

فهرست مطالب

صفحه	عنوان
1	1- وای فای (Wi-Fi) چیست؟.....
1	2- چرا امنیت شبکه وای فای مهم است؟.....
1	3- مراحل امن سازی وای فای مودم.....
1	3-1- ایجاد یک پسورد اختصاصی برای مودم (مرحل اول).....
4	3-2- فعال کردن رمزعبور وای فای (مرحله دوم).....
5	3-3- تغییر نام شبکه وای فای یا SSID (مرحله سوم).....
6	3-4- پنهان سازی شبکه وای فای یا SSID (مرحله چهارم).....
8	3-4-1- روش اتصال به شبکه‌های پنهان شده.....
18	3-4-1-1- اتصال به شبکه وای فای پنهان شده در ویندوز.....
10	3-4-1-2- اتصال به شبکه وای فای پنهان شده در اندروید.....
13	3-4-1-3- اتصال به شبکه وای فای پنهان شده در IOS.....
17	3-5- فیلتر کردن آدرس مک (مرحله پنجم).....
19	3-6- بروزرسانی فریم ویر (firmware) مودم (مرحله ششم).....
20	3-7- چک کردن افراد استفاده کننده از وای فای (مرحله هفتم).....
20	3-8- غیر فعال کردن WPS (مرحله هشتم).....
21	3-9- غیر فعال کردن وای فای هنگام خروج از خانه (مرحله نهم).....
21	4- نکات ایمنی استفاده از وای فای‌های عمومی.....
22	5- تفاوت وای فای عمومی و وای فای اشتراک گذاری شده.....

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 می‌شود 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:

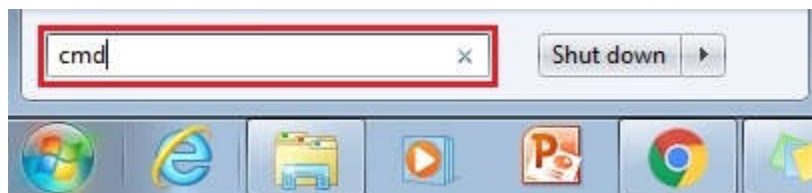
- مصرف حجم اینترنت به صورت غیر عادی افزایش پیدا خواهد کرد و در نتیجه هزینه دریافت خدمات اینترنتی نیز برای شما افزایش می‌یابد.
- سرعت اینترنت شما کاهش می‌یابد.
- در صورت هک شدن وای‌فای در واقع در معرض یک خطر امنیتی قرار گرفته‌اید که امکان دارد هکر از این طریق به کامپیوتر شما نیز نفوذ کرده و به فایل‌های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

3- مراحل امن سازی وای‌فای مودم

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

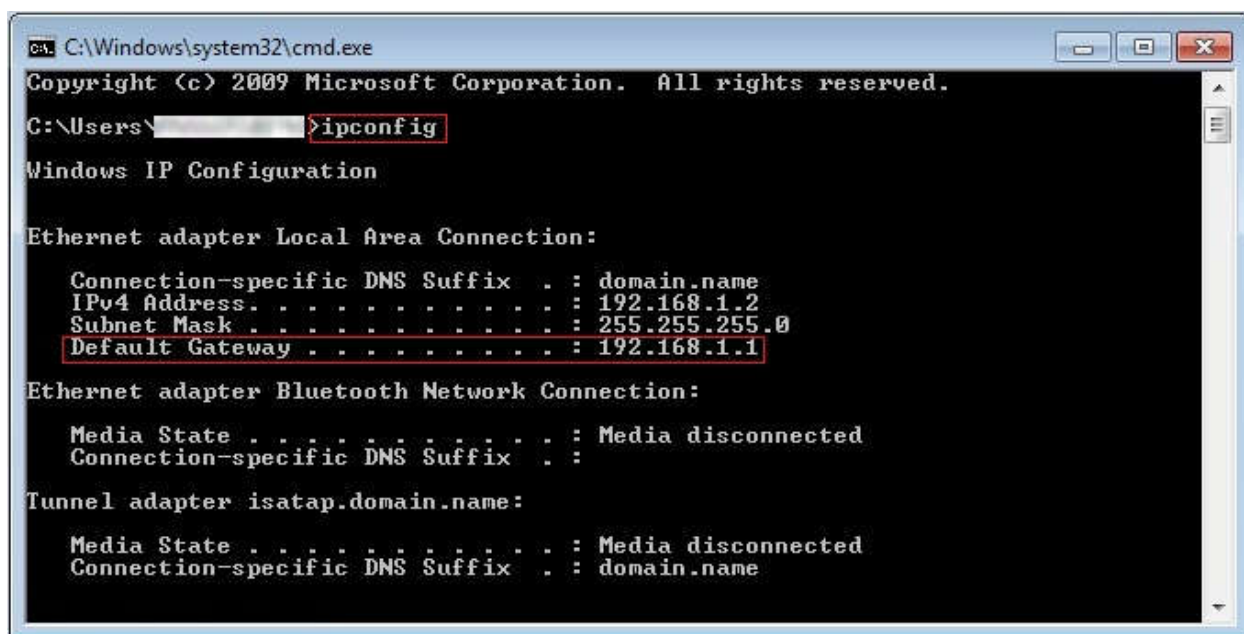
تولیدکنندگان مودم‌های ADSL، صفحات وبی را برای راه‌اندازی و پیکربندی این تجهیزات در اختیار کاربران قرار داده‌اند. این ابزارهای وب با یک صفحه Login (با نام کاربری و کلمه عبور) محافظت می‌شوند تا فقط دارندگان قانونی مودم بتوانند به این تنظیمات دسترسی داشته باشند. با این حال، اطلاعات Login پیش‌فرض بیشتر تجهیزات شبکه بسیار ساده بوده (معمولاً admin و admin است هم برای نام کاربری و رمزعبور) و هک‌های 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 وای‌فای 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 شکل 1، عبارت CMD را نوشته سپس در قسمت نتایج جستجو CMD را انتخاب نمایید.



