دانشگاه علوم پزشکی و خدمات بهداشتی درمانی سپرجند

حراست

امن کردن شبکه بی سیم

تنظیم کننده :

حراست فناوری اطلاعات دانشگاه

اگر شما امنیت شبکه بی -سیم خود را تامین نکنید، غریبه- ها می توانند از این شبکه استفاده کنند و به اطلاعات شخصی و مالی شما که در کامپیوترتان ذخیره شده دسترسی یابند. با استفاده از سیستم رمزنگاری WPA از کامپیوترتان محافظت کنید.

با چگونگی کارکرد یک شبکه بی سیم آشنا شوید

به طور کلی برای ارسال اطلاعات از طریق شبکه بی سیم (Router)) به یک روتر بی سیم به عنوان نقطه دستیابی به اینترنت (Access Point) نیاز است. این روتر بی سیم که وظیفه اش مانند مودم کابلی یا DSL است، امواجی را در فضا منتشر می - کند که گاهی محدوده پوشش این امواج به صدها متر می رسد. هر کامپیوتری که در این محدوده قرار گرفته است و کارت (دستگاه) مخصوص دریافت امواج بی سیم را دارد ،این امواج را دریافت می کند و به اینترنت متصل می شود.

تا زمانی که اقدامات امنیتی و احتیاطی خاصی را به مرحله اجرا نگذارید، هر شخصی که در محدودهٔ پوشش امواج است و دستگاه های قابل حمل (مانند لپ تاپ یا تلفن همراه) و یا کامپیوتر مجهز به کارت (دستگاه) مخصوص دریافت امواج بی سیم را دارد، می تواند از شبکه شما استفاده کند. این به آن معنا است که همسایه شما و یا هکری که در نزدیکی شماست می تواند از شبکه شما استفاده کند و یا به اطلاعات موجود در کامپیوتر شما دسترسی یابند . اگر یک شخص غیر مجاز از شبکه شما برای انجام فعالیت های مجرمانهٔ خود و ارسال هرزنامه (Spam) استفاده کند، انجام این فعالیت ها به ردیابی و شناسایی حساب کاربری شما (از طرف ارائه دهنده خدمات اینترنت ISP) منجر می شود.

از سیستم رمزنگاری استفاده کنید

سیستم رمزنگاری از اطلاعاتی که شما در اینترنت رد و بدل می کنید، محافظت می کند و آن را به شکل یک کد در می آورد. بنابراین دسترسی به آن برای دیگران امکان پذیر نیست. استفاده از سیستم

رمزنگاری موثرترین روش برای محافظت از شبکه تان در برابر مزاحمان است.

دو سیستم اصلی رمز نگاری عبارت است از:

۱. دستیابی محافظت شده Wi-Fi WPA

۲. سیستم امنیتی شبه سیمی (WEP).

کامپیوتر و روتر و تجهیزات قابل استفاده شما باید از یک سیستم مشابه استفاده کنند. WPA2 قوی ترین سیستم است. اگر قدرت انتخاب دارید، از این سیستم استفاده کنید. این سیستم می‌تواند از شما در برابر اکثر هکرها محافظت کند . برخی از روترهای قدیمی تر، تنها از سیستم رمزنگاری WEP استفاده می کنند. این سیستم ها نمی توانند از شما در برابر برخی از برنامه‌های هک محافظت کنند. خریدن یک روتر جدید که از سیستم WPA2 پشتیبانی می کند، را در نظر بگیرید . روترهای بی سیم در زمان خرید سیستم رمزنگاری شان غیر فعال هستند، شما باید این سیستم را فعال کنید. در دفترچه راهنمایی که همراه با روتر است، توضیحاتی درباره چگونگی فعال کردن سیستم رمزنگاری وجود دارد. اگر چنین توضیحاتی وجود نداشت، از وب سایت شرکت سازنده اطلاعات لازم را به دست آورید.

امنیت کامپیوتر و روتر خود را تامین کنید

از یک نرم افزار ضد ویروس و ضد برنامه های جاسوسی و یک دیواره آتش (Firewall) استفاده کنید. از استانداردها و شیوه های اولیهٔ امنیت کامپیوتر که به طور متعارف برای هر کامپیوتر متصل به اینترنت، به کاربرده می شود، استفاده کنید.

اسم اولیه روتر را تغییر دهید

اسم روترتان (شناسه واحد خدمات یا به طور مخفف SSID می نامند.) به احتمال زیاد یک اسم استاندارد است که به طور پیش فرض توسط واحد ID شرکت سازنده تعیین شده است. اسم روترتان را به یک اسم منحصر به فرد که فقط شما آن را می دانید، تغییر دهید.

رمز عبور پیش فرض روتر خود را تغییر دهید

شرکت سازنده روتر بی سیم شما؛ احتمالاً یک رمزعبور پیش فرض استاندارد را تعیین کرده است که به شما اجازه می دهد، روتر خود را نصب کنید و با آن کار کنید. هکرها این رمزهای عبور پیش فرض را می دانند؛ بنابراین این رمز را به رمزی که فقط شما از آن اطلاع دارید، تغییر دهید . از رمزهایی استفاده کنید که حداقل حاوی ۱۰ کاراکتر است. هر چقدر که یک رمز عبور طولانی تر باشد، شناسایی آن کار سخت تری می شود. جهت تغییر رمز عبور روتر می توانید از کارشناسان کمک بگیرید.

دسترسی به شبکه را محدود کنید

تنها به کاربران خاصی اجازه دهید تا به شبکه بی سیم شما دسترسی داشته باشند: هر کامپیوتری که قادر به برقراری ارتباط با شبکه است یک MAC آدرس (آدرسی برای کنترل دسترسی) مخصوص به خود دارد. روترهای بی سیم معمولاً این قابلیت را دارند که تنها به دستگاه هایی که MAC آدرس

های مخصوص دارند، اجازه دسترسی به شبکه را بدهند. بعضی از هکرها از MAC آدرس های مشابه استفاده می کنند. پس تنها به این گزینه اکتفا نکنید. زمانی که از شبکه بی سیم تان استفاده نمی کنید، آن را خاموش کنید: هکرها زمانی که یک روتر خاموش است، نمی توانند به آن دسترسی پیدا کنند

تصور نکنید که شبکه های عمومی Wi-Fi امن هستند: در مورد اطلاعاتی که از طریق شبکه های بی سیم عمومی ارسال و یا دریافت می کنید، حساس و محتاط عمل کنید، بسیاری از کافی شاپ ها، هتل ها، فرودگاه ها و اماکن عمومی شبکه های بی سیم را جهت استفاده در اختیار مشتریان شان قرار می دهند. استفاده از این شبکه ها در اماکن عمومی کار راحتی است؛ اما این شبکه ها در بعضی مواقع امن نیستند.

منبع: ایران هشدار