شبکه‌های Fi–Wi و خطر سرقت اطلاعات بانکی

با گسترش و رواج استفاده از ابزارهای دیجیتال قابل حمل مانند موبایل های هوشمند و تبلت ها ، افزایش ضریب نفوذ اینترنت و دسترسی افراد به سرویس های اینترنت بانک و موبایل بانک بیشتر شده است. با این اوصاف، ممکن است بسیاری از ما بارها و بارها وقتی به یکی از شبکه های عمومی اینترنت Fi-Wi یا اصطلاحا « هات اسپات »دسترسی پیدا می کنیم، به این فکر بیفتیم که کارهای بانکی خودمان را ازاین طریق انجام بدهیم. اما نباید فراموش کرد که شبکه های Fi-Wi عمومی اصولا از نظر امنیت چندان قابل اعتماد نیستند که بتوان از آن ها برای انجام امور بانکی و کارهای شخصی و محرمانه خود استفاده کرد. اما بعضی معتقدند با توجه به اینکه ارتباط با وب سایت های بانکی و مشابه آن به صورت رمزگذاری شده انجام می‌شود، امنیت لازم برای انجام این امور به صورت مجازی و از طریق شبکه های اینترنت بی سیم عمومی هم فراهم می شود.

پاسخ کوتاه به این سوال که چرا نباید برای انجام امور بانکی و دیگر کارهای محرمانه از شبکه بی سیم عمومی استفاده کرد، این است که ساختار باز چنین شبکه‌هایی اجازه جاسوسی را به افراد متخصص و حرفه ای می‌دهد. از طرف دیگر ممکن است شبکه، شامل کامپیوترهای آلوده و خطرناک باشد و از همه بدتر اینکه ممکن است هات‌اسپات یا نقطه اتصال شما به شبکه، خودش آلوده باشد.

سرقت اطلاعات کاربران

رمزگذاری اطلاعات اساسا بسیار مفید است و بسیاری از مشکلات امنیتی را حل می‌کند. به عنوان مثال، اگر شبکه بی سیم شما دارای رمز عبور باشد، همسایه‌هایی که در فاصله ای محدود از خانه تان هستند، نمی‌توانند صفحاتی را که در حال مرور آن هستید ، ببینند. بنابراین ، همیشه توصیه می‌شود که برای شبکه بی سیم خانگی خود یک رمز عبور خوب انتخاب کنید و بعد از آن با گوشی، تبلت و یا لپ تاپ خودتان به آن متصل شوید.

این در حالی است که وقتی بیرون از خانه و در مکانی عمومی مثل هتل، فرودگاه و مجتمع‌های تجاری به شبکه بی سیم آن مکان متصل می‌شوید، ارتباط شما با روتر یا هات اسپات، رمزگذاری شده نیست. در واقع برای اتصال به چنین شبکه‌هایی، معمولا به رمزعبور نیازی نیست. ترافیک رمزگذاری نشده شما توسط هر کسی که به شبکه متصل باشد، قابل رویت خواهد بود و لذا افراد می توانند به راحتی صفحاتی را که مرور می‌کنید، ببینند. آنچه تایپ می‌کنید هم قابل رویت است و حتی مشخص می‌شود که به کدام وب سایت رمزگذاری شده سر زده‌اید! بنابراین به عنوان مثال ،اگر به وب سایت یک بانک متصل شوید، این ارتباط از چشم متخصصین پنهان نمی‌ماند، هر چند آنها متوجه نمی‌شوند که شما در وب سایت بانک خود دقیقا چه کارهایی انجام می‌دهید.

برای جاسوسی و سرقت اطلاعات در این شبکه‌های بی سیم، نرم‌افزارهای ساده‌ای هم وجود دارد. به عنوان مثال ، یک کاربر ساده با استفاده از Firesheep امکان جاسوسی از افراد دیگر متصل به شبکه را دارد. نرم‌افزارهای حرفه‌ای‌تر مثل Wireshark هم برای ذخیره کردن و تحلیل ترافیک اینترنتی کاربران وجود دارند.

در مقابل، می توان در چنین شبکه‌هایی که امنیت کامل وجود ندارد، با استفاده از پروتکل HTTPS ارتباط با وب سایت‌های مختلف را به صورت رمزگذاری شده انجام داد. وب سایت‌های مهم مثل وب سایت بانک‌ها از این پروتکل استفاده می‌کنند، اما در مورد وب سایت‌های دیگر هم می‌توان یک افزونه ساده روی مرورگر نصب کرد تا همه چیز ایمن‌تر از حالت معمولی ، یعنی همان استفاده از پروتکل HTTP شود. بنابراین توصیه می‌شود که از افزونه Everywhere HTTPS و مانند آن استفاده کنید.

