كيف تحمي شبكتك الانترنت من المخترقين ؟

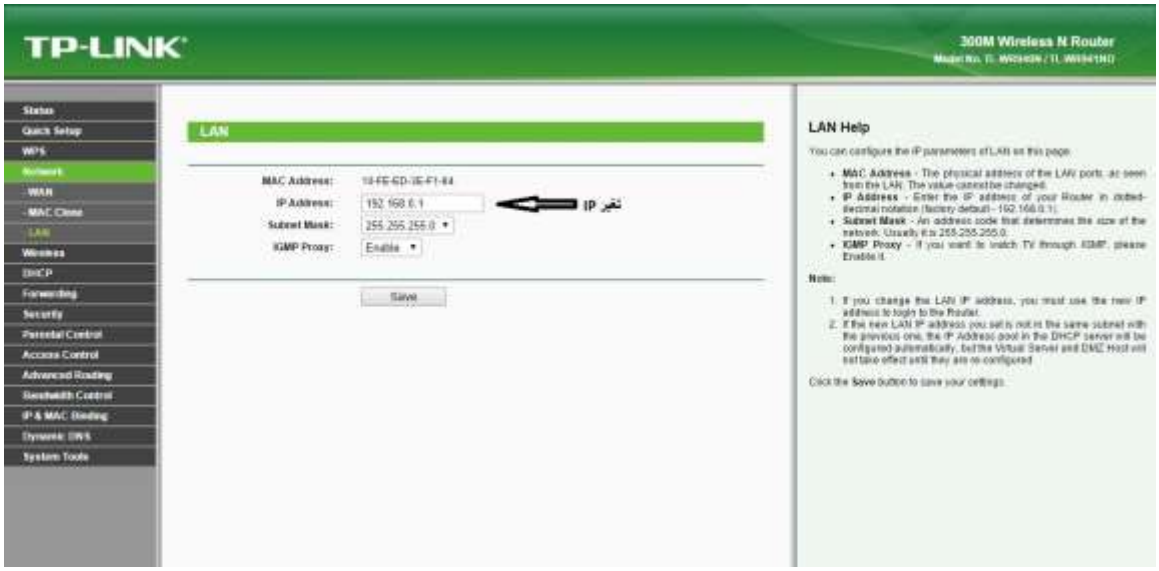
لو كنت تستخدم الكيبل للاتصال بشبكة الإنترنت فهذا يصّعب على المخترقين الدخول معك في الشبكة واختراق جهاز البث الانترنت واستغلال اتصالك بالانترنت أو سرقة معلوماتك.
لكن مع الشبكات اللاسلكية فهذا يسّهل على الأشخاص الذين يسكنون بجوارك او قريبين من السكن بالدخول على شبكتك الخاصة. وقد يضرك بأحد هذه الأمور:

- **يستطيع سرقة بياناتك ومعرفة ما تقوم به على الإنترنت وقد يقوم بسرقة أرقامك السرية أو أي بيانات حساسة ومهمة.**
- **يسّهل 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 انت !**
- **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 طبعا.**

ولهذا هناك عدة اجرائات حماية وخطوات جدا مهمة يجب اتباعها لتقليل حالات الاختراق على شبكتك وهذه الاجرائات الحماية ليست كاملة مئة في المئة بل انها تبعدك من أن تصبح هدفا سهلا من المخترقين، والخطوات التالية لن تبعد المتسلل الخبير والمحترف ولكنها تصّعب علية عملية الاختراق وتاخذ وقت اكثر للاختراق قد تصل الى عدة ساعات او اكثر من يوم لكسر كلمة المرور الخاصة بجهازك وبدون هذة الخطوات والاجرائات قد يحتاج الى دقائق لاختراق كلمة المرور والدخول الى شبكتك .

اذن ما هي هذة الاجرائات والخطوات ؟

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



2. **هذة 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 واقوى نوع تشفير يجب اختيارة هو النوع الثاني وهذا التشفير يساعد على زيادة الحماية وصعوبة الاختراق على المخترقين وبينما النوع الاول جدا سهل للمخترقيين 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 مكّونة من ارقام وحروف ورموز وتجنب اختيار ارقام موبايلات وتواريخ مهمة او اسماء مقربين لك لكلمات المرور.**
4. **تغير 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. **هذة 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) ، وهذة الخطوة جدا مهمة لانها تساعد على صعوبة الاتصال بالجهاز بعد الاختراق .**

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

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

www.whoisonmywifi.com/windows/

الكاتب م.م مغرب عبد الرضا الرماحي