـک می‌کنـد.

راه‌حل نهایی

اگـر واقعـا از شـبکه وای‌فـای فعلـی خـود بـه سـتوه آمده‌ایـد، سـبک جدیـدی از محصـولات بی‌سـیم بـه بـازار عرضـه شـده اسـت کـه البتـه قیمت‌هـای بالایـی هـم دارنـد امـا نتایـج مثبـت و قابـل قبولـی را به شـما ارائـه می‌کننـد. Eero و Luma سیسـتم‌های جدیـد و یکپارچـه وای‌فـای خانگـی هسـتند کـه ممکـن اسـت بـرای بهرمنـدی از حداکثـر قابلیـت آنهـا مجبـور باشـید چندیـن دسـتگاه دیگـر را خریـداری کنیـد، امـا آنهـا منحصـرا بـه گونـه‌ای طراحـی شـده‌اند تـا محـدوده تحـت پوشـش امواج بی‌سـیم را گسـترش دهنـد، بـه ایـن شـکل کـه شـما به جـای خریـد یک روتـر تـک، چنـد دسـتگاه از آن را خریـداری می‌کنیـد و آنهـا بـه راحتـی

یک دیگر را شناسایی کرده و قدرت سیگنال را تقویت می‌کنند. دستگاه‌های Eero که هر کدام شبیه به یک جعبه کوچک با لبه‌های منحنی هستند در بسته بندی‌های سه تایی و به قیمت ۴۹۹ دلار در ایالات متحده به فروش می‌رسند و شما با چیدن آنها در اطراف خانه یک شبکه منسجم را تشکیل می‌دهید. Luma نیز از شیوه مشابه‌ای استفاده می‌کند و کمی ارزان‌تر است، اما متاسفانه عرضه جهانی هیچ کدام از آنها هنوز شروع نشده است.