۷ گام تا امن کردن شبکه وای فای خود

وای فای توسط ابزارها و برنامه های بسیار زیادی پشتیبانی می شود. از کنسولهای بازی گرفته تا تلفنهای هوشمند. همینطور تقریبا همه سیستم عاملها هم از وای فای پشتیبانی می کنند. سازمان Alliance Fi-Wi بعد از آزمایش و بررسی به ابزارهای وای فای اعتبارنامه وای فای Certified Fi-Wi می دهد. همه دستگاه هایی که این اعتبارنامه را داشته باشند قابلیت اتصال به همدیگر را دارند، فرقی هم نمی کند که چه شرکتی سازنده دستگاه باشد. هر وسیله ای که قابلیت اتصال به وای فای را داشته باشد و اعتبارنامه Certified Fi-Wi را دریافت نموده باشد می تواند به هر اکسس پوینتی که اعتبارنامه وای فای را دریافت کرده وصل شود. دستگاه هایی که اعتبارنامه را دریافت کرده اند با قرار دادن نشان اعتبارنامه بر روی بسته بندی مشخص می شوند.

ادامه مطلب ...

می‌توان گفت امنیت شبکه بی‌سیم(وای-فای) نسبت به شبکه سیمی پایین‌تر است؛ زیرا:

بعضی افراد با نحوه صحیح پیکربندی وای-فای آشنایی ندارند و از الگوریتم های قدیمی، مانند محرمانگی معادل سیمی(WEP) استفاده می‌کنند. الگوریتم امنیتی WEP یکی از ضعیف ترین روش های رمز گذاری است. این نوع رمز گذاری را نسبت به طول رمز و ترافیک شبکه می‌توان در مدت نسبتاً کوتاهی شکست.برخی از نسخه های WPS هم از امنیت خوبی برخوردار نیستند.
در وای-فای شنود نیاز به سخت‌افزار پیچیده‌ای ندارد و از دور امکان پذیر است؛ زیرا سیگنال‌های وای-فای در فضا حرکت می‌کنند.یکی از این روش‌های متداول Sniff است. یکی از معروف‌ترین نرم‌افزارهای تحت ویندوز برای متصل سیم‌بی شبکه به نفوذگر که شد خواهد اجرا زمانی روش این در شنود البته .دارد نام Cain ،شبکه Sniff باشد.
با استفاده از نرم‌افزار و سخت‌افزارهای مسدود کننده (jammer WIFI)، نفوذگر بدون نیاز به رمز عبور توانایی قطع ارتباط وای-فای را دارد.

چگونه شبکه‌ی وای فای خود را امن کنیم؟

گام نخست: جایگزین کردن یک رمز عبور قوی به جای رمز عبور پیش‌فرض

کاربران شبکه اینترنت بی‌سیم معمولا رمز عبور پیش‌فرض روتر را تغییر نمی‌دهند. شرکت‌ها معمولا پایگاه داده‌ای از رمزهای عبور پیش‌فرض دارند که احتمال اینکه هکرها به آن دسترسی داشته باشند زیاد است. این پایگاهها در بازار سیاه خرید و فروش‌های اینترنتی نیز موجود است. درست مثل یک دسته کلید با هزاران کلید متفاوت که ممکن است یکی از آن‌ها بتواند قفل درب شما را باز کند. پس بهتر است در نخستین قدم، رمز عبور روتر خود را تغییر دهید و به جای رمز عبور پیش‌فرض، یک رمز عبور قوی و پیچیده قرار دهید.

گام دوم: تغییر نام شبکه

هر شبکه بی‌سیم دارای یک شناسه یا SSID است که معمولا این نام، نام سازنده روتر به همراه شماره مدل روتر است. اگر هکرها از شرکت اینترنتی شما و شمال مدل روتر آن آشنا باشند، شاید کار برای آن‌ها راحت‌تر باشد. پس بهتر است که این نام را نیز تغییر دهید تا کار را برای هکرها، دشوارتر کنید.