با این حال اما نمی توانیدمطمئن باشید که با استفاده از پروتکل HTTPS مشکل به کلی حل می‌شود. نرم‌افزارهایی مثل sslstrip وجود دارند که می‌توانند لینک‌های معمولی http را به شکل https برای کاربر نمایش دهند و او را فریب دهند. در حقیقت نام دامنه یک وب سایت جعلی درست مثل وب سایت یک بانک به صورت https شبیه سازی می‌شود و کاربر به اشتباه می‌افتد. بنابراین هکر به کمک هات‌اسپات آلوده، اطلاعات حیاتی و مهم کاربر را به سرقت می‌برد.

راه حل دیگر مخصوص افرادی است که معمولا زیاد از چنین شبکه‌های نا امنی استفاده می‌کنند. بهتر است این دسته از کاربران از شبکه خصوصی مجازی یا VPN استفاده کنند، چون در این صورت تنها می‌توان ارتباط آن ها با یک سرور VPN را رویت کرد و در نتیجه امنیت اینترنتی افزایش می‌یابد.

کامپیوترهای آلوده

هر کامپیوتر، لپ تاپ و هر ابزار دیگری که به شبکه‌های بی سیم عمومی متصل شده، ممکن است آلوده به بدافزارهایی باشد که از طریق شبکه منتقل می‌شوند و به این ترتیب ابزار و دستگاه های دیگر متصل شده را آلوده می‌کنند و بنابراین شبکه‌های بی سیم عمومی کامپیوتر شما را به خطر می‌اندازند.

هنگام اتصال به این شبکه‌ها، معمولا فایروال ویندوز و یا هر فایروال دیگری که نصب کرده باشید، از شما در مورد شبکه جدید و تنظیمات امنیتی مناسب سؤال می‌کند. در مورد فایروال ویندوز، به جای انتخاب شبکه خانگی و کاری، شبکه عمومی یا Network Public را انتخاب کنید. در این صورت ویندوز فایل‌ها و اطلاعات حساس را با سایر کامپیوترهای موجود در شبکه به اشتراک نمی‌گذارد.

نکته دیگر به روز کردن ویندوز و نصب آخرین بسته‌های امنیتی عرضه شده است. در نهایت مهم‌ترین موضوعی که گاهی غفلت از آن تمام تلاش شما را هدر می‌دهد، فعال بودن فایروال است. آنتی ویروس‌ها و فایروال‌ها، سرعت سیستم عامل را با اشغال منابع سخت‌افزاری، کاهش می‌دهند و برخی از کاربران عادت کرده‌اند که نرم‌افزارهای امنیتی خود را تنها هنگام اتصال فلش یا سایر ابزارهای ذخیره سازی اجرا و فعال کنند. بنابراین مراقب باشید که فایروال کامپیوتر یا هر ابزار دیگری که با آن به شبکه بی سیم عمومی متصل شده‌اید، اجرا شده و فعال باشد.

هات‌اسپات آلوده

خطرناک‌ترین اتفاق ممکن اما این است که خود هات‌اسپات یا شبکه Fi-Wi عمومی آلوده باشد. دو احتمال وجود دارد، اول اینکه هات‌اسپات توسط بدافزارها آلوده شده و دوم اینکه شما به یک شبکه هانی‌پات متصل شده‌اید. هانی‌پات تله‌ای است که مدیران سرورها برای به دام انداختن هکرها، آشنایی با روش‌های نفوذ آن ها و آشنایی با کدهای دستکاری شده آن ها و از طرفی شناسایی حفره‌های امنیتی موجود، ایجاد می‌کنند.

در واقع هنگامی که به یک شبکه عمومی متصل می‌شویم، مشخص نیست که آیا این شبکه یک شبکه واقعی و سالم و یا یک تله است. حتی ممکن است یک هکر برای سرقت اطلاعات، یک شبکه بی سیم عمومی ایجاد کرده باشد. جالب است بدانید که ابزارهای ساده‌ای مثل Pineapple WiFi وجود دارند که درست مثل یکی از شبکه های بی سیمی که قبل به آن متصل شده‌اید ظاهر می‌شوند، در حالی که امکان انواع حملات کامپیوتری را برای هکر فراهم می‌کنند و از طرفی کاربر به راحتی به این شبکه‌های ساختگی اعتماد می‌کند.

به طور کلی اما حفظ امنیت و محافظت از حریم خصوصی در فضای گسترده وب بسیار مشکل است و همیشه باید مراقب بود تا هکرها اطلاعات مهم را از طریق جاسوسی سرقت نکنند. با توجه به توصیه‌های مطرح شده، بهتر است از شبکه‌های بی سیم عمومی که گاهی رایگان هم هستند، کمتر استفاده کنیم و در صورت استفاده بهتر است کارهای بانکی و دیگر امور شخصی خود را انجام ندهیم.