آیا شبکه بی‌سیم شما امن است؟

ترفندهایی که وای‌فای شخصی شما را امن نگه می‌دارد

ما برای محافظت از اموال خود درها را قفل می‌کنیم، زنگ خطر نصب می‌کنیم و حتی به شیشهها نوار محافظتی وصل می‌کنیم، اما وای‌فای خانگی خود را ناامن رها می‌کنیم. اما چرا خیلی از ما آنگونه که باید به امنیت شبکه خانگی خود اهمیت نمی‌دهیم؟

رشد روزافزون شبکه‌های وای‌فای و به واسطه آن حملات هکری که فناوری بی‌سیم را نشانه رفته‌اند ضرورت توجه به امنیت را دو چندان می‌کند. به ویژه آن که هکرها در اغلب موارد به دنبال آن هستند تا کلمه عبور مربوط به شبکه‌های وای‌فای را شکسته و از امکانات آن سوء استفاده کنند. بنابراین برای محافظت از شبکه وای‌فای خود اقداماتی لازم است که باید به آنها توجه کنید.

چگونه وای‌فای خود را امن نگه داریم

1. یک کلمه عبور جدید برای وای‌فای خود انتخاب کنید.

این یک راهکار مقدماتی و پایه برای افزایش سطح امنیت شبکه وای‌فای است که به جلوگیری از دسترسی غیرمجاز به شبکه کمک می‌کند. نداشتن کلمه عبور یا باقی نگه داشتن کلمه عبور پیش فرض کارخانه شبیه به این است که شما یک وای‌فای عمومی را در اختیار دیگران قرار داده باشید که همه می‌توانند به آن ملحق شوند. کلمات عبور شبکه بی‌سیم حداقل باید از 20 کاراکتر تشکیل‌شده باشد و ترکیبی از اعداد، حروف و نمادهای مختلف باشد. کلمات عبور را از کلمه‌های ساده انتخاب نکنید و تا حد امکان اندازه آنها را طولانی انتخاب کنید. این کار باعث می‌شود کلمه عبور در برابر حملاتی نظیر جست و جوی فراگیر ایمن باشد.

2. تنظیمات پیش فرض شبکه خود را تغییر دهید

خیلی از روترها از کلمات عبور، نام شبکه (SSID) و تنظیمات دیگر پیش فرض استفاده می‌کنند که باعث می‌شود به راحتی توسط دیگران قابل شناسایی باشد. به عنوان یک قانون کلی شما باید تنظیمات هر چیزی را که روی عملکرد شبکه تاثیر نمی‌گذارد را تغییر دهید.

3. آدرس‌های مک را فیلتر کنید.

شما با فیلتر کردن آدرس‌های مک دستگاه‌های متصل به شبکه می‌توانید سطح امنیت شبکه وای‌فای خود را افزایش دهید. به این شکل تنها دستگاه‌هایی که آدرس مک آنها در تنظیمات روتر وارد شده باشد می‌توانند به شبکه متصل شوند و امکان دسترسی سایر دستگاه‌ها و هک شبکه دشوارتر خواهد شد.

4. از انتشار و نمایش نام شبکه جلوگیری کنید

نام شبکه (SSID) شما تمام مدت منتشر شده و توسط سایرین قابل مشاهده است. این قابلیت به دستگاه‌های جدید امکان می‌دهد تا شبکه وای‌فای شما را راحت‌تر پیدا کرده و به آن متصل شوند، اما از طرفی شناسایی شما توسط مجرمین سایبری را نیز ساده‌تر می‌کند. با خاموش کردن نام شبکه خود شناسایی آن را برای سایرین دشوارتر کنید.

غیرفعال کردن SSID به این معنا نیست که شما دیگر نمی‌توانید وای‌فای خود را پیدا کنید. شما تنها باید نام شبکه وای‌فای را در زمان اتصال به طور دستی وارد کنید.

5. UPnP را غیرفعال کنید.

در خیلی از روترها UPnP به طور پیش فرض فعال است. این ویژگی به دستگاه‌های خارجی کمک می‌کند تا به طور خودکار به شبکه متصل شده و سایر دستگاه‌ها را شناسایی کند. اما از آنجا که روتر شما بررسی نمی‌کند که آیا اتصال برقرار شده از طریق پروتکل UPnP قابل اطمینان است یا خیر، این کار آسیب پذیری روتر شما را افزایش می‌دهد.

بدون UPnP شما باید پیکربندی پورت فورواردینگ را به طور دستی انجام دهید. اما انجام این کار ارزش صرف کار و وقت شما را دارد زیرا امنیت کلی شبکه شما را افزایش می‌دهد.