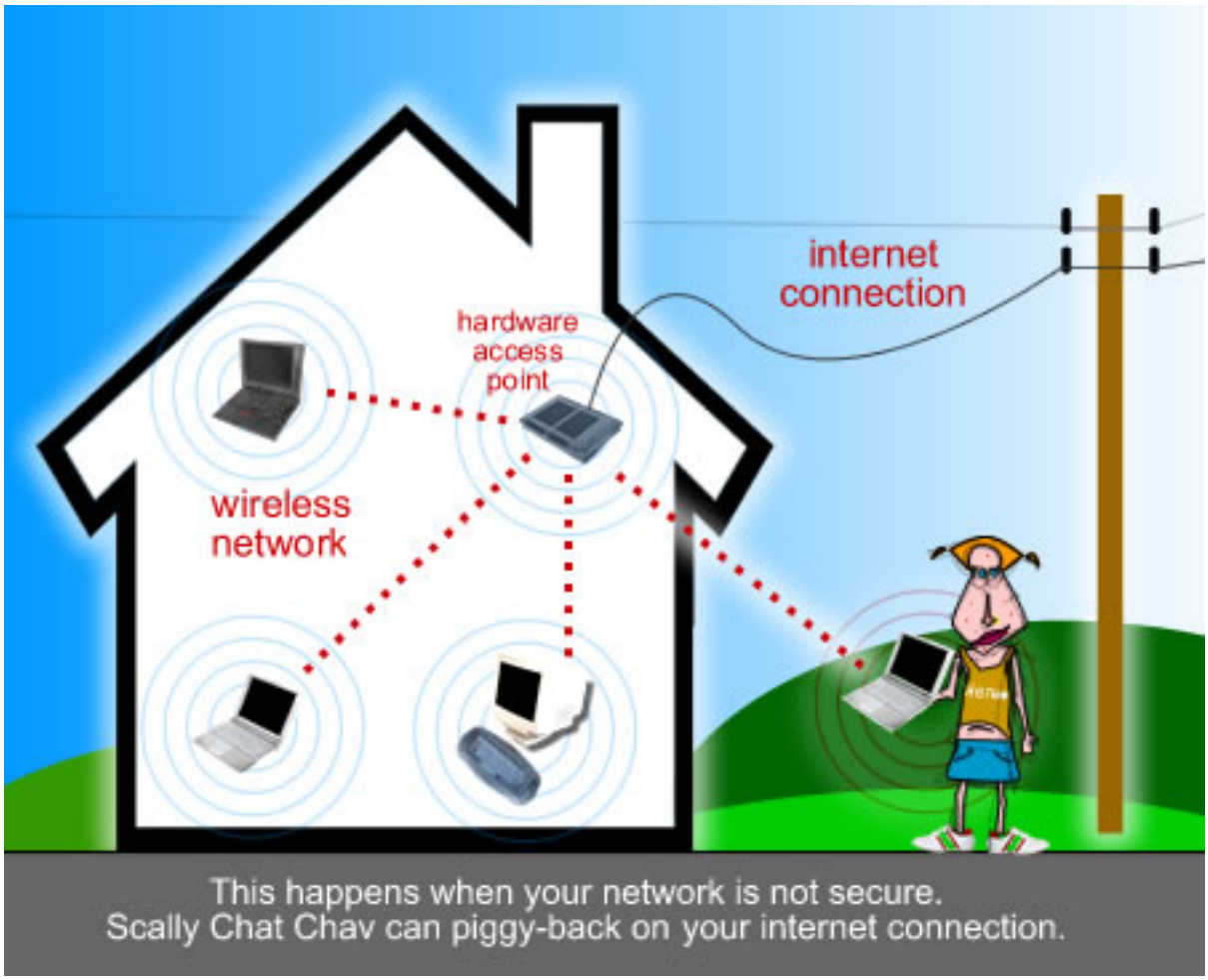
گام سوم: بررسی تناوبی لیست دستگاههای متصل شده

بسیاری از روترها (خصوصا روترهای نسل جدید) قابلیت این را دارند که به شما نشان دهند چه دستگاه یا دستگاههایی به شبکه وای فای شما متصل شده اند. بهتر است هر از چندی این مساله را بررسی کنید تا مطمئن شوید تنها رایانه‌ها و تبلت‌های موجود در منزل شما به شبکه وای فای شما متصل شده‌اند.

