فهرست مطالب

عنوان **صفحه**

1- وای‌فای (Wi-Fi) چیست؟

شبکه وای‌فای یک نوع شبکه داخلی بی‌سیم است که می‌تواند دستگاه‌های موجود در یک محدوده خاص را به هم متصل کند. امروزه بیشتر مودم‌های ADSL می‌توانند شبکه وای‌فای ایجاد کنند. به این ترتیب مودم اطلاعات را از شبکه اینترنت گرفته و در شبکه وای‌فای خود توزیع می‌کند. هر دستگاهی که به شبکه وای‌فای ایجاد شده دسترسی داشته باشد می‌تواند به اینترنت متصل شود.

2- چرا امنیت شبکه وای‌فای مهم است؟

اگر شبکه وای‌فای شما به خوبی حفاظت نشده باشد، هرکسی می‌تواند به آن نفوذ کند، اولین ضرر این کار هم این است که حجم اینترنت شما دزدیده می‌شود و متحمل هزینه بیشتری در دریافت خدمات اینترنتی خواهید شد. علاوه بر این، استفاده کنندگان غیرمجاز با مصرف پهنای باند اینترنت شما، سرعت را به شدت پایین می‌آورند.

اما مهمترین ضربه وقتی وارد می شود که نفوذ کنندگان فقط به مصرف اینترنت قانع نباشند و بخواهند به دستگاه‌های دیگر که به شبکه وای‌فای وصل هستند دسترسی پیدا کنند. از آنجا که وای‌فای نوعی شبکه داخلی است، اگر افراد غیرمجاز وارد این شبکه شوند، ممکن است بتوانند به موبایل، لپ‌تاپ یا دیگر دستگاه‌های موجود در شبکه نفوذ کنند، به خصوص اگر دستگاه‌های شما قابلیت اشتراک فایل‌ها را فعال کرده و یا تنظیمات امنیتی‌شان مشکلی داشته باشد.

به صورت خلاصه، استفاده از وای‌فای هک شده، سه نقطه ضعف خواهد داشت:

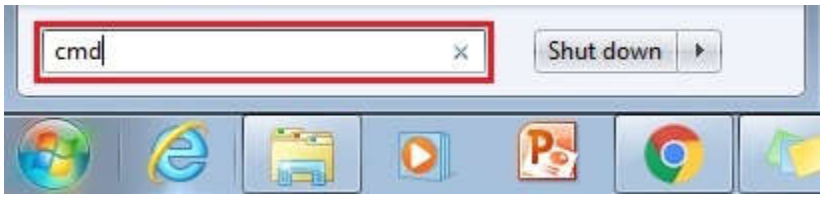
- مصرف حجم اینترنت به صورت غیر عادی افزایش پیدا خواهد کرد و در نتیجه هزینه دریافت خدمات اینترنتی نیز برای شما افزایش می‌یابد.
- سرعت اینترنت شما کاهش می‌یابد.
- در صورت هک شدن وای‌فای در واقع در معرض یک خطر امنیتی قرار گرفته‌اید که امکان دارد هکر از این طریق به کامپیوتر شما نیز نفوذ کرده و به فایل های شخصی‌تان دسترسی پیدا کند.

3- مراحل امن سازی وای‌فای مودم

3-1- ایجاد یک پسورد اختصاصی برای مودم (مرحل اول)

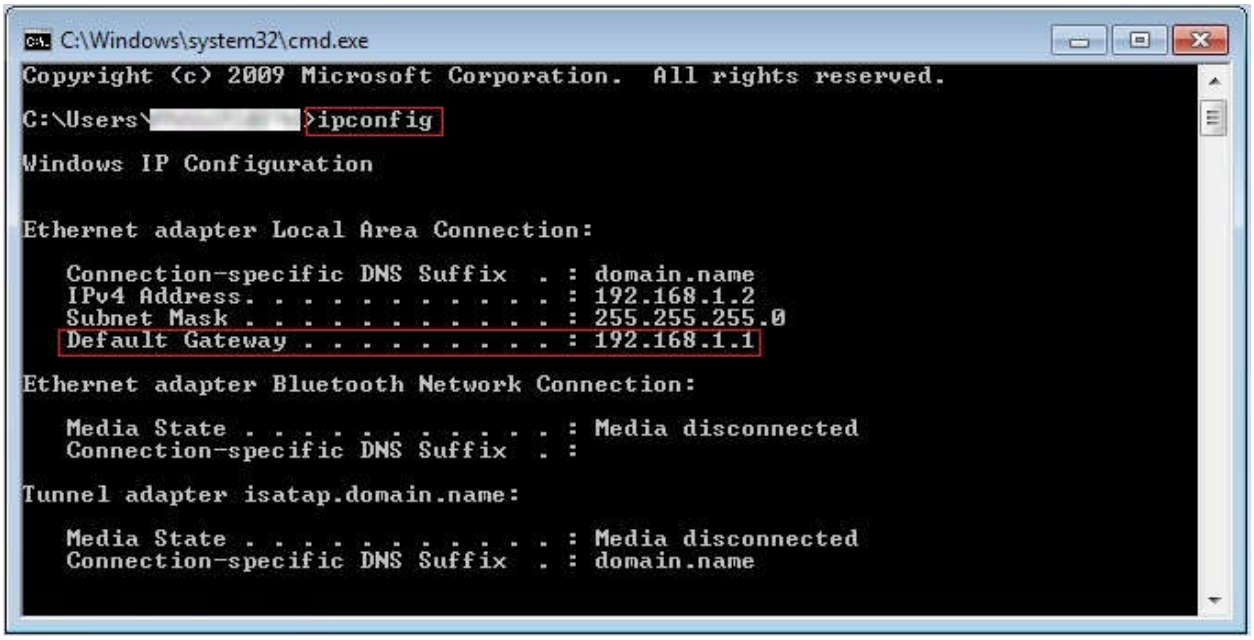
تولیدکنندگان مودم‌های ADSL، صفحات وبی را برای راه‌اندازی و پیکربندی این تجهیزات در اختیار کاربران قرار داده‌اند. این ابزارهای وب با یک صفحه Login (با نام کاربری و کلمه عبور) محافظت می‌شوند تا فقط دارندگان قانونی مودم بتوانند به این تنظیمات دسترسی داشته باشند. با این‌حال، اطلاعات Login پیش‌فرض بیشتر تجهیزات شبکه بسیار ساده بوده (معمولاً admin و admin است هم برای نام کاربری و رمزعبور) و هکرهای اینترنتی کاملاً از آنها آگاهی دارند. بنابراین، بهتر است به محض ورود به صفحه تنظیمات مودم، پسورد مودم را تغییر دهید. فراموش نکنید پس از تغییر دادن رمز حتماً پسورد جدید را به خاطر بسپارید تا اگر بار دیگر خواستید وارد صفحه تنظیمات مودم شوید به مشکل بر نخورید. این کار از دسترسی دیگران به مودم شما جلوگیری کرده و امنیت شبکه وایرلس خانگی شما را افزایش می‌دهد. برای تغییر

پسورد مودم، در ابتدا، IP مودم خود را با دستور ipconfig در ویندوز و دستور ifconfig در سیستم‌عامل‌های مک (Mac) و لینوکس به دست آورید. در سیستم‌عامل ویندوز در قسمت جستجوی برنامه در پایین و سمت چپ صفحه نمایش مطابق شکل1، عبارت CMD را نوشته سپس در قسمت نتایج جستجو CMD را انتخاب نمایید.



شکل1: اجرای برنامه خط فرمان

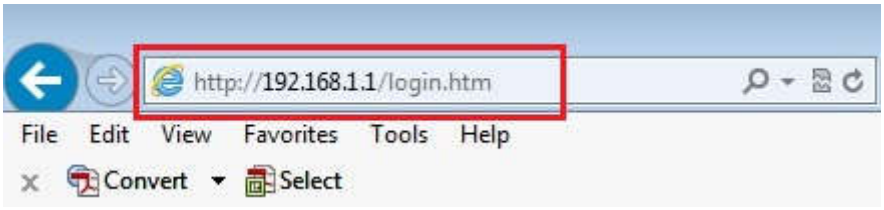
پس از اینکه CMD اجرا شد یک پنجره سیاه رنگ مطابق شکل2 نمایش داده می‌شود در این قسمت دستور ipconfig را نوشته کلید Enter را بزنید.