شکل 1: اجرای برنامه خط فرمان

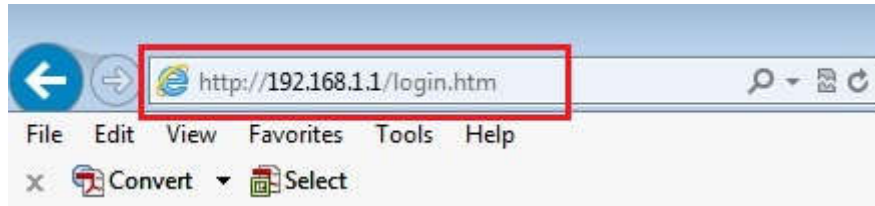
پس از اینکه CMD اجرا شد یک پنجره سیاه رنگ مطابق شکل 2 نمایش داده می‌شود در این قسمت دستور ipconfig را نوشته کلید Enter را بزنید.



شکل 2: اجرای دستور ipconfig

عدد نوشته شده روبروی Default Gateway که IP مودم شما می‌باشد را کپی کرده و مطابق شکل 3 در آدرس بار مرورگر خود Paste نموده و کلید Enter را بزنید.

نکته: آدرس IP، نام کاربری و رمز عبور بر روی جعبه‌ی تمامی مودم‌ها 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 مرورگر خود کپی نمایید.



شکل 3: روش دسترسی به تنظیمات مودم

در پنجره نمایش داده شده مانند شکل 4، نام کاربری و رمزعبور را وارد نماید. به صورت پیش فرض در بیشتر مودمها نام کاربری و رمزعبور Admin می باشد.

شکل 4: 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 شکل 5، رمزعبور را تغییر دهید. اگر اولین بار است که مودم را راه اندازی می کنید در همان صفحه اول، گزینه تغییر رمزعبور برای شما نمایش داده می شود در غیر این صورت می توانید بر روی گزینه Setup در صفحه اول کلیک کرده و در قسمت مربوطه وارد و رمزعبور مودم را تغییر دهید.

User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	<input type="text" value="admin"/>
Privilege:	<input type="text" value="Root"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

شکل 5: صفحه تغییر رمز عبور تنظیمات مودم

2-3- فعال کردن رمزعبور وای فای (مرحله دوم)

برای جلوگیری از هک وای فای 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 وای فای 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 وای فای خود، وارد صفحه تنظیمات مودم و بخش Wireless Security Setup مانند شکل 6 شده روش رمزنگاری موردنظر خود را از قسمت Encryption انتخاب نموده و در قسمت Pre-Shared Key رمز وای فای مطلوب خود را وارد نمایید. بقیه تنظیمات این صفحه را در حالت پیش فرض 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.

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to the wireless network.

SSID TYPE: WPA1 WPA2 WPA3

Encryption: None WEP WPA (TKIP) WPA (AES) WPA2(AES) WPA2(TKIP) WPA2 Mixed

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

Pre-Shared Key Format:

Pre-Shared Key:

Authentication RADIUS Server: Port IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

شکل 6: صفحه تنظیمات امنیتی مودم

نکته: در برخی برندهای مودم به جای WPA2 Mixed گزینه‌های مشخص شده در شکل 7 را انتخاب نمایید.



شکل 7: 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 **Service Set Identifier** بوده و یک مقدار قابل فهم و خواندن برای انسان است که بتواند شبکه‌های مختلف را تشخیص دهد.

اگر می‌خواهید شبکه خانگی وای‌فای خود را امن کنید حتماً 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 شکل 8 یا هنگام راه‌اندازی از قسمت **Setup** اقدام به تغییر نام وای‌فای 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 می‌اندازد.

