چرا آی‌فون پیغام Security Recommendation را در زمان اتصال به وای‌فای نشان می‌دهد؟

زمانی که از طریق آی‌فون به یک شبکه وای‌فای متصل می‌شوید، ممکن است پیغام Security Recommendation را در پایین نام شبکه مشاهده کنید. این پیغام زمانی ظاهر می‌شود که به یک شبکه غیر ایمن یا شبکه‌ای که از رمزنگاری ضعیف WEP استفاده کرده باشد متصل شوید.

شبکه‌های غیر ایمن همراه با رمزنگاری ضعیف

بعضی مواقع در زمان انتخاب و اتصال به یک شبکه وای‌فای عبارت Security Recommendation مشاهده می‌شود. این یک پیغام امنیتی مهم بوده که باید از سوی شما جدی قلمداد شود. در اکثر مواقع، آی‌فون به شما اجازه می‌دهد به یک شبکه غیر ایمن Unsecured Network که به نام شبکه‌های باز از آن‌ها نام برده می‌شود متصل شوید. برای ورود به این شبکه‌ها به هیچ گذرواژه‌ای نیاز نیست و هیچ‌گونه رمزنگاری نیز روی آن‌ها اعمال نشده است. شما با نگاه کردن به فهرست شبکه‌های نشان داده شده به خوبی فرق میان یک شبکه ایمن و رمزنگاری شده با یک شبکه غیر ایمن را تشخیص می‌دهید. شبکه‌هایی که با یک آیکن قفل نشان داده می‌شوند رمزنگاری شده و به یک گذرواژه برای ورود نیاز دارند. در مقابل شبکه‌های فاقد هرگونه قفلی غیر ایمن بوده و ممکن است اطلاعات را در معرض خطر قرار دهند.

مطلب پیشنهادی

با قابلیت‌های پنهان و جالب گوشی آیفونتان آشنا شوید
چگونه لیبل آیکون اپلیکیشن‌ها را از منوی آیفون حذف کنیم

پیغام Security Recommendation چه اطلاعاتی در اختیار ما قرار می‌دهد؟

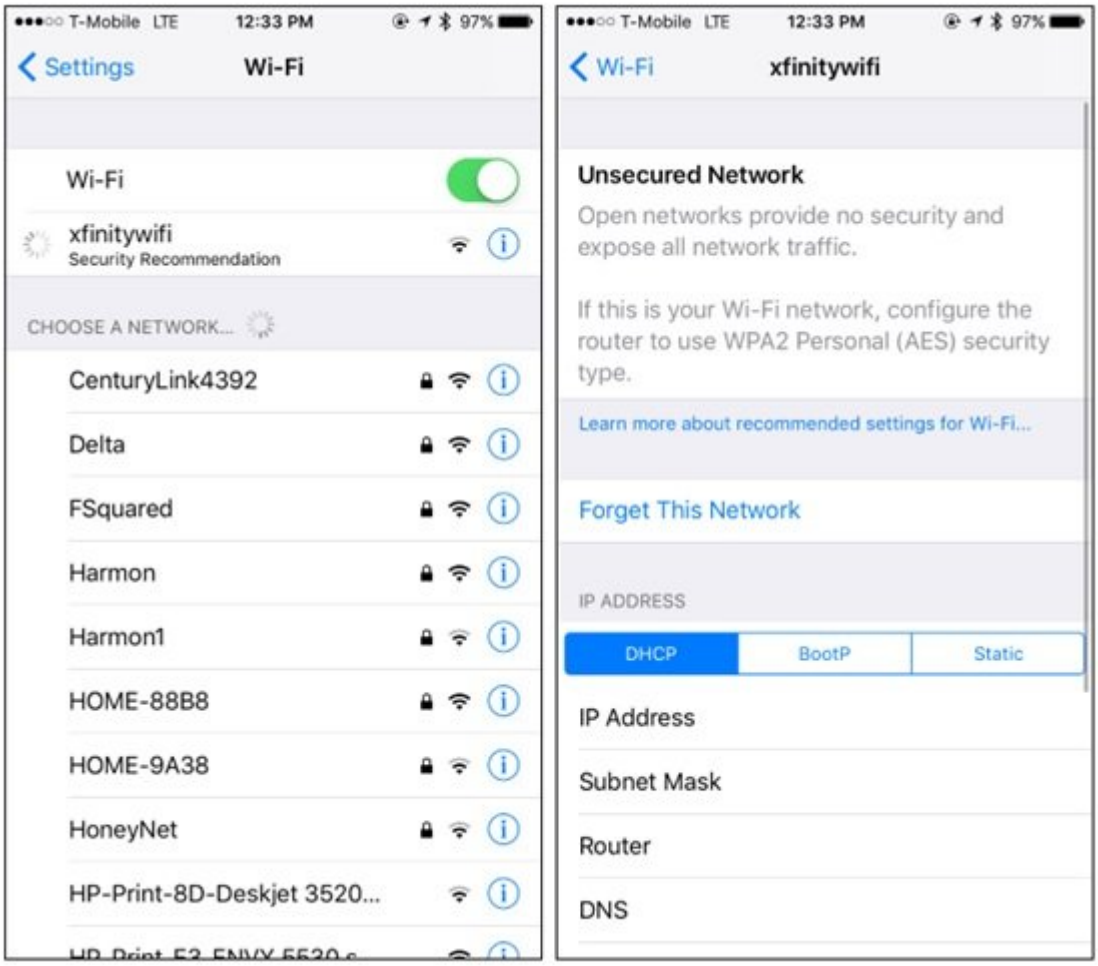
این پیغام زمانی ظاهر می‌شود که به یک هات‌اسپات رمزنگاری شده متصل شده‌اید که از یک استاندارد رمزنگاری منسوخ شده WEP به جای رمزنگاری مدرن WPA2 استفاده کرده باشد.