شکل2: اجرای دستور ipconfig

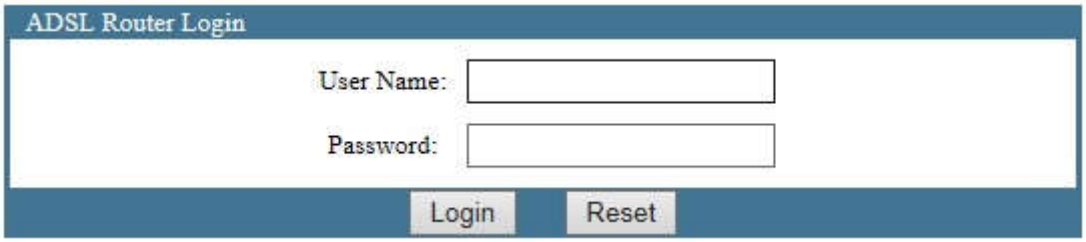
عدد نوشته شده روبروی Default Gateway که IP مودم شما می‌باشد را کپی کرده و مطابق شکل3 در آدرس بار مرورگر خود Paste نموده و کلید Enter را بزنید.

نکته: آدرس IP، نام کاربری و رمز عبور بر روی جعبه‌ی تمامی مودم ها نوشته شده است. در صورت دسترسی به جعبه مودم نیازی به طی مراحل بالا نیست و IP نوشته شده بر روی جعبه را آدرس بار مرورگرخود کپی نمایید.



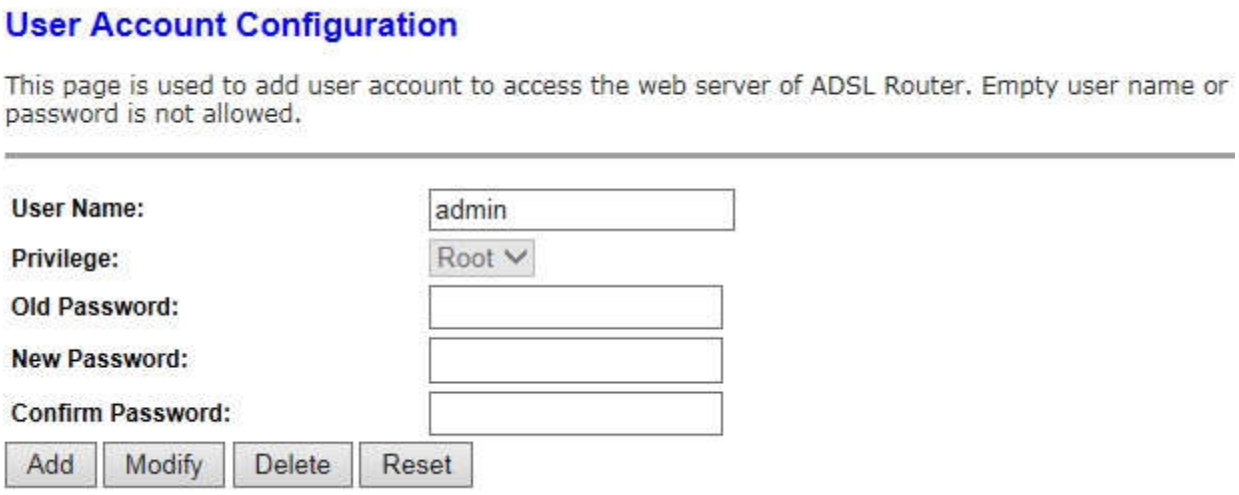
شکل3: روش دسترسی به تنظیمات مودم

در پنجره نمایش داده شده مانند شکل4، نام کاربری و رمزعبور را وارد نماید. به صورت پیش فرض در بیشتر مودم‌ها نام کاربری و رمزعبور Admin می باشد.



شکل4: صفحه Login تنظیمات مودم

سپس با توجه به برند مودم، وارد بخش تنظیمات Administration یا Maintenance شده و در قسمت مربوط به تغییر پسورد مانند شکل5، رمزعبور را تغییر دهید. اگر اولین بار است که مودم را راه اندازی می‌کنید در همان صفحه اول، گزینه تغییر رمزعبور برای شما نمایش داده می‌شود در غیر این صورت می‌توانید بر روی گزینه Setup در صفحه اول کلیک کرده و در قسمت مربوطه وارد و رمزعبور مودم را تغییر دهید.



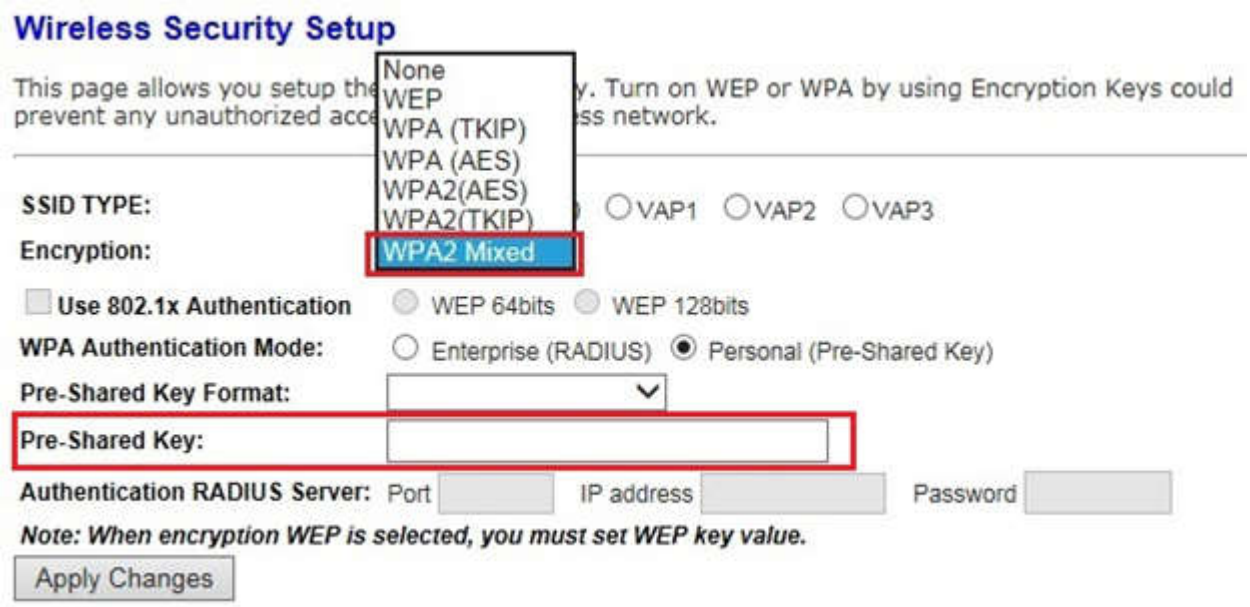
شکل5: صفحه تغییر رمز عبور تنظیمات مودم

2-3- فعال کردن رمزعبور وای‌فای (مرحله دوم)

برای جلوگیری از هک وای‌فای از رمزهای عبور قابل اطمینان استفاده نمایید. چندین روش رمزنگاری برای حفاظت از شبکه‌های بی‌سیم وجود دارد از جمله می‌توان WEP، WPA و WPA2 را نام برد. رمزنگاری از طریق WEP یک روش قدیمی می‌باشد و به راحتی قابل هک شدن است با این حال با اکثر دستگاه‌های سخت افزاری قدیمی سازگاری دارد. اما روش رمزنگاری WPA2 که امن‌ترین روش رمزنگاری برای وای‌فای می‌باشد تنها با سخت افزارهای تولید شده از سال ۲۰۰۶ به بعد سازگار است. اگر مودم شما از روش رمزنگاری WPA2 یا WPA پشتیبانی می‌کند این روش را انتخاب نمایید و در غیر این صورت از روش‌های دیگر استفاده نمایید.