Wireless Basic Settings

This page is used to configure the parameters for your wireless network.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N) ▾

Mode: ▾

SSID:

Channel Width: 20/40MHZ ▾

Control Sideband: Upper ▾

Channel Number: Auto ▾ Current Channel: 1

Radio Power: 100% ▾

Associated Clients:

شکل 8: صفحه تغییر نام شبکه وای فای یا SSID

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

وارد صفحه تنظیمات مودم شده و در قسمت تنظیمات Wireless مودم همانند شکل 9 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.

Device Info
Advanced Setup
Wireless |
 Basic
 Security
 MAC Filter
 Wireless Bridge
 Advanced
 Station Info
 Diagnostics
 Management

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point ۲

Clients Isolation

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 78:54:2E:73:BD:0A

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	DLink0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	DLink0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	DLink0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

۳

شکل 9: پنهان سازی شبکه وای فای یا SSID

نکته: در برخی برندهای مودم به جای گزینه Hide Access Point برای پنهان سازی شبکه وای فای می بایست گزینه Broadcast SSID را مطابق شکل 10 غیرفعال (Disabled) نمود.

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
DTIM Interval:	<input type="text" value="1"/> (1-255)
Data Rate:	<input type="text" value="Auto"/>
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
Broadcast SSID:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Relay Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Ethernet to Wireless Blocking:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wifi Multicast to Unicast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Apply Changes

شکل 10: پنهان سازی شبکه وای فای

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

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

3-4-1-1- اتصال به شبکه وای فای پنهان شده در ویندوز

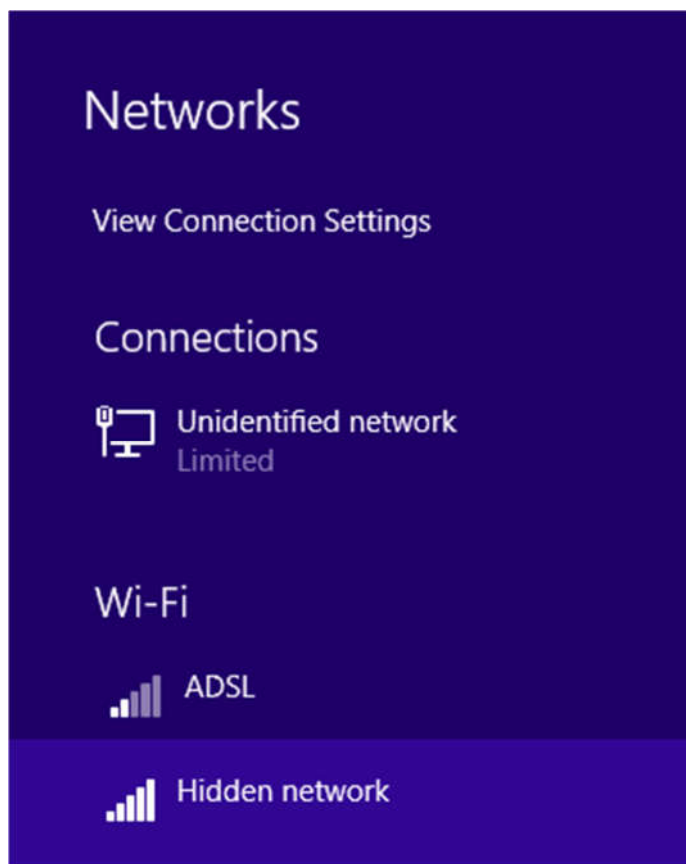
در این قسمت روش اتصال به شبکه وای فای پنهان شده در ویندوز 8 شرح داده شده است. لازم به ذکر است اتصال در نسخه‌های دیگر ویندوز نیز مشابه این روش می‌باشد.

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

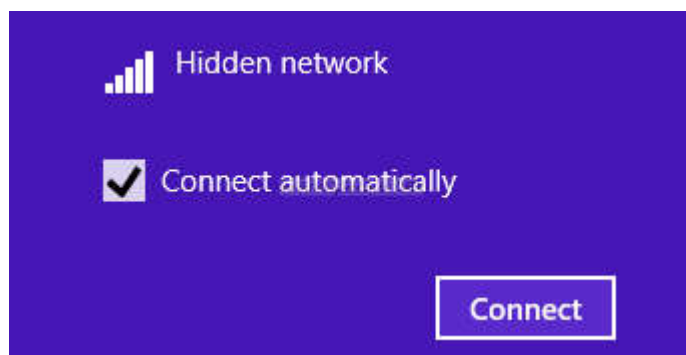


شکل 11: محل علامت وای فای در تسک بار ویندوز

روی Hidden network مطابق شکل 12 و سپس روی Connect مطابق شکل 13 کلیک نمایید.