مطلب پیشنهادی

عدم دسترسی به سیگنال وای‌فای
هفت مورد از رایج‌ترین مشکلات وای‌فای همراه با راه‌حل آن‌ها

این پیغام اعلام می‌دارد که شبکه فوق برای انجام یکسری کارهای حساس همچون ورود به حساب‌های بانکی یا وارد کردن گذرواژه و نام کاربری در شبکه‌های اجتماعی مناسب نیست. WEP یک استاندارد رمزنگاری قدیمی بوده که به آسانی ممکن است هک شود. توصیه ما این است که از شبکه‌هایی که از استاندارد WPA2 همراه با الگوی رمزنگاری AES استفاده می‌کنند برای ورود به فضای مجازی استفاده کنید.

چرا شبکه‌های ضعیف و غیر ایمن خطرناک هستند؟



چرا نباید به یک شبکه وای‌فای باز که نیاز به هیچ‌گونه گذرواژه‌ای ندارد متصل شویم؟ در جواب این پرسش باید بگوییم شبکه‌های باز هیچ‌گونه مکانیزم امنیتی را در اختیار شما قرار نداده و در نتیجه ترافیک شبکه شما به راحتی قابل شنود است. این حرف به معنای آن است که هر شخصی منجمله هکرها قادر هستند بدون نیاز به هیچ گذرواژه‌ای به این شبکه‌ها متصل شوند.

مطلب پیشنهادی

حمایت LTE از اینترنت اشیا

اگر شبکه خانگی خود را به این شکل پیکربندی کرده‌اید باید بدانید که هر شخصی قادر است به شبکه شما متصل شده و فعایت‌های غیرقانونی را به نام شما انجام داده و مهم‌تر از آن به ردیابی آدرس IP شما بپردازد. فقدان رمزنگاری به معنای شنود راحت ترافیک شبکه است. خوشبختانه در زمان به‌کارگیری چنین شبکه‌های غیرایمنی هنوز هم یک لایه امنیتی اضافی به واسطه پروتکل HTTPS که بعضی از سایت‌ها از آن استفاده می‌کنند وجود دارد. با این وجود نباید این موضوع را نادیده بگیرید که بازهم در چنین حالتی هر فردی می‌تواند اطلاع پیدا کند شما به چه سایتی مراجعه کرده‌اید.

مطلب پیشنهادی

با قابلیت‌های پنهان و جالب گوشی آیفونتان آشنا شوید
چگونه صدای سیری در آیفون را از زنانه به مردانه تغییر دهیم

چگونه می‌توانیم از شبکه‌های غیرایمن به شکل ایمن استفاده کنیم؟

به‌طور معمول پیغام توصیه‌های امنیتی را زمانی که به شبکه‌های وای‌فای فرودگاه‌ها، هتل‌ها و کافی‌شاپ‌ها متصل می‌شوید مشاهده می‌کنید. متاسفانه پیکربندی این شبکه‌ها به گونه‌ای است که هر فردی بتواند به سادگی از آن‌ها استفاده کند. اما برای ایمن‌سازی چنین شبکه‌هایی می‌توانید از راه‌حل VPN که یک لایه رمزنگاری ایمن را روی همه ترافیک شما به وجود می‌آورد و به شما اجازه می‌دهد به شکل ایمنی به هات‌اسپات‌های عمومی متصل شوید استفاده کنید. در چنین شرایطی اگر فردی تصمیم بگیرید ترافیک شما را شنود کند تنها یک ارتباط با سرور VPN که داده‌ها را با یک الگوریتم رمزنگاری کدگذاری کرده است مشاهده می‌کند.

خبر خوب این است که در آینده شبکه‌های وای‌فای عمومی از استاندارد شبکه Hotspot 2.0 استفاده خواهند کرد که هر دو فاکتور اتصال ایمن و رمزنگاری ایمن را در اختیار شما قرار خواهند داد.

تاریخ انتشار:
04 مرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/8689/%DA%86%D8%B1%D8%A7-%D8%A2%DB%8C%E2%80%8C%D9%81%D9%88%D9%86-%D9%BE%DB%8C%D8%BA%D8%A7%D9%85-security-recommendation-%D8%B1%D8%A7-%D8%AF%D8%B1-%D8%B2%D9%85%D8%A7%D9%86-%D8%A7%D8%AA%D8%B5%D8%A7%D9%84-%D8%A8%D9%87-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C-%D9%86%D8%B4%D8%A7%D9%86