برای فعال‌سازی رمزعبور و انتخاب روش رمزنگاری شبکه وای‌فای خود، وارد صفحه تنظیمات مودم و بخش Wireless Security Setup مانند شکل6 شده روش رمزنگاری موردنظر خود را از قسمت Encryption انتخاب نموده و در قسمت Pre-Shared Key رمز وای‌فای مطلوب خود را وارد نمایید. بقیه تنظیمات این صفحه را در حالت پیش‌فرض قرار دهید.

نکته: بهتر است برای دستیابی به امنیت بیشتر یک پسورد طولانی شامل حروف بزرگ و کوچک، اعداد و کاراکترهای خاص برای شبکه وای فای خود انتخاب نمایید.



شکل6: صفحه تنظیمات امنیتی مودم

نکته: در برخی برندهای مودم به جای WPA2 Mixed گزینه‌های مشخص شده در شکل7 را انتخاب نمایید.

شکل7: تنظیمات امنیتی مودم

3-3- تغییر نام شبکه وای‌فای یا SSID (مرحله سوم)

نام شبکه وای‌فای یا SSID معمولاً به صورت پیش‌فرض بر روی نام برند مودم شما تنظیم شده است. SSID مخفف عبارت **S**ervice **S**et **Id**entifier بوده و یک مقدار قابل فهم و خواندن برای انسان است که بتواند شبکه‌های مختلف را تشخیص دهد.

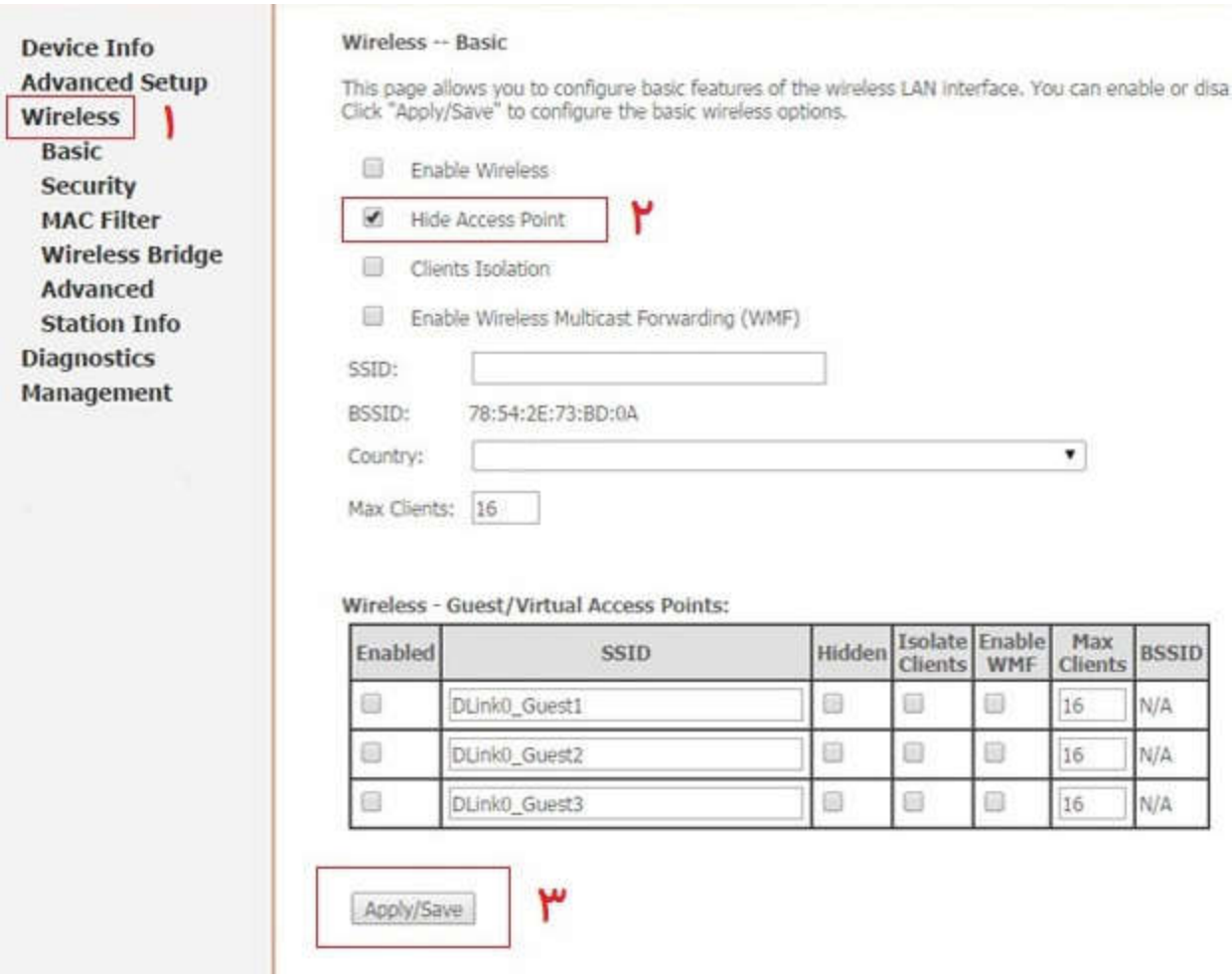
اگر می‌خواهید شبکه خانگی وایرلس خود را امن کنید حتما نام وای‌فای خود را به نام دلخواهی که قابل شناسایی نباشد، تغییر دهید. برای تغییر نام وای‌فای می‌توانید از صفحه تنظیمات مودم و بخش Wireless Settings مانند شکل8 یا هنگام راه‌اندازی از قسمت Setup اقدام به تغییر نام وایرلس شبکه خانگی خود نمایید. بعد از تغییر نام شبکه وای‌فای، از اتصال مجدد خود اطمینان حاصل نمایید.

نکته: بهتر است از نام، نام خانوادگی، آدرس یا شماره تلفن به عنوان نام وای‌فای استفاده نکنید زیرا این کار امنیت وای‌فای شما را به خطر می اندازد.

شکل8: صفحه تغییر نام شبکه وای‌فای یا SSID

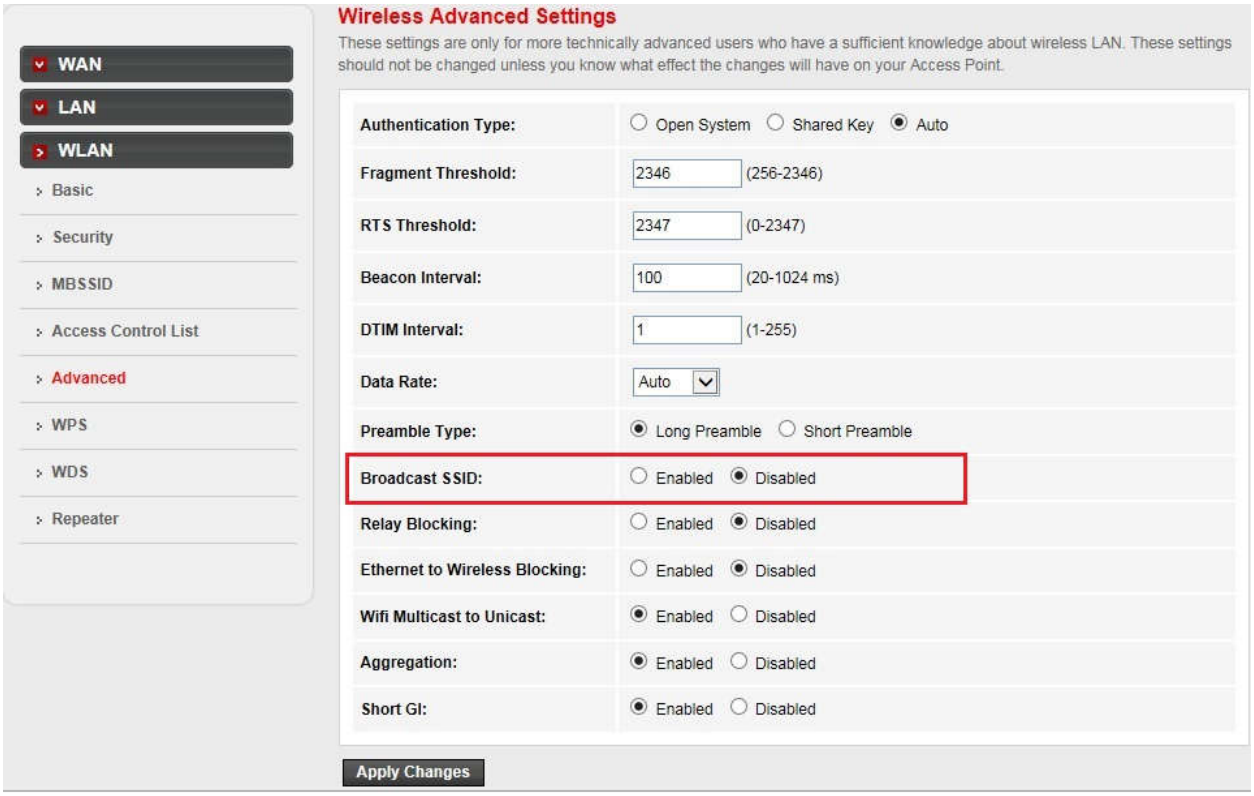
4-3- پنهان سازی شبکه وای‌فای یا SSID (مرحله چهارم)