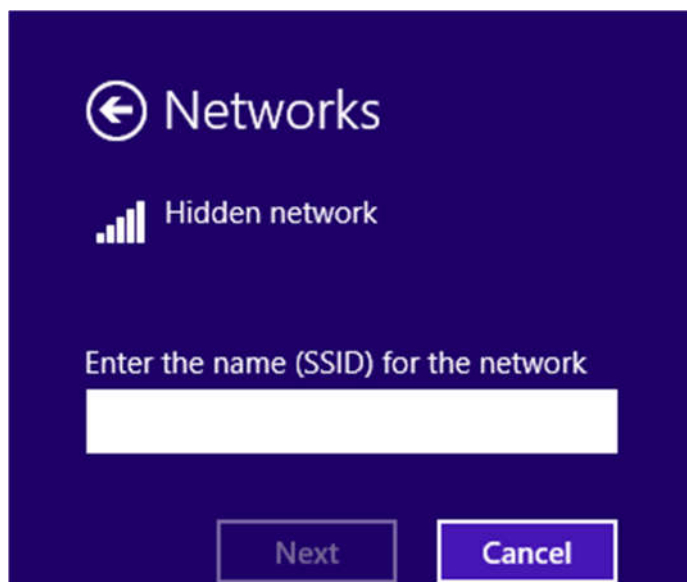


شکل 12: انتخاب شبکه وای فای پنهان



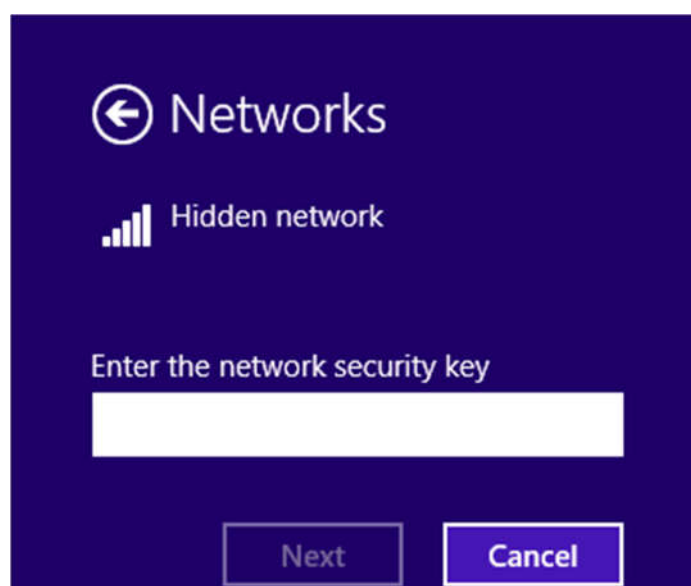
شکل 13: انتخاب شبکه وای فای پنهان

در پنجره باز شده مطابق شکل 14، نام وای فای (SSID) خود را وارد نمایید. توجه داشته باشید نام وای فای به حروف کوچک و بزرگ حساس است.



شکل 14: محل وارد کردن نام وای فای (SSID)

و در پنجره باز شده مانند شکل 15، رمز وای فای خود را وارد نمایید.

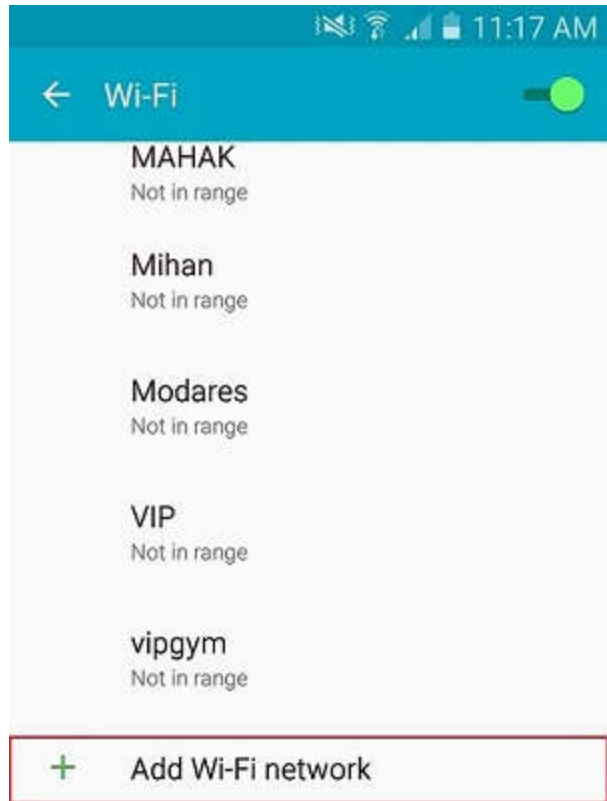


شکل 15: محل وارد کردن پسورد وای فای (SSID)

بعد از زدن Next تلفن هوشمند شما به شبکه وای فای وصل می شود.

