## ایمن سازی مودم اینترنت خانگی

Wi-Fi خانه خود را در ۷ مرحله ساده ایمن نگه دارید.

چقدر به Wi-Fi خانگی خود متکی هستید؟ اگر مانند اکثر مردم هستید، از آن برای بانکداری آنلاین، برای پرداخت کارت اعتباری خود، برای رزرو اتاق هتل، برای چت با دوستان و تماشای فیلم استفاده می‌کنید، این فعالیت زیادی است. در بسیاری از موارد، همه چیز از لپ‌تاپ و تلفن گرفته تا سیستم‌های امنیتی، ترموستات‌ها و تهویه مطبوع همگی به Wi-Fi خانگی متصل هستند، این یک فایده است.

اما هنگامی که محافظت نمی‌شود، شبکه Wi-Fi خانگی شما می‌تواند زمین بازی برای کلاهبرداران، هکرها و سایر مجرمان سایبری باشد. یک آسیب پذیری کوچک در شبکه Wi-Fi خانگی شما می‌تواند به مجرم دسترسی تقریباً تمام دستگاه‌هایی که به آن شبکه متصل می‌شوند، بدهد. هکرها و کلاهبرداران ممکن است بتوانند به حساب‌های بانکی آنلاین یا درگاه‌های کارت اعتباری شما دسترسی پیدا کنند. آن‌ها ممکن است بتوانند از ایمیل‌هایی که برای پزشکتان ارسال می‌کنید جاسوسی کنند. حتی ممکن است دستگاه‌های شما را با بدافزار و نرم افزارهای جاسوسی پر کنند.

1- نام پیش فرض Wi-Fi خانه خود را تغییر دهید.

ابتدا SSID (شناسه مجموعه سرویس) یا نام شبکه Wi-Fi خانگی خود را تغییر دهید. بسیاری از تولیدکنندگان به همه روترهای بی سیم خود یک SSID پیش فرض می‌دهند. در بیشتر موارد این نام شرکت است. هنگامی که یک کامپیوتر شبکه‌های بی سیم اطراف را جستجو و نمایش می‌دهد، هر شبکه‌ای را که به طور عمومی SSID خود را پخش می‌کند لیست می‌کند. این به یک هکر شانس بیشتری برای نفوذ به شبکه شما می‌دهد. بهتر است SSID شبکه را به چیزی تغییر دهید که هیچ اطلاعات شخصی را فاش نکند و در نتیجه هکرها را از ماموریت خود دور کنید.

2- رمز عبور شبکه بی سیم خود را منحصر به فرد و قوی کنید.

اکثر روترهای بی سیم از پیش تنظیم شده با رمز عبور پیش فرض ارائه می‌شوند. این رمز عبور پیش فرض توسط هکرها به راحتی قابل حدس زدن است، به خصوص اگر سازنده روتر را بشناسند. هنگام انتخاب یک رمز عبور خوب برای شبکه

بی سیم خود، مطمئن شوید که حداقل 20 کاراکتر شامل اعداد، حروف و نمادها داشته باشد. هرچه رمز عبور شما پیچیده‌تر باشد، نفوذ هکرها به شبکه شما دشوارتر است.

3- رمزگذاری شبکه را فعال کنید.

تقریباً همه روترهای بی سیم دارای ویژگی رمزگذاری هستند. با این حال، برای اکثر روترها، به طور پیش فرض خاموش است. روشن کردن تنظیمات رمزگذاری روتر بی سیم می‌تواند به امنیت شبکه شما کمک کند. مطمئن شوید که بلافاصله پس از نصب روتر توسط ارائه دهنده پهنای باند، آن را روشن کنید. از میان بسیاری از انواع رمزگذاری موجود، جدیدترین و موثرترین آن‌ها "WPA2" است.

4- پخش نام شبکه را خاموش کنید

هنگام استفاده از روتر بی سیم در خانه، به شدت توصیه می‌شود که پخش نام شبکه را برای عموم مردم غیرفعال کنید. هنگامی که کاربران نزدیک سعی می‌کنند یک شبکه Wi-Fi پیدا کنند، دستگاه آن‌ها لیستی از شبکه‌های اطراف را نشان می‌دهد که می‌توانند از بین آن‌ها انتخاب کنند. با این حال، اگر پخش نام را غیرفعال کنید، شبکه شما نمایش داده نمی‌شود و اتصال Wi-Fi شما برای کسانی که نمی‌دانند به دنبال آن بگردند نامرئی می‌ماند.

این ویژگی برای مشاغل، کتابخانه‌ها، هتل‌ها و رستوران‌هایی که می‌خواهند دسترسی به اینترنت بی‌سیم را به مشتریان خود ارائه دهند مفید است، اما برای یک شبکه بی‌سیم خصوصی، از جمله شبکه Wi-Fi خانگی شما، غیر ضروری است.

5- نرم افزار روتر خود را به‌روز نگه دارید

گاهی اوقات firmware روتر، مانند هر نرم‌افزار دیگری، حاوی نقص‌هایی است که می‌توانند به آسیب‌پذیری‌های بزرگ تبدیل شوند، مگر اینکه به سرعت توسط نسخه‌های میان‌افزار سازنده‌شان برطرف شوند. همیشه جدیدترین نرم افزارهای موجود برای روتر خود را نصب کنید و آخرین وصله‌های امنیتی را فوراً دانلود کنید. این احتمال را افزایش می‌دهد که هکرها نتوانند به شبکه Wi-Fi شما دسترسی پیدا کنند.

6- مطمئن شوید که فایروال خوبی دارید

فایروال برای محافظت از رایانه‌ها در برابر بدافزارها، ویروس‌ها و سایر نفوذهای مضر طراحی شده است. روترهای بی‌سیم معمولاً حاوی فایروال‌های داخلی هستند، اما گاهی اوقات با خاموش بودن این فایروال‌ها ارسال می‌شوند. بررسی کنید که فایروال روتر بی سیم شما روشن باشد. اگر روتر شما چنین فایروالی ندارد، مطمئن شوید که یک فایروال خوب را روی سیستم خود نصب کرده‌اید تا در برابر تلاش‌های دسترسی مخرب در شبکه بی سیم خود محافظت کنید.

7- برای دسترسی به شبکه خود از VPN استفاده کنید

شبکه خصوصی مجازی یا VPN، گروهی از رایانه‌ها یا شبکه‌هایی است که با هم از طریق اینترنت کار می‌کنند. افراد می توانند از VPNها مانند Norton Secure VPN به عنوان روشی برای ایمن سازی و رمزگذاری ارتباطات خود استفاده کنند. هنگامی که به یک VPN متصل می‌شوید، یک سرویس گیرنده VPN روی رایانه شما راه اندازی می‌شود.
هنگامی که با اعتبار خود وارد سیستم می‌شوید، رایانه شما کلیدها را با سرور دیگری مبادله می‌کند. هنگامی که هر دو رایانه یکدیگر را به عنوان معتبر تأیید کردند، تمام ارتباطات اینترنتی شما رمزگذاری شده و از کنجکاوی خارجی پنهان می‌شود.

بیشتر از همه، بررسی کنید که چه دستگاه‌هایی به شبکه خانگی شما متصل می‌شوند و مطمئن شوید که نرم افزار امنیتی قابل اعتمادی مانند Norton Security در برابر ویروس‌ها و جاسوس افزارها نصب شده است.