وارد صفحه تنظیمات مودم شده و در قسمت تنظیمات Wireless مودم همانند شکل9 به قسمت Basic بروید. برای پنهان کردن مودم تیک گزینه Hide Access Point را بزنید. (ممکن است در مودم‌های مختلف این گزینه در قسمت های دیگر منو Wireless باشد که با کمی جستجو می‌توانید آن را پیدا کنید). در پایان برای ذخیره تنظیمات بر روی گزینه Apply/Save کلیک نمایید تا تغییرات اعمال شود.



شکل9: پنهان سازی شبکه وای‌فای یا SSID

نکته: در برخی برندهای مودم به جای گزینه Hide Access Point برای پنهان سازی شبکه وای‌فای می‌بایست گزینه‌ی Broadcast SSID را مطابق شکل10 غیرفعال(Disabled) نمود.



شکل10: پنهان سازی شبکه وای‌فای

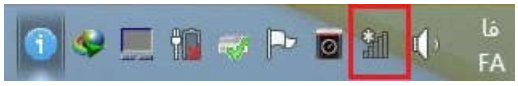
1-4-3- روش اتصال به شبکه‌های پنهان شده

برای اتصال به شبکه های پنهان شده باید نام وای فای(SSID) و رمز رو به صورت دستی وارد کنید.

1-1-4-3- اتصال به شبکه وای‌فای پنهان شده در ویندوز

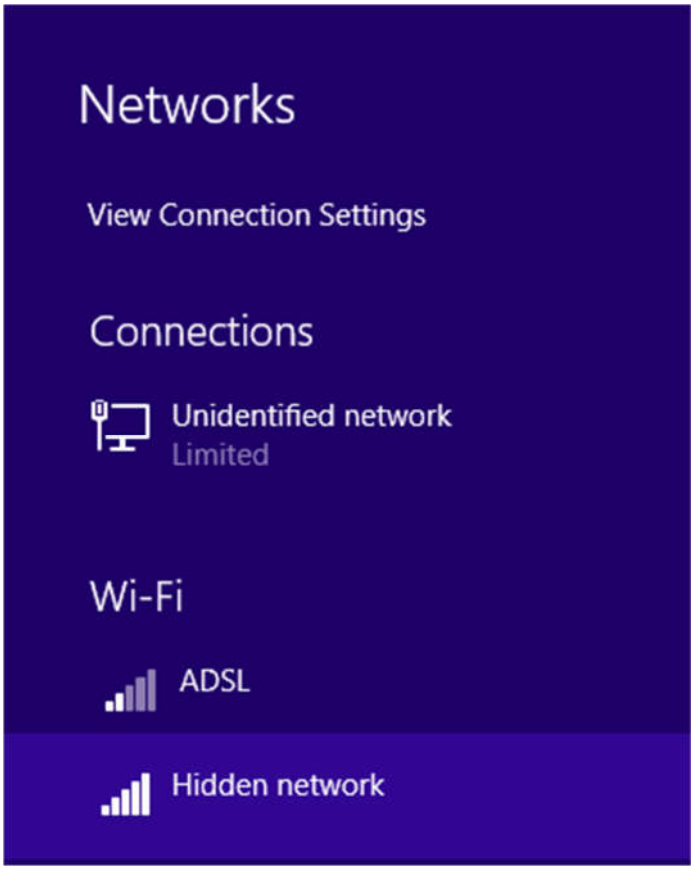
در این قسمت روش اتصال به شبکه وای‌فای پنهان شده در ویندوز۸ شرح داده شده است. لازم به ذکر است اتصال در نسخه‌های دیگر ویندوز نیز مشابه این روش می‌باشد.

در قسمت تسک بار (Taskbar) ویندوز، روی علامت وای‌فای مطابق شکل 11 کلیک نمایید.

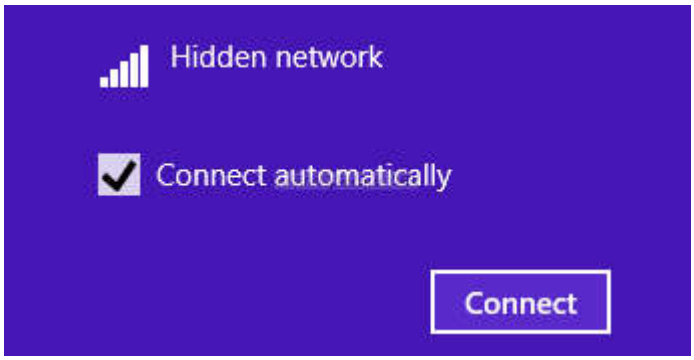


شکل11: محل علامت وای‌فای در تسک بار ویندوز

روی Hidden network مطابق شکل12 و سپس روی Connect مطابق شکل13 کلیک نمایید.

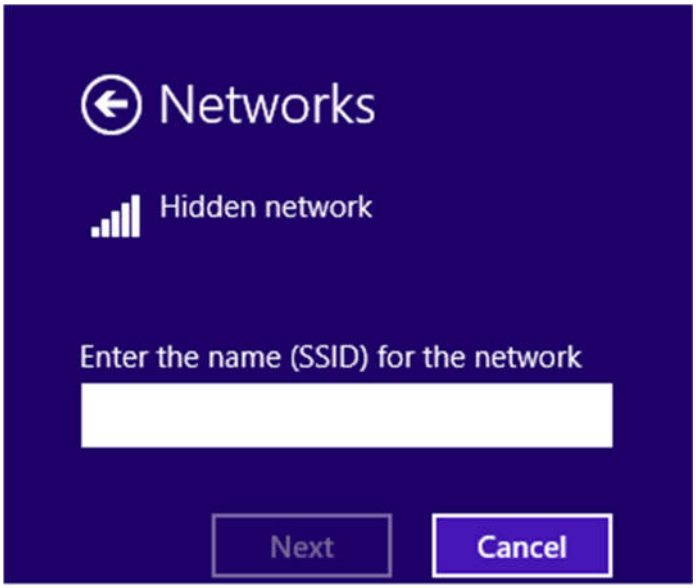


شکل12: انتخاب شبکه وای‌فای پنهان



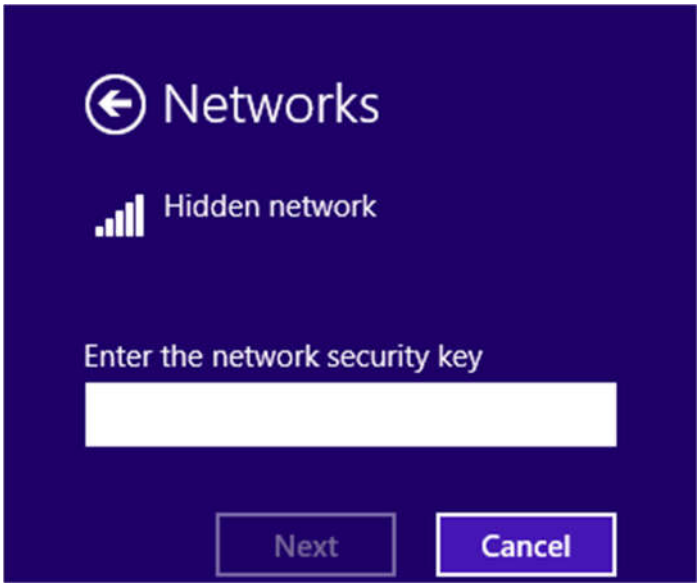
شکل13: انتخاب شبکه وای‌فای پنهان

در پنجره باز شده مطابق شکل14، نام وای‌فای (SSID) خود را وارد نمایید. توجه داشته باشید نام وای‌فای به حروف کوچک و بزرگ حساس است.