6. از رابط وب صفحه تنظیمات روتر خود خارج شوید.

بعضی از روترها ممکن است در برابر حملات تزریق اسکریپت از طریق وبگاه (XSS) آسیب پذیر باشند. به همین دلیل شما باید همیشه بعد از انجام تنظیمات روتر از طریق رابط وب از آن خارج شده یا اصطلاحا log out کنید. اگر فراموش کنید این کار را انجام دهید هکرها می‌توانند از آن بر علیه شما استفاده کرده و با دسترسی به اطلاعات ورود به شبکه شما نفوذ کنند.

7. از سیستم کدگذاری روی روتر خود استفاده کنید.

آیا می‌دانستید که می‌توانید روتر خود را کدگذاری کنید؟ بله شما می‌توانید با رفتن به صفحه تنظیمات امنیتی روتر خود به دنبال گزینه Encryption بگردید. با فعال کردن این گزینه تمام اطلاعات تبادل شده بین روتر و دستگاه‌های متصل به آن به صورت کدگذاری شده انجام می‌شود. توصیه می‌شود که از سیستم کدگذاری WPA2 برای این کار استفاده شود. کلمه عبور طولانی و پیچیده را هم فراموش نکنید.

8. دسترسی از راه دور را غیرفعال کنید

اغلب روترها را می‌توان از طریق یک رابط کاربری تحت وب پیکربندی و تنظیم کرد. تمام کاری که شما باید انجام دهید این است که مرورگر وب خود را باز کرده و آدرس آی‌پی روتر خود را در نوار آدرس وارد کنید. شما باید تنها در صورتی قادر باشید این کار را انجام دهید که به شبکه محلی خود متصل شده باشید. اما برخی از روترها هم هستند که امکان دسترسی از راه دور را هم فراهم می‌کنند، به این معنا که شما از آن سر دنیا و از طریق اینترنت هم می‌توانید به تنظیمات این روتر دسترسی پیدا کنید.

اگر این قابلیت فعال باشد نشان دهنده آن است که هکرها هم قادر خواهند بود به تنظیمات روتر شما دسترسی پیدا کنند. برای غیرفعال کردن این ویژگی، از طریق رابط وب تنظیمات روتر به دنبال عبارات Remote Access، Remote Administration یا Remote Management بگردید. در اغلب روترها این قابلیت به طور پیش فرض غیرفعال است، اما بهتر است خودتان یک بار آن را بررسی کنید.

9. اطمینان حاصل کنید که فایروال ویندوز شما روشن باشد.

اگر از کاربران ویندوز هستید مطمئن شوید این قابلیت امنیتی داخلی ویندوز روشن باشد. فایروال برنامه‌های بالقوه مضری که ممکن است در حین ارتباط با شبکه به کامپیوتر شما آسیب بزند را فیلتر و مسدود می‌کند. شما با تایپ عبارت firewall در نوار جستجو و بازکردن اپلیکیشن Windows Defender Firewall می‌توانید وضعیت روشن یا

خاموش بودن آن را بررسی کنید.

10. میان افزار روتر خود را به‌روزرسانی کنید

نرم افزاری که روی روتر اجرا می‌شود (تحت عنوان میان افزار یا firmware شناخته می‌شود) هم مثل هر نرم افزار دیگری با نقص‌هایی همراه است و هر از گاهی از طرف تولیدکننده به‌روزرسانی می‌شود تا علاوه بر افزایش کارایی دستگاه نقاط ضعف امنیتی احتمالی آن نیز برطرف شود. اما مشکل اینجا است که روتر شما مثل سیستم عامل شما را از وجود یک نسخه به‌روزرسانی جدید مطلع نمی‌کند.

برای بررسی این که آیا به به‌روزرسانی میان افزار احتیاج دارید تا نه به صفحه تنظیمات روتر بروید، نسخه میان افزار فعلی روتر خود را یادداشت کنید، سپس به وب‌سایت تولیدکننده روتر خود مراجعه کرده و اگر نسخه جدیدتری از میان افزار فعلی شما منتشر شده بود آن را دریافت و از طریق رابط وب تنظیمات روتر آن را نصب کنید.

تاریخ انتشار:

16 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/network-tricks/internet-tricks/16083/%D8%AA%D8%B1%D9%81%D9%86%D8%AF%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C-%D8%B4%D8%AE%D8%B5%DB%8C-%D8%B4%D9%85%D8%A7-%D8%B1%D8%A7-%D8%A7%D9%85%D9%86-%D9%86%DA%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%AF%D8%A7%D8%B1%D8%AF