2-4-3- اتصال به شبکه وای فای پنهان شده در اندروید

ابتدا به قسمت تنظیمات وای فای گوشی رفته و مطابق با شکل 15 گزینه اضافه نمودن شبکه وای فای (Add Wi-Fi network) را انتخاب نمایید.



شکل 16: محل انتخاب شبکه وای فای پنهان شده

در قسمت Network SSID مانند شکل 17 نام شبکه وای فای (SSID) را وارد نمایید. دقت کنید که SSID به حروف کوچک و بزرگ حساس است.

روی گزینه Security مانند شکل 17 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).

Add Wi-Fi network

Network SSID

Enter SSID.

Security

None

WEP

WPA/WPA2/FT PSK

802.1x EAP

شکل 17: محل وارد کردن نام وای فای (SSID) و انتخاب روش اعتبارسنجی

در قسمت Enter password مانند شکل 18 رمز وای فای خود را وارد نمایید. پس از کلیک روی Connect به اینترنت وصل می شوید.

Add Wi-Fi network

Network SSID
Enter SSID.

Security
WPA/WPA2/FT PSK

Enter password

Show password

Show advanced options

CANCEL CONNECT

شکل 18: محل وارد کردن پسورد وای فای (SSID)

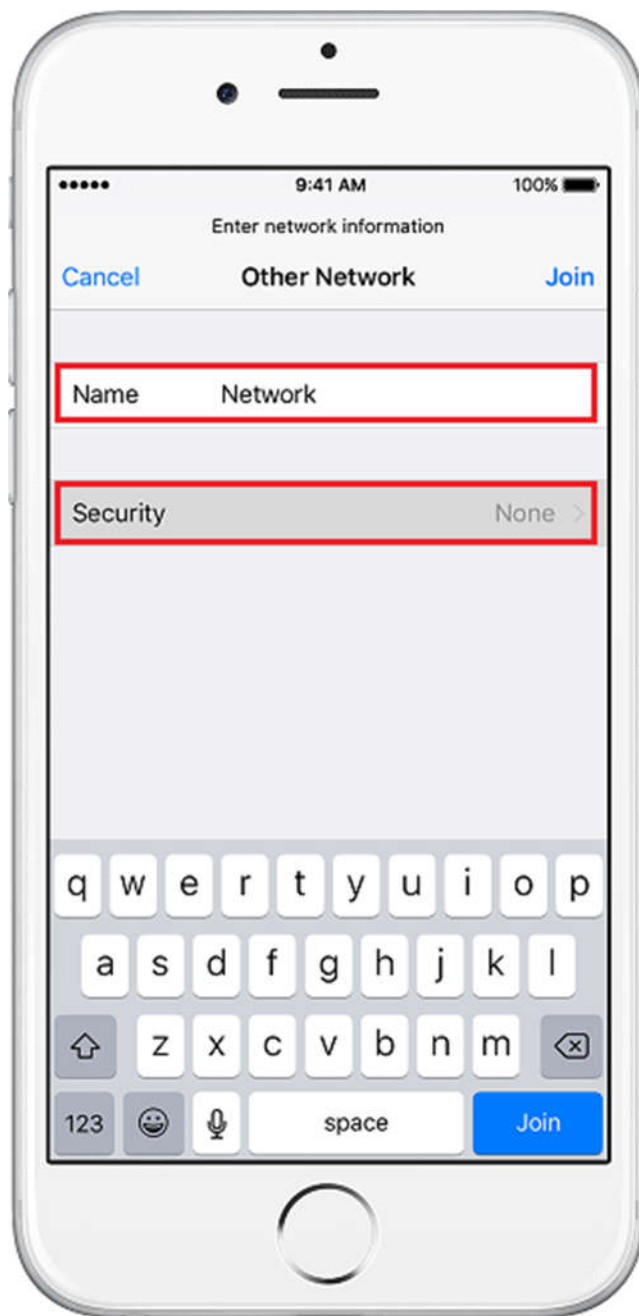
3-4-1-3- اتصال به شبکه وای فای پنهان شده در IOS

در منوی Settings بخش Wi-Fi گزینه Other... را مطابق شکل 19 انتخاب نمایید. اگر Wi-Fi خاموش است آن را فعال کنید.



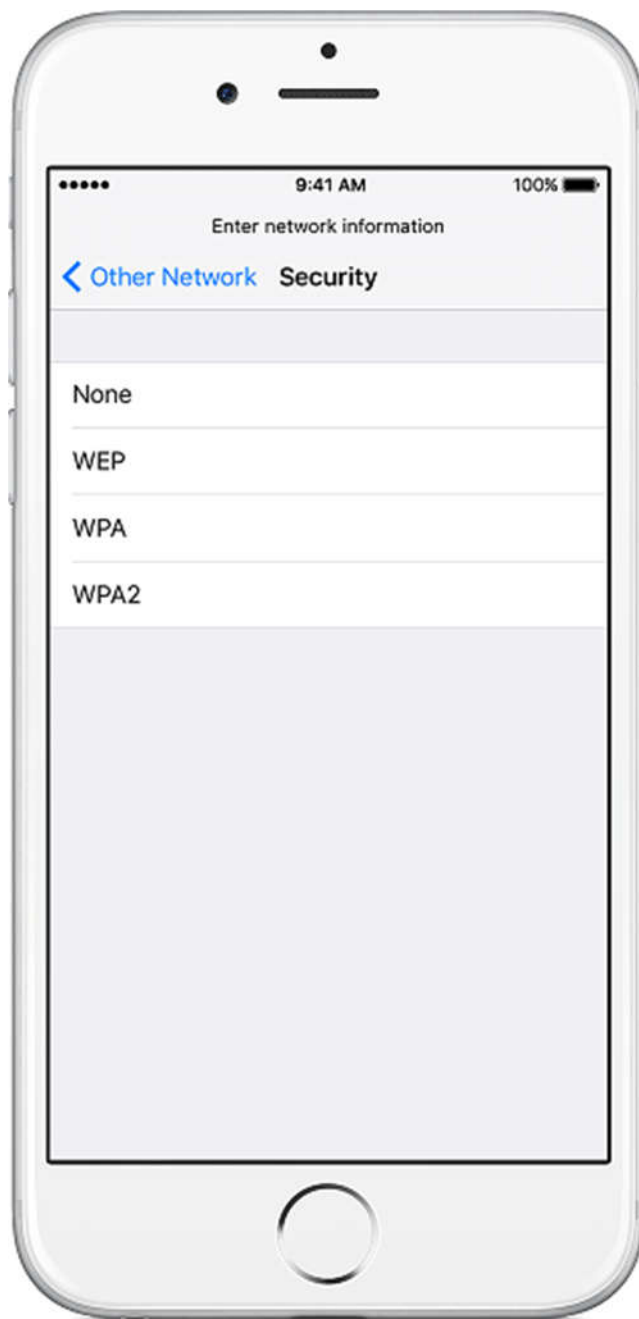
شکل 19: صفحه تنظیمات وای فای

در پنجره ی باز شده مطابق شکل 20 نام شبکه‌ی مورد نظر را وارد و تنظیمات Security را انتخاب نمایید.



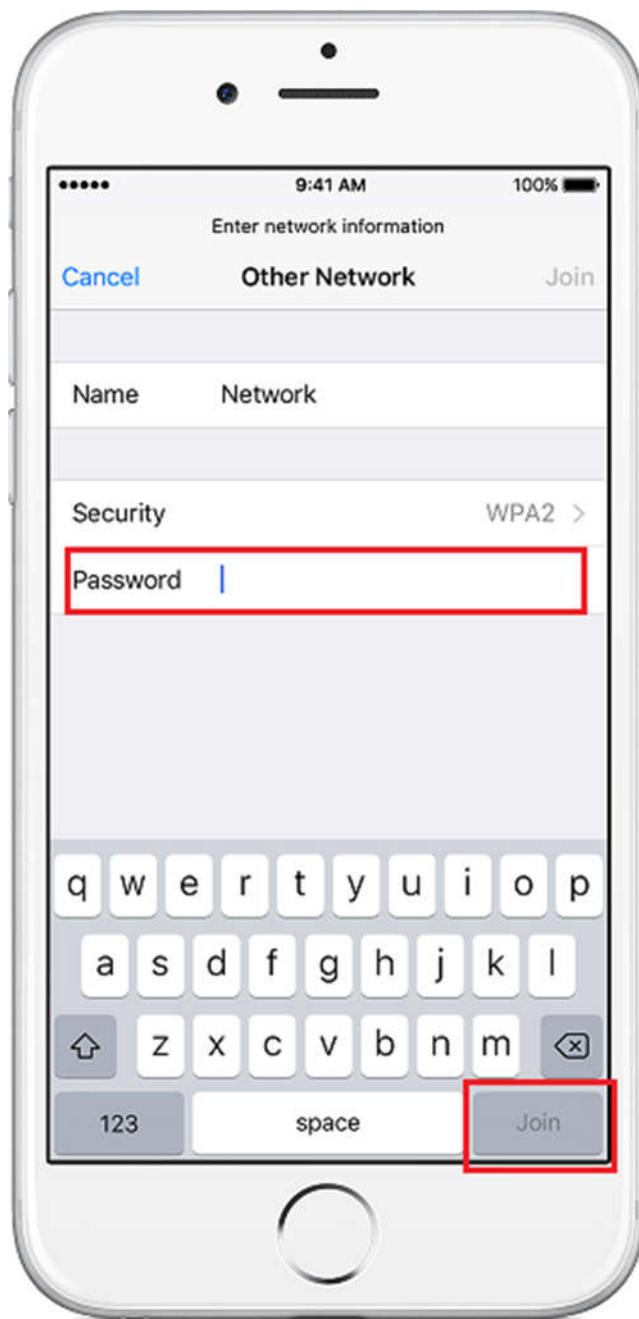
شکل 20: صفحه وارد نمودن نام شبکه وای فای

روش اعتبارسنجی موردنظر خود را مطابق شکل 21 انتخاب نمایید. پیشنهاد می شود از WPA2 به دلیل امنیت بیشتر در مقایسه با سایر روش ها استفاده شود.



شکل 21: صفحه انتخاب روش اعتبارسنجی

در صفحه باز شده مطابق شکل 22، پسورد شبکه وای فای خود را وارد سپس Join را انتخاب نمایید.



شکل 22: 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. حتماً 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 آن‌ها 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 مودم‌ها به کمک مک فیلترینگ، می‌توان 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 Network بروید. در این قسمت اگر Allow یا Permit را انتخاب کنید، کاربرانی که مک آدرس آن‌ها را اضافه می‌کنید 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.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable **Allow Listed** Deny Listed Apply Changes

MAC Address: (ex. 00E086710502) Add Reset

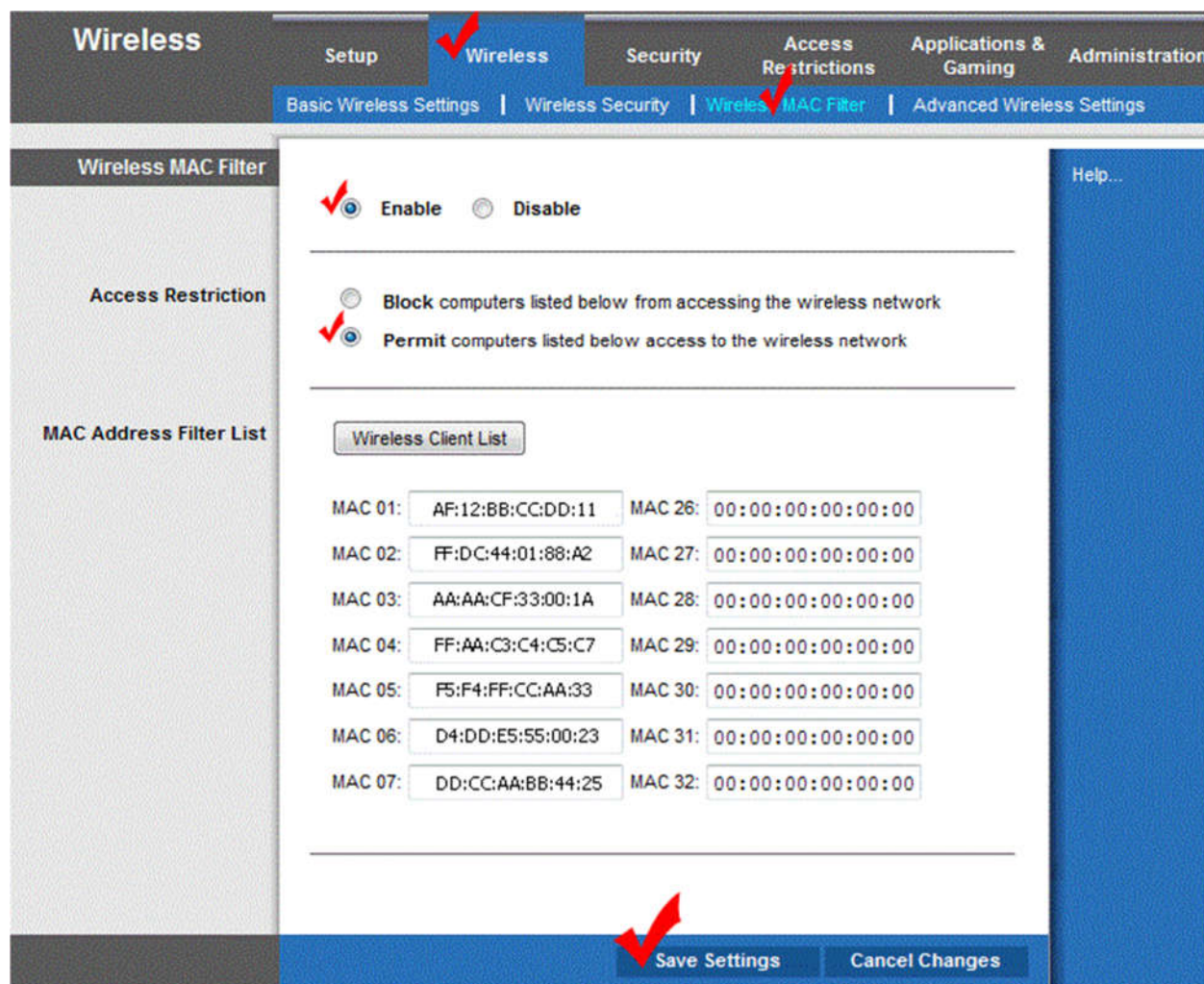
Current Access Control List:

MAC Address	Select
30f9edd5d1c2	<input type="radio"/>
a0f9ecd515f7	<input type="radio"/>

Delete Selected Delete All

شکل 23: صفحه تنظیمات Mac Filtering

نکته: در بعضی مودم‌ها همانند شکل 24 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.



شکل 24: صفحه تنظیمات Mac Filtering

6-3- بروزرسانی 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 شکل 25 در منوی Status و در قسمت Firmware Version قادر خواهید بود نسخه فریم ویر مودم خود را مشاهده کنید.

ADSL Router Status
This page shows the current status and some basic settings of the device.

System	
Alias Name	RTL867x ADSL Modem
Uptime	0 0:48:15
Date/Time	Sun Jan 1 0:48:15 2012
Firmware Version	RTK V2.2.1
Built Date	Oct 31 2014 15:22:49
Serial Number	000EF4FD0748

شکل 25: محل رویت نسخه فریم‌ویر

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

Upgrade Firmware
This page allows you upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Note: System will reboot after file is uploaded.

Select File:

شکل 26: 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 (Status > Local DHCP Clients) Network مراجعه کنید. در این قسمت شما می‌توانید نام کامپیوترها و دستگاه‌های بی‌سیم که در حال استفاده از وای فای شما هستند را مشاهده نمایید.

3-8- غیر فعال کردن WPS (مرحله هشتم)

یکی دیگر از اقداماتی 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 مودم‌ها است که به کاربران اجازه می‌دهد بدون استفاده از رمز عبور مطمئن، از بین هشت رقمی مودم یا فعال کردن دکمه WPS به شبکه وای‌فای متصل شوند، استفاده از این قابلیت خطرانی 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 حتماً آن را غیرفعال نمایید و همچنین وارد تنظیمات مودم خود شده و از بخش مربوط به تنظیمات WPS همانند شکل 27، این قابلیت را غیرفعال نمایید.



شکل 27: صفحه تنظیمات WPS

3-9- غیر فعال کردن وای‌فای 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 نمی‌توانند 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 می‌تواند 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 وای فای عمومی و وای فای به اشتراک گذاشته شده

دانستن تفاوت میان این دو شبکه می تواند کمک زیادی به امنیت کاربران نماید. برخی شبکه های وای فای عمومی برای کاربران مهمان حساب کاربری و رمز عبور تعریف می کنند. این نوع شبکه ها در مقایسه با وای فای عمومی باز، قابل اعتمادتر و مطمئن تر هستند و یک مرحله احراز هویت دارند که باعث می شود از دسترسی های غیرمجاز جلوگیری شود. معمولاً وای فای عمومی کتابخانه ها این گونه هستند و دسترسی آزاد به وای فای ندارند. بنابراین اگر در مراکز عمومی بتوانید به وای فای مدیریت شده و محافظت شده دسترسی پیدا کنید، بهتر از وای فای عمومی بدون رمز عبور است.

استفاده از نرم افزارهای امنیتی

کارشناسان حوزه امنیت اطلاعات توصیه می کنند هنگامی به شبکه وای فای عمومی متصل شوید که مطمئن باشید نرم افزارهای امنیتی روی دستگاه شما نصب و فعال است. نرم افزارهای امنیتی مانند ضد ویروس، ضد تروجان، ضد بد افزار، دیوار آتش و دیگر نرم افزارهای امنیتی که شرکت های معتبر برای پلتفرم های موبایل ارائه می دهند، ارتباطات و اطلاعات ورودی - خروجی دستگاه را بررسی می کنند و می توانند جلوی برخی سوء استفاده ها از رخنه ها یا حملات علیه دستگاه را بگیرند. کارشناسان می گویند هر دستگاه موبایل یا دسکتاپی حداقل باید یک ضد ویروس به همراه یک دیوار آتش داشته باشد. همچنین، مطمئن شوید که نرم افزار امنیتی دستگاه شما قبل از اتصال به وای فای عمومی، به روزرسانی شده است. استفاده از نرم افزار امنیتی به منزله امنیت کامل در وای فای عمومی نیست و به شدت توصیه می شود از کارهای مالی و حساس جلوگیری شود، اما بزرگ ترین فایده شان سخت تر 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 تراکنش های 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.