شکل14: محل وارد کردن نام وای‌فای (SSID)

و در پنجره باز شده مانند شکل15، رمز وای‌فای خود را وارد نمایید.

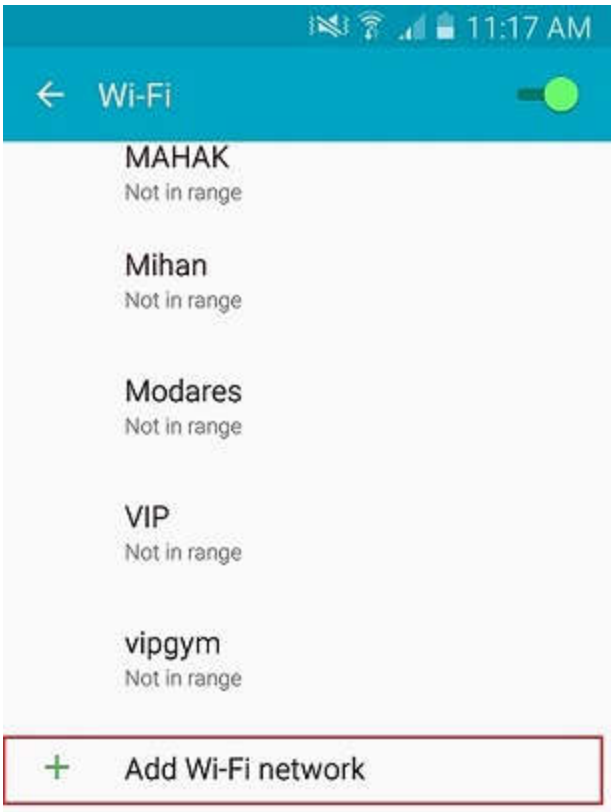


شکل15: محل وارد کردن پسورد وای‌فای (SSID)

بعد از زدن Next تلفن هوشمند شما به شبکه وای‌فای وصل می‌شود.

2-1-4-3- اتصال به شبکه وای‌فای پنهان شده در اندروید

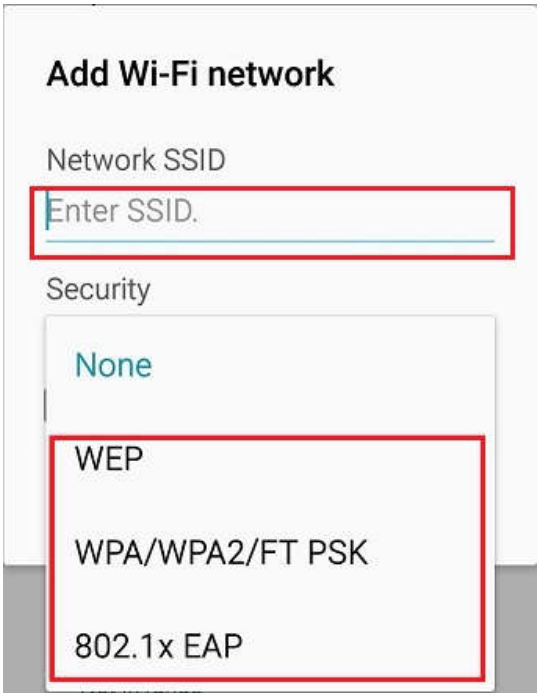
ابتدا به قسمت تنظیمات وای‌فای گوشی رفته و مطابق با شکل15 گزینه اضافه نمودن شبکه وای‌فای (Add Wi-Fi network) را انتخاب نمایید.



شکل16: محل انتخاب شبکه وای‌فای پنهان شده

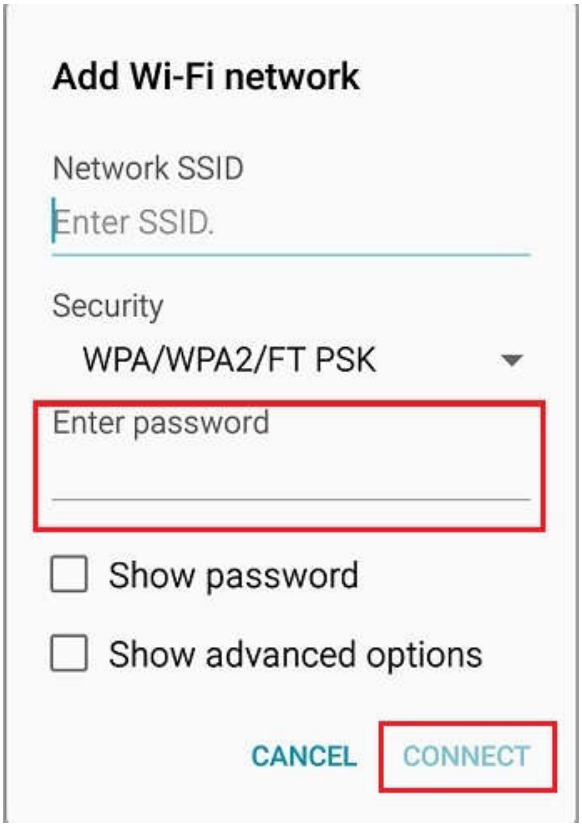
در قست Network SSID مانند شکل17 نام شبکه وای‌فای (SSID) را وارد نمایید. دقت کنید که SSID به حروف کوچک و بزرگ حساس است.

روی گزینه Security مانند شکل17 کلیک نموده و از لیست کشویی باز شده روش اعتبار سنجی شبکه رو انتخاب کنید (با توجه به نوع امنیتی که برای مودم خود تعیین کردید).



شکل17: محل وارد کردن نام وای‌فای (SSID) و انتخاب روش اعتبارسنجی

در قسمت Enter password مانند شکل18 رمز وای‌فای خود را وارد نمایید. پس از کلیک روی Connect به اینترنت وصل می‌شوید.



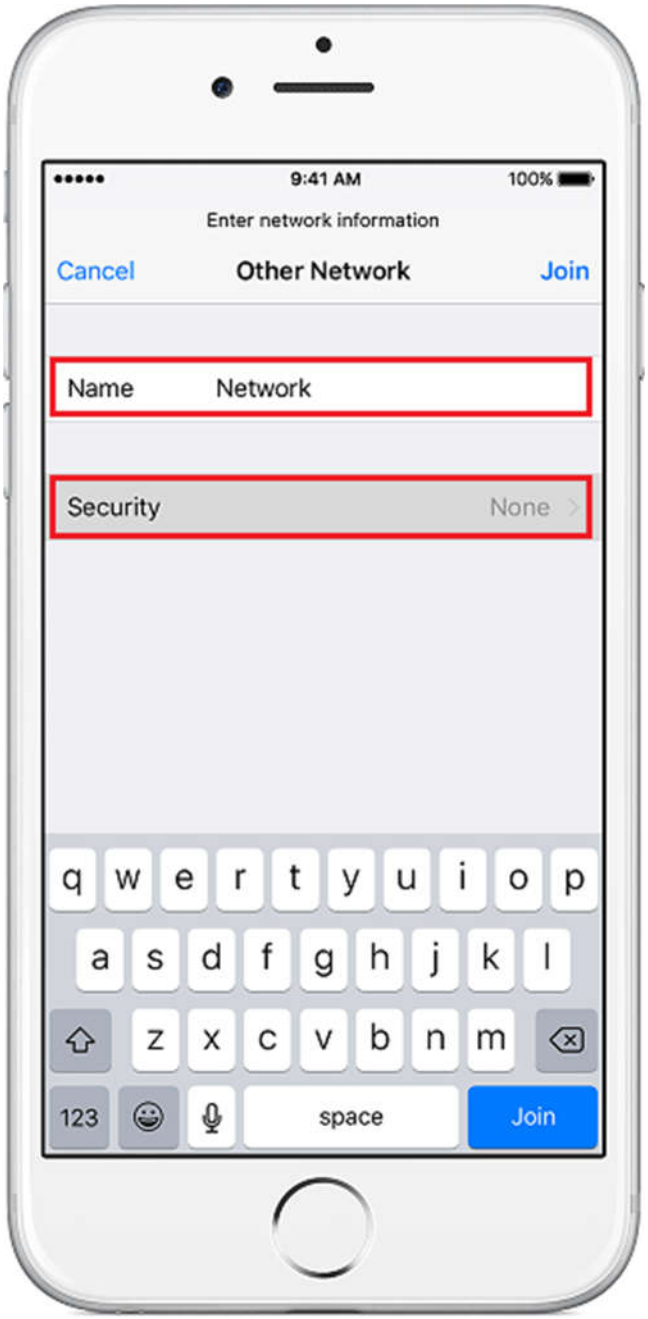
شکل18: محل وارد کردن پسورد وای‌فای (SSID)

3-1-4-3- اتصال به شبکه وای‌فای پنهان شده در IOS

در منوی Settings بخش Wi-Fi گزینه Other… را مطابق شکل19 انتخاب نمایید. اگر Wi-Fi خاموش است آن را فعال کنید.

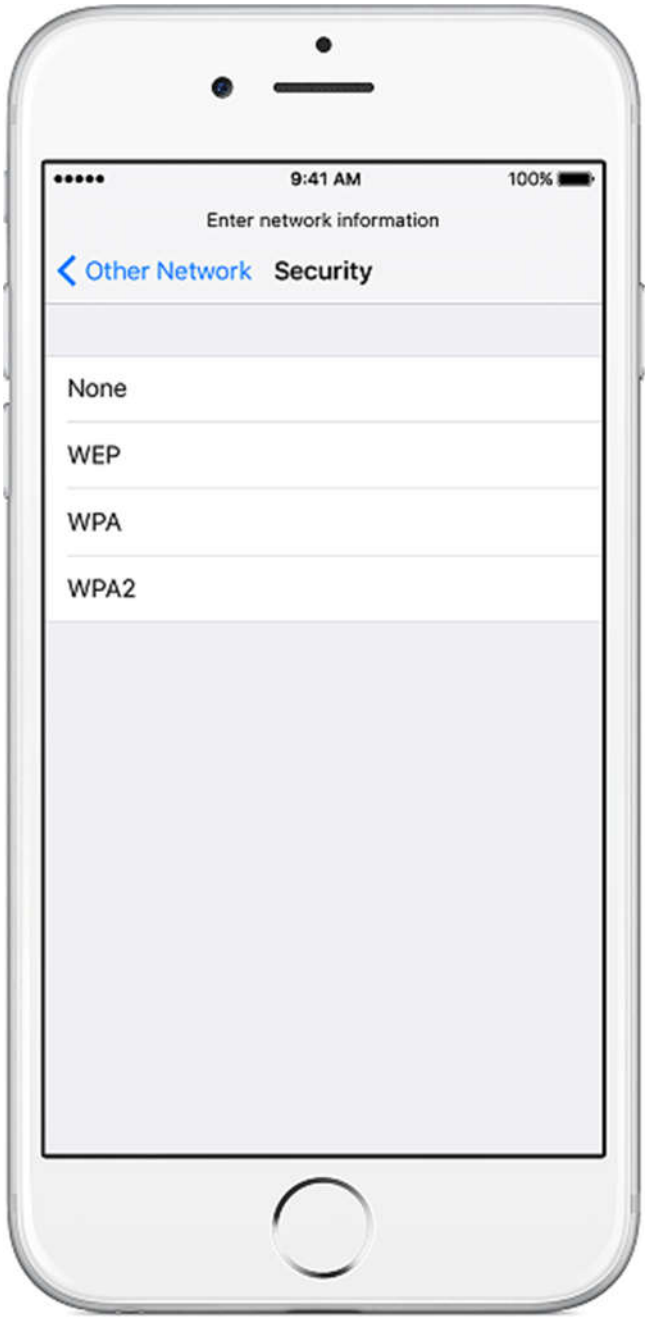
شکل19: صفحه تنظیمات وای‌فای

در پنجره ی باز شده مطابق شکل20 نام شبکه‌ی مورد نظر را وارد و تنظیمات Security را انتخاب نمایید.



شکل20: صفحه وارد نمودن نام شبکه وای‌فای

روش اعتبارسنجی موردنظر خود را مطابق شکل21 انتخاب نمایید. پیشنهاد می‌شود از WPA2 به دلیل امنیت بیشتر در مقایسه با سایر روش‌ها استفاده شود.



شکل21: صفحه انتخاب روش اعتبارسنجی

در صفحه باز شده مطابق شکل22، پسورد شبکه وای‌فای خود را وارد سپس Join را انتخاب نمایید.

شکل22: صفحه وارد نمودن پسورد

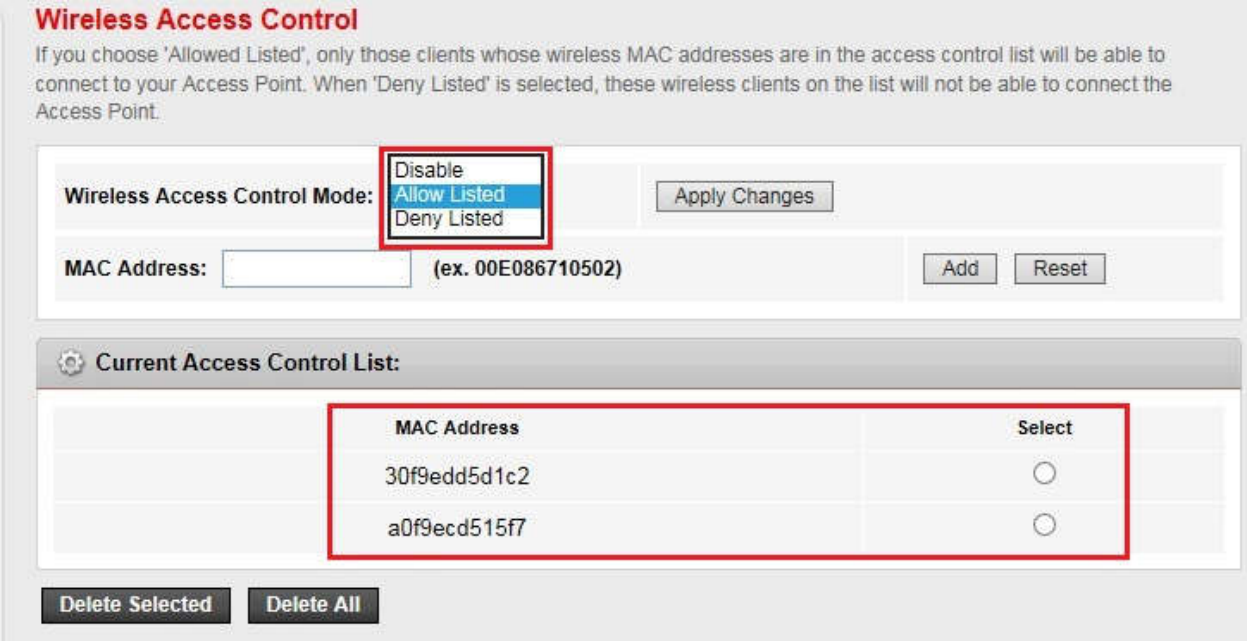
5-3- فیلتر کردن آدرس مک (مرحله پنجم)

همه دستگاه‌ها از جمله لپ‌تاپ، کامپیوتر، تلفن همراه و تبلت دارای یک آدرس منحصر به فرد به نام آدرس مک (Mac Address) هستند (این هیچ ربطی به مک اپل ندارد). از این رو برای ایجاد امنیت بیشتر می‌توانید آدرس مک دستگاه‌هایی که می‌خواهید به وای‌فای وصل شوند را در صفحه تنظیمات مودم خود وارد کنید به طوری که تنها دستگاه‌های مشخص شده بتوانند به شبکه وای‌فای شما متصل شوند.

فیلتر کردن آدرس‌های MAC دستگاه‌ها یک اقدام امنیتی بسیار خوب است چرا که هر دستگاه با آدرس منحصر به فرد اجازه‌ی اتصال به شبکه وایرلس را دارد و هکر تنها با دانستن و جعل کردن آدرس مک دستگاه شما می‌تواند از وای‌فای شما استفاده کند. برای اینکه بتوانید از اتصال هکر به شبکه وای‌فای خود جلوگیری کنید ، می‌بایست آدرس مک هکر را فیلتر کنید. حتما قبل از این کار از مهاجم بودن آدرس مک فرد مورد نظر اطمینان حاصل کنید.

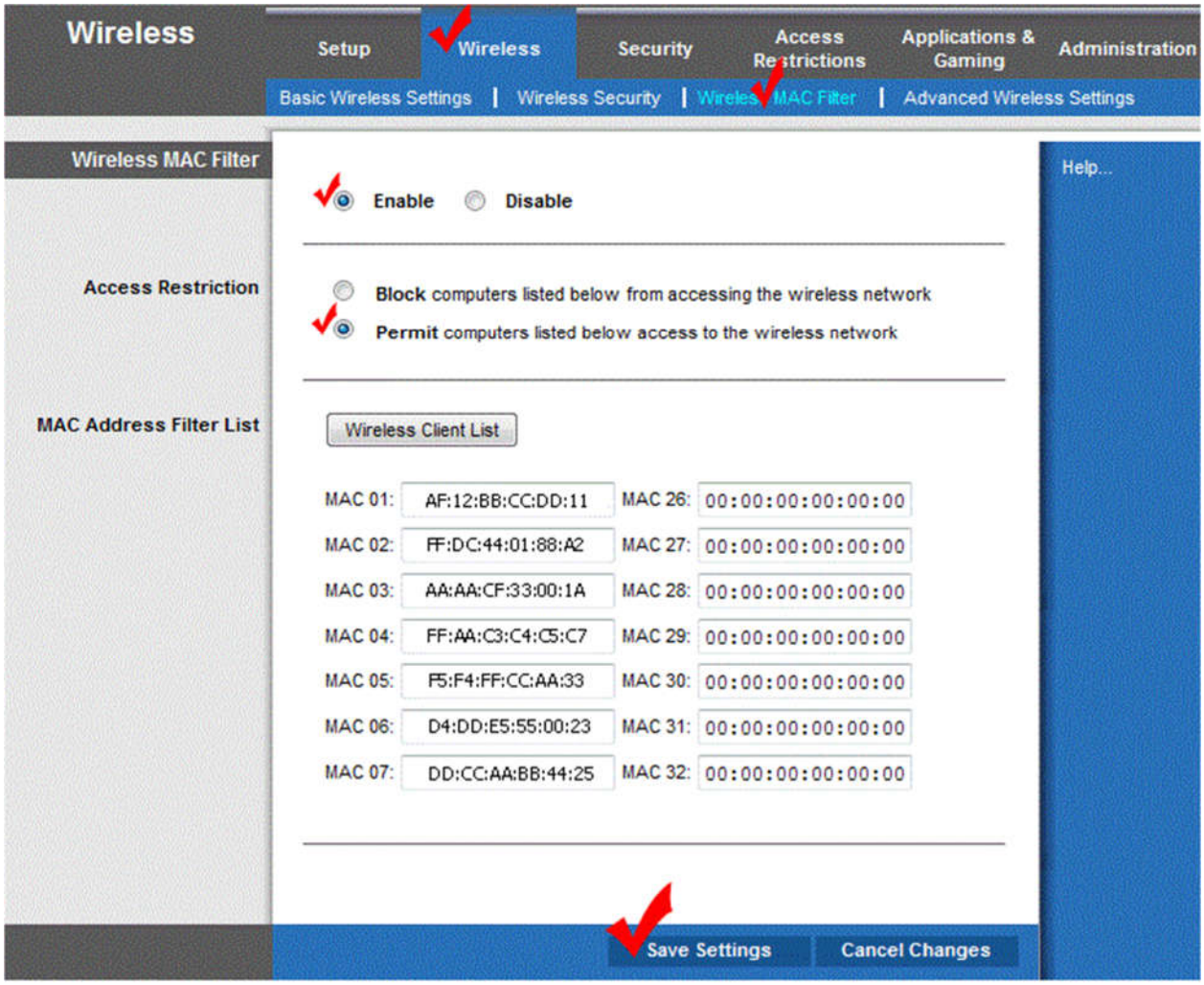
مک آدرس یک دستگاه می‌توان در قسمت تنظیمات شبکه آن مشاهده کرد. کاربرد این ویژگی زمانی است که بخواهید علاوه بر رمز اتصال به مودم، امنیت شبکه بالاتری را نیز اعمال کنید تا تنها کاربرانی که مک آدرس آنها در مودم تعریف شده است اجازه‌ی دسترسی به اینترنت را داشته باشند و یا اینکه کاربران خاصی را فیلتر کنید. همچنین کاربرد دیگر این ویژگی در محدود کردن تعداد کاربران متصل به یک مودم است. مودم‌های خانگی معمولاً بین ۱۰- ۱۵ کاربر را پشتیبانی می‌کنند و هنگامی که بیش از این تعداد کاربر به آن ها متصل شود دچار مشکل شده و کاربران به طور تصادفی قطع خواهند شد. راه حل مورد استفاده در این مواقع اضافه کردن یک مودم دیگر است اما در این حالت نیز به دلیل عدم توزیع یکسان کاربران بین ۲ مودم باز هم امکان وقوع مشکل ذکر شده وجود دارد. در اینجا نیز با تقسیم کاربران بر روی مودم ها به کمک مک فیلترینگ، می توان از بروز این مشکل جلوگیری کرد.

مک‌های مورد نظرتان را کپی کرده و سپس مطابق شکل 23 به قسمت Wireless Mac Filtering در قسمت Wireless یا Network بروید. در این قسمت اگر Allow یا Permit را انتخاب کنید، کاربرانی که مک آدرس آن‌ها را اضافه می کنید مجاز به استفاده از مودم خواهند بود و در صورت انتخاب Deny، کاربران اضافه شده اجازه‌ی استفاده از مودم را نخواهد داشت. پس از انتخاب یکی از این دو گزینه، با کلیک بر روی Add New ، مک آدرس مورد نظر را کپی کنید.



شکل23: صفحه تنظیمات Mac Filtering

نکته: در بعضی مودم‌ها همانند شکل24 در قسمت Setup و سپس WLAN رفته و در قسمت Wireless Control List آدرس‌های مک مورد نظر خود را وارد نموده و سپس Allow را انتخاب نمایید.



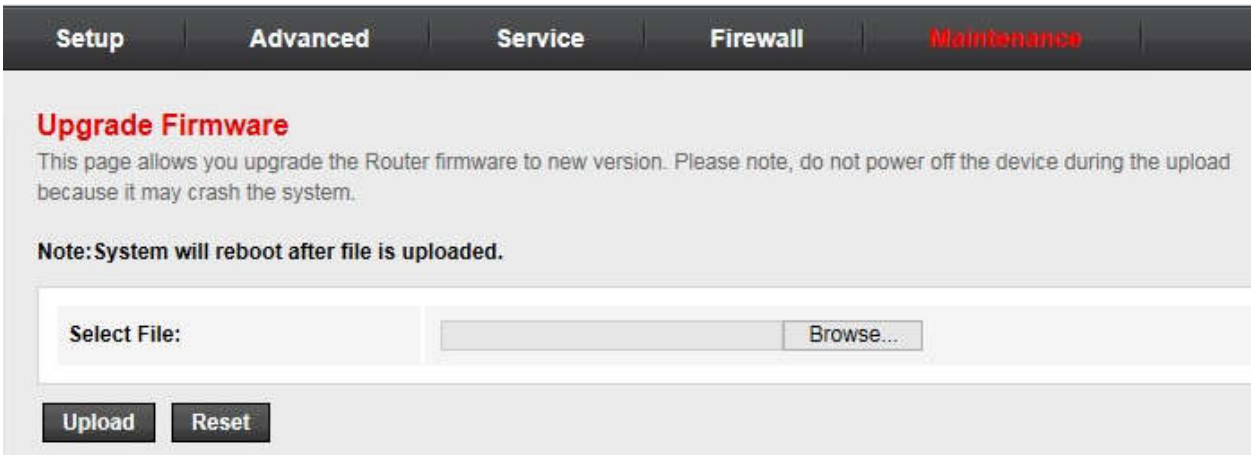
شکل24: صفحه تنظیمات Mac Filtering

6-3- بروزسانی فریم ویر (firmware) مودم (مرحله ششم)

پیشنهاد می‌شود همواره وب سایت سازنده مودم را چک کرده و از بروز بودن فریم ویر مودم خود اطمینان کسب کنید. فریم ویرهای جدید از امنیت بیشتری برخوردارند. به دلیل اینکه در نسخه‌های جدیدتر مشکلات امنیتی نسخه‌های پیشین حل شده است. برای دیدن نسخه فریم‌ویر فعلی مودم وارد صفحه تنظیمات مودم شده و مطابق با شکل25 در منوی Status و در قسمت Firmware Version قادر خواهید بود نسخه فریم ویر مودم خود را مشاهده کنید.

شکل25: محل رویت نسخه فریم‌ویر

برای به‌روز رسانی فریم ویر مودم خود وارد منوی Maintenance و بخش Upgrade Firmware مودم شده و فایل فریم ور از قسمت Browse انتخاب و سپس بر روی Upload کلیک نمایید.



شکل26: صفحه به‌روز رسانی فریم‌ویر

3-7- چک کردن افراد استفاده کننده از وای فای (مرحله هفتم)

اگر شما نگران هستید که فرد یا افرادی در حال استفاده غیرمجاز از شبکه وای فای شما است و می‌خواهید از این موضوع اطمینان حاصل نمایید، می‌توانید وارد صفحه تنظیمات مودم شده و به بخش (DHCP Clients (Status > Local Network مراجعه کنید. در این قسمت شما میتوانید نام کامپیوترها و دستگاه های بی سیمی که در حال استفاده از وای فای شما هستند را مشاهده نمایید.

3-8- غیر فعال کردنWPS (مرحله هشتم)

یکی دیگر از اقدامتی که می‌توانید برای جلوگیری از هک وای‌فای مودم انجام دهید خاموش یا غیر فعال کردن کلید و امکان WPS در مودم است. WPS یا همان Wi-Fi Protected Setup استاندارد نه چندان مطمئنی در مودم ها است که به کاربران اجازه می‌دهد بدون استفاده از رمز عبور مطمئن، از پین هشت رقمی مودم یا فعال کردن دکمه WPS به شبکه وای‌فای متصل شوند، استفاده از این قابلیت خطراتی را نیز به دنبال دارد و هکرها می‌توانند با استفاده از روش‌های مختلف مانند بروت فورس و... به سادگی امنیت شبکه وای‌فای شما را دور بزنند.

پیشنهاد می‌شود اگر دکمه WPS بر روی مودم شما قرار دارد حتما آن را غیرفعال نمایید و همچنین وارد تنظیمات مودم خود شده و از بخش مربوط به تنظیمات WPS همانند شکل27، این قابلیت را غیرفعال نمایید.

شکل27: صفحه تنظیمات WPS

3-9- غیر فعال کردن وای فای هنگام خروج از خانه (مرحله نهم)

اگر از وای‌فای خانه و یا محل کارتان استفاده می‌کنید فراموش نکنید که هنگام خروج از محل، وای‌فای مودم را قطع و یا در صورتی که برای مدتی طولانی در آنجا حضور ندارید مودم را خاموش نمایید. با اینکار هکرها تحت هیچ شرایطی نمی-توانند به مودم شما دسترسی داشته باشند.

4- نکات ایمنی استفاده از وای‌فای‌های عمومی

ممکن است شما به یک فروشگاه، فرودگاه، مرکز تفریحی و ... بروید و متوجه شوید که در آنجا وای‌فای رایگان و آزاد در دسترس شماست. توجه داشته باشید اگر نکات امنیتی را رعایت نکنید ممکن است به راحتی اطلاعات خصوصی خود را در وای‌فای‌های عمومی در اختیار افراد سودجو قرار دهید. رعایت نکات زیر می تواند امنیت شما را در شبکه‌های وای‌فای عمومی بهبود بخشد:

- قابلیت اشتراک گذاری فایل را غیرفعال نمایید
- نرم‌افزار ضدویروس به روز رسانی شده نصب و فعال نمایید
- دیوار آتش (Firewall) سیستم خود را فعال نمایید
- از پروتکل امن SSL استفاده کنید
- در صورت امکان از وی پی ان (VPN) استفاده کنید

- برنامه های خود را به روز نگه دارید

5- تفاوت میان وای‌فای عمومی و وای‌فای به اشتراک گذاشته شده

دانستن تفاوت میان این دو شبکه می‌تواند کمک زیادی به امنیت کاربران نماید. برخی شبکه‌های وای‌فای عمومی برای کاربران مهمان حساب کاربری و رمز عبور تعریف می‌کنند. این نوع شبکه‌ها در مقایسه با وای‌فای عمومی باز، قابل اعتمادتر و مطمئن‌تر هستند و یک مرحله احراز هویت دارند که باعث می‌شود از دسترسی‌های غیرمجاز جلوگیری شود. معمولاً وای‌فای عمومی کتابخانه‌ها این‌گونه هستند و دسترسی آزاد به وای‌فای ندارند. بنابراین اگر در مراکز عمومی بتوانید به وای‌فای مدیریت‌شده و محافظت‌شده دسترسی پیدا کنید، بهتر از وای‌فای عمومی بدون رمز عبور است.

استفاده از نرم‌افزارهای امنیتی

کارشناسان حوزه امنیت اطلاعات توصیه می‌کنند هنگامی به شبکه وای‌فای عمومی متصل شوید که مطمئن باشید نرم‌افزارهای امنیتی روی دستگاه شما نصب و فعال است. نرم‌افزارهای امنیتی مانند ضدویروس، ضدتروجان، ضدبدافزار، دیوار آتش و دیگر نرم‌افزارهای امنیتی که شرکت های معتبر برای پلتفرم‌های موبایل ارائه می‌دهند، ارتباطات و اطلاعات ورودی- خروجی دستگاه را بررسی می‌کنند و می‌توانند جلوی برخی سوءاستفاده‌ها از رخنه‌ها یا حملات علیه دستگاه را بگیرند. کارشناسان می‌گویند هر دستگاه موبایل یا دسکتاپی حداقل باید یک ضدویروس به همراه یک دیوار آتش داشته باشد. همچنین، مطمئن شوید که نرم‌افزار امنیتی دستگاه شما قبل از اتصال به وای‌فای عمومی، به‌روزرسانی شده است. استفاده از نرم‌افزار امنیتی به‌منزله امنیت کامل در وای‌فای عمومی نیست و به شدت توصیه می‌شود از کارهای مالی و حساس جلوگیری شود، اما بزرگ‌ترین فایده‌شان سخت‌تر کردن روند نفوذ و هک دستگاه است.

از شبکه های عمومی برای نقل و انتقال مهم استفاده نکنید

از شبکه های عمومی برای نقل و انتقال مهم مانند انجام تراکنش‌های بانکی، امور مالی، دسترسی به پست الکترونیکی و ... استفاده نکنید. برای انجام چنین اموری بهتر است تا رسیدن به یک نقطه امن برای اتصال به اینترنت صبر نمایید.