Ασφάλεια του Ασύρματου Δικτύου

Εάν έχετε φτιάξει ένα ασύρματο δίκτυο στο σπίτι σας και δεν θέλετε να μπαίνουν οι γείτονες και να καταναλώνουν το bandwidth σας ή δεν θέλετε ο 15χρονος κομπιουτεράκιας να κάνει τα πρώτα του βήματα στο hacking από το ασύρματο router σας, τότε διαβάστε τον οδηγό μας για να ασφαλίσετε πλήρως το δίκτυο σας.
Σε αυτό τον οδηγό θα δείτε πως θα προφυλαχθείτε από όλες αυτές τις περιπτώσεις.

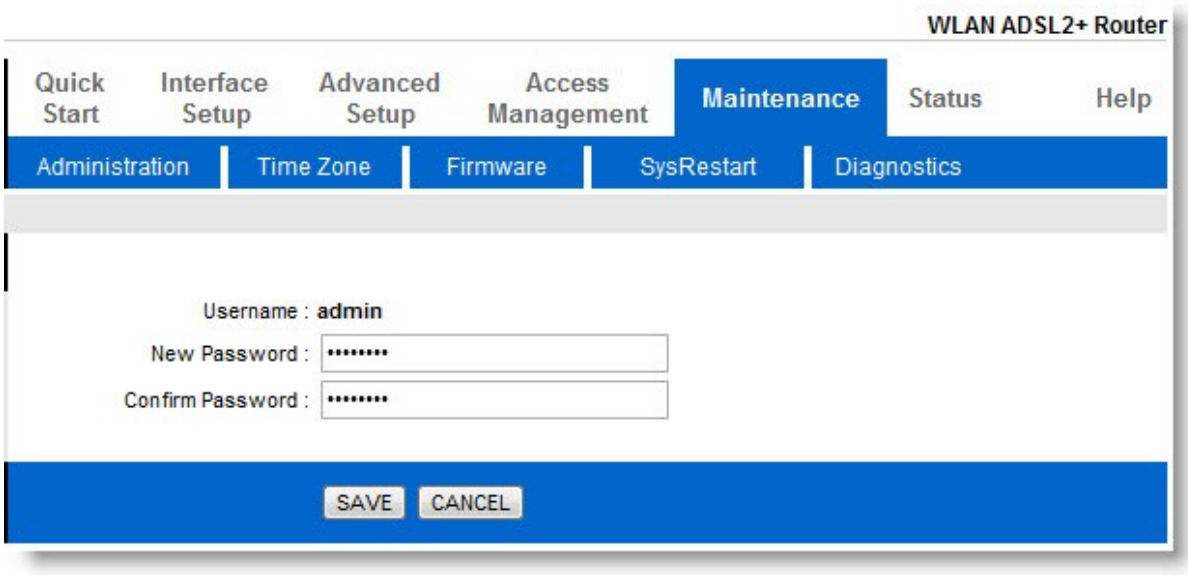
1. Βάλτε κωδικό πρόσβασης στο router σας

Όλα τα ασύρματα routers έχουν μια σελίδα διαχείρισης, στην οποία έχετε πρόσβαση από οποιοδήποτε browser. Για να αποτρέψετε τους εισβολείς από το να αλλάξουν τις ρυθμίσεις του router σας, θα πρέπει να βάλετε ένα κωδικό πρόσβασης που απαιτείτε κάθε φορά που θέλετε να αλλάξετε τις ρυθμίσεις.

Για να συνδεθείτε με τη διαχείριση του router σας, βεβαιωθείτε ότι ο υπολογιστής σας είναι συνδεμένος στο ασύρματο δίκτυο. Ανοίξτε τον browser σας και πληκτρολογείστε στη γραμμή διευθύνσεων την διεύθυνση του router. Συνήθως είναι "192.168.1.1", "192.168.2.1" ή για τα Thomson routers της Forthnet "192.168.1.254".

Εάν είναι η πρώτη φορά που ανοίγετε τις ρυθμίσεις του router, τότε το πιθανότερο είναι ότι θα σας ζητηθεί ένα username και ένα password τα οποία μπορείτε να βρείτε στο manual του router. Καλό θα είναι και σε αυτή την περίπτωση να αλλάξετε τον κωδικό, αφού τα περισσότερα routers μιας εταιρείας έρχονται με στάνταρ κωδικούς.

Ανάλογα το router, επιλέξτε "Maintenance" ή "Administration" ή "Management" για να σας εμφανιστούν τα πεδία όπου μπορείτε να πληκτρολογήσετε ένα password για αλλαγή. Μετά πατήστε αποθήκευση.

