



كيف تحمي شبكتك الانترنت من المخترقين ؟

لو كنت تستخدم الكيبل للاتصال بشبكة الإنترنت فهذا يصعب على المخترقين الدخول معك في الشبكة واختراق جهاز البث الانترنت واستغلال اتصالك بالانترنت أو سرقة معلوماتك.

لكن مع الشبكات اللاسلكية فهذا يسهل على الأشخاص الذين يسكنون بجوارك أو قريبين من السكن بالدخول على شبكتك الخاصة. وقد يضر بك بأحد هذه الأمور:

- يستطيع سرقة بياناتك ومعرفة ما تقوم به على الإنترنت وقد يقوم بسرقة أرقامك السرية أو أي بيانات حساسة ومهمة.
- يسهل عليه الدخول إلى ملفاتك وسرقة معلومات من على جهاز الحاسوب أو الجوال المتصل بالشبكة اللاسلكية.
- قد يقوم بالدخول على مواقع مشبوهة أو يقوم بعمليات نصب واحتيال أو اختراقات باستخدام شبكتك، وبالتالي فإن الشخص المطلوب للسلطات سيكون أنت !
- سيكون سبب في خفض سرعة الإنترنت لديك لأنه يشاركك نفس الإتصال.
- وإذا كنت تستخدم إتصال بالانترنت من نوع حساب تكلفته يكون معتمد على حجم البيانات المستخدمة (مثل خدمات شرائح البيانات) سيزيد من قيمة فاتورتك وهذا شيء لا تريده طبعاً.

ولهذا هناك عدة اجراءات حماية وخطوات جدا مهمة يجب اتباعها لتقليل حالات الاختراق على شبكتك وهذه الاجراءات الحماية ليست كاملة مئة في المئة بل انها تبعدك من أن تصبح هدفا سهلا من المخترقين، والخطوات التالية لن تبعد المتسلل الخبير والمحترف ولكنها تصعب عملية الاختراق وتأخذ وقت أكثر للاختراق قد تصل الى عدة ساعات او أكثر من يوم لكسر كلمة المرور الخاصة بجهازك وبدون هذه الخطوات والاجراءات قد يحتاج الى دقائق للاختراق كلمة المرور والدخول الى شبكتك .

اذن ما هي هذه الاجراءات والخطوات ؟

1. عند شراء جهاز (Access Point) وهو جهاز بث داخلي للانترنت يجب عملة اولا تغيير IP الخاص بالجهاز وتغيير حساب الدخول للجهاز (User name , Password) وهذه الخطوة جدا مهمة واسباسية لكل جهاز يراد تنصيبه لبث اشارة الانترنت في البيت او لشركة .

TP-LINK 300M Wireless N Router
Model No. TL-WR544N / TL-WR541ND

LAN

MAC Address: 18-EE-ED-3E-F1-84

IP Address: 192.168.0.1 ← **تغير IP**

Subnet Mask: 255.255.255.0

IGMP Proxy: Enable

Save

LAN Help

You can configure the IP parameters of LAN on this page:

- **MAC Address** - The physical address of the LAN ports, as seen from the LAN. The value cannot be changed.
- **IP Address** - Enter the IP address of your Router in dotted-decimal notation (factory default - 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Usually it is 255.255.255.0.
- **IGMP Proxy** - If you want to watch TV through IGMP, please Enable it.

Note:

1. If you change the LAN IP address, you must use the new IP address to login to the Router.
2. If the new LAN IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

Click the Save button to save your settings.

TP-LINK 300M Wireless N Router
Model No. TL-WR544N / TL-WR541ND

Password

The username and password must not exceed 14 characters in length and must not include any spaces!

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

← **تغير User name and Password**

Save Clear All

Password Help

It is strongly recommended that you change the factory default user name and password of this device. All users who try to access this device's web-based utility will be prompted for this device's user name and password.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the Save button when finished.

Click the Clear All button to clear all.

2. هذه الخطوة جدا مهمة وهي معرفة اختيار نوع التشفير المستخدم لكلمة المرور وذلك عن طريق الدخول على الجهاز البث ومن ثم الى (Wireless + Wireless Security) وهذا يختلف من جهاز الى اخر، وهناك نوعين من التشفير اولا WEP وثانيا WPA or WPA2 وافضل واغوى نوع تشفير يجب اختياره هو النوع الثاني وهذا التشفير يساعد على زيادة الحماية وصعوبة الاختراق على المخترقين وبينما النوع الاول جدا سهل للمخترقين وهي ضعيفة جدا ويمكن كسرها بسهولة ، وبعد اختيار النوع الثاني يتم وضع كلمة مرور .



3. كلمة المرور : اغلب وقت الاختراق يعتمد على قوة كلمة المرور بحيث اذا كانت كلمة المرور قصيرة وسهلة عندها تساعد المخترق على سرعة الاختراق والعكس صحيح، من اهم مواصفات اختيار كلمة المرور للبث الاشارة هي يجب ان تكون مكوّنة من ارقام وحروف ورموز وتجنب اختيار ارقام موبايلات وتواريخ مهمة او اسماء مقربين لك لكلمات المرور.
4. تغيير كلمة المرور بشكل دوري اسبوعيا او اقل من شهر .
5. إغلاق جهاز البث عند عدم استعماله لفترة طويلة مثل وقت النوم في الليل أو خروجك للعمل فهذا يقلل نسبة الاختراق بدرجة عالية ، لان كما اشرنا سابقا عند الاختراق قد تحتاج الى ساعات او اكثر وهذا الوقت يكون متوفر في اغلب الاوقات في الليل وتركة يعمل وعدم اطفاء الجهاز .
6. هذه الخطوة يمكن استخدامها لحالات معينة وهي تخصيص فقط بعض الحواسيب واجهزة الموبايلات التي تستطيع الدخول لجهاز البث (Access Point) والاستفادة من الانترنت من خلال MAC Filter عندها لو امتلك المخترق كلمة المرور لن يستطيع الدخول إلى الشبكة لأنه تم تحديد عناوين الأجهزة المسموح لها باستخدام جهاز (Access Point) ، وهذه الخطوة جدا مهمة لانها تساعد على صعوبة الاتصال بالجهاز بعد الاختراق .

TP-LINK 300M Wireless N Router
Model No. TL-WR541N / TL-WR541ND

Wireless MAC Filtering

Wireless MAC Filtering: Disabled **MAC Filter** ← اختيار

Filtering Rules

- Deny the stations specified by any enabled entries in the list to access.
- Allow the stations specified by any enabled entries in the list to access.

MAC Address	Status	Description	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>			

Wireless MAC Filtering Help

The Wireless MAC Address Filtering feature allows you to control the wireless stations accessing the AP, which depend on the station's MAC addresses.

- MAC Address** - The wireless station's MAC address that you want to apply the filtering rules to.
- Description** - A simple description of the wireless station.
- Status** - The status of this entry, either Enabled or Disabled.

To enable the Wireless MAC Address Filter Status, keep the default setting Disabled.

To set up an entry, click Enable, and follow these instructions:

- First, you must decide whether the specified wireless station can or cannot access the AP. If you desire that the specified wireless station can access the AP, please select the radio button Allow the stations specified by any enabled entries in the list to access, otherwise, select the radio button Deny the stations specified by any enabled entries in the list to access.
- To add a Wireless MAC Address filtering entry, clicking the Add New... button, and following these instructions:
 - Enter the appropriate MAC Address into the MAC Address field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example, 00-0A-ED-D3-00-00.
 - Enter a simple description of the wireless station in the Description field. For example, Wireless station A.
 - Status - Select Enabled or Disabled for this entry in the Status pull-down list.
 - Click the Save button to save this entry.
- To add another entry, repeat steps 1-4.
- To modify or delete an existing entry:

7. هذه الخطوة ثانوية ولكنها ايضا فعالة لانها تساعد على تحديث (Upgrade) برنامج الجهاز البث وبعد التحديث قد تكتسب بعد الاضافات الحماية للبرنامج للجهاز .

TP-LINK 300M Wireless N Router
Model No. TL-WR541N / TL-WR541ND

Firmware Upgrade

File: No file chosen ← تحديث برنامج جهاز البث

Firmware Version: V 1.6.9 Build 150104 Rel.52205n
Hardware Version: WR541N v8 88888000

Firmware Upgrade Help

To upgrade this device's firmware, follow these instructions:

- Download a most recent firmware upgrade file from our website www.tp-link.com.
- Enter or select the path name where you save the downloaded file on the computer into the File Name field.
- Click the Upgrade button.
- This device will reboot while the upgrading has been finished.

Firmware Version - Displays the current firmware version.

Hardware Version - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note: The firmware version must correspond to the hardware. The upgrade process takes a few moments and the device reboots automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the device.

8. اخيرا ولمعرفة اذا كان جهازك مخترق ويوجد اشخاص اخرين يشاركون اشارتك الانترنت هناك طريقتين اولاً: من خلال الدخول الى جهاز البث (Access Point) واختيار الاعدادات التالية (Wireless + Wireless Statistics) ثانياً : تنصيب برنامج في الحاسبة لمعرفة الاشخاص المتصلين بالجهاز البث واسمه (Who is On My Wi-Fi) وهذا البرنامج يعطيك تفاصيل ومعلومات اكثر على كل مستخدم متصل بالشبكة، وتنزيل البرنامج من خلال الرابط ادناه

www.whoisonmywifi.com/windows/

Who's On My Wifi - Free Edition UPGRADE

Scan برنامج لمعرفة الأشخاص المتصلين بالجهاز البث Scan Now

Detected Network Devices: 6 Save Changes

Block	Description	Mac Address	Last Computer Name	Last IP Address	Connected	Known/Unknown	Remove
<input type="checkbox"/>	TYPE IN NAME	02:4A:80:08:03:2C		192.168.1.107	YES	UNKNOWN	
<input type="checkbox"/>	TYPE IN NAME	00:09:40:0F:0A:4E	HP4410P	192.168.1.109	YES	UNKNOWN	
<input type="checkbox"/>	TYPE IN NAME	02:08:3A:00:5D:37		192.168.1.100	NO	UNKNOWN	
<input type="checkbox"/>	TYPE IN NAME	00:03:09:63:CA:95		192.168.1.102	NO	UNKNOWN	
<input type="checkbox"/>	TYPE IN NAME	8C:76:AD:61:80:03		192.168.1.103	YES	UNKNOWN	
<input checked="" type="checkbox"/>	TYPE IN NAME	08:00:FA:45:82:C5		192.168.1.100	YES	UNKNOWN	

Network Device

- Device: 02:4A:80:08:03:2C
- Device: 02:09:40:0F:0A:4E
- Device: 02:08:3A:00:5D:37
- Device: 00:03:09:63:CA:95
- Device: 8C:76:AD:61:80:03
- Device: 08:00:FA:45:82:C5

UNKNOWN

Digital Signature: 3D40C78D05A0C1479C
Mac Address: 08:00:FA:45:82:C5

Network Name:

Last IP: 192.168.1.100

Currently Connected: YES

Last Time Found: 28/06/2016 03:36

First Discovered on Network: 25/06/2015 03:36

View Manufacturer Network Connection

Version: 3.0.2

الكاتب م.م مغرب عبد الرضا الرماحي