برای این‌کار باید با استفاده از مرورگر اینترنتی خود، به روتر متصل شوید. در بسیاری از روترها شیوه‌های اتصال به روتر را توضیح داده است.

معمولا روترها برای وارد شدن به تنظیمات از آی‌پی‌های ۱۹۲.۱۶۸.۱.۱ یا ۱۹۲.۱۶۸.۰.۱ استفاده می‌کنند. بدین‌ترتیب باید یکی از مرورگرهای خود را باز کنید و یکی از این دو آی‌پی را وارد کنید تا وارد مدیریت روتر خود شوید. معملا شناسه و رمز عبور، واژه‌ی Admin است مگر اینکه شرکت اینترنتی شما، واژه‌ی خاصی را در حین نصب، برای ورود مشخص کرده باشد.

پس از ورود به بخش مدریریت روتر، لیستی از Clients DHCPها وجود دارد که به راحتی می توانید ببینید که آیا کسی به وای فای شما متصل است یا نه. این آدرس در برخی روترها کمی تفاوت دارد اما پیدا کردن آن چندان دشوار نیست.



گام چهارم: استفاده از نرم‌افزارهای امنیتی

یکی دیگر از روش‌های افزایش امنیت وای‌فای، استفاده از برنامه های کاربردی‌ای است که بدین منظور تولید شده‌اند. بعضی از برنامه‌ها، پیش از اتصال کاربر به اینترنت، چند سوال امنیتی از کاربر می‌پرسد که در صورت پاسخ صحیح، کاربر می‌تواند به وای‌فای متصل شود. البته تمامی این سوالات توسط خود کاربر و به منظور حفاظت امنیت بیشتر ایجاد شده است. در این مورد، برنامه‌ی Guardian WiFi توصیه می‌شود.

نرم افزار دیگری نیز برای امنیت وای فای وجود دارد که شما را از گزند ورود غریبه‌ها در امان می‌دارد. یکی از این نرم‌افزارها Watcher Network Wireless است که به محض اتصال یک فرد غریبه به وای فای شما، این مساله را به شما اطلاع می‌دهد.

گام پنجم: خاموش کردن مهمان شبکه

روترها در حالت پیش‌فرض، بخش «مهمان شبکه» را غیر فعال می‌کنند. این بخش، برای به اشتراک گذاری اینترنت شما به کسانی که شما تعریف می‌کنید کاربرد دارد. بهتر است برای اطمینان، از خاموش بودن این گزینه مطلع باشید. این گزینه در بسیاری از روترها و در بخش مدیریت روتر، با عنوان Access Guest درج شده است که با انتخاب گزینه‌های Off و On می‌توانید آن را خاموش یا روشن کنید.

گام ششم: به روز رسانی تناوبی سیستم عامل روتر

روترها معمولا هر از چندی نرم‌افزارهای امنیتی سیستم خود را به روز رسانی می‌کنند. این نرم‌افزاها معمولا در وب‌سایت روتر قرار داده می‌شود که بهتر است روتر خود را به روز نگه دارید.

گام هفتم: خاموش کردن روتر در زمان‌های غیر فعال
بهتر است در زمان‌هایی که به اینترنت متصل نیستید، و یا به مسافرت می‌روید، دستگاه روتر خود را خاموش کنید. این کار به شما اطمینان صد در صدی می‌دهد که کسی به شبکه وای‌فای شما متصل نیست

نویسنده: admin، تاریخ ارسال: چهارشنبه 16 اردیبهشت 1394 ساعت 03:54 بعد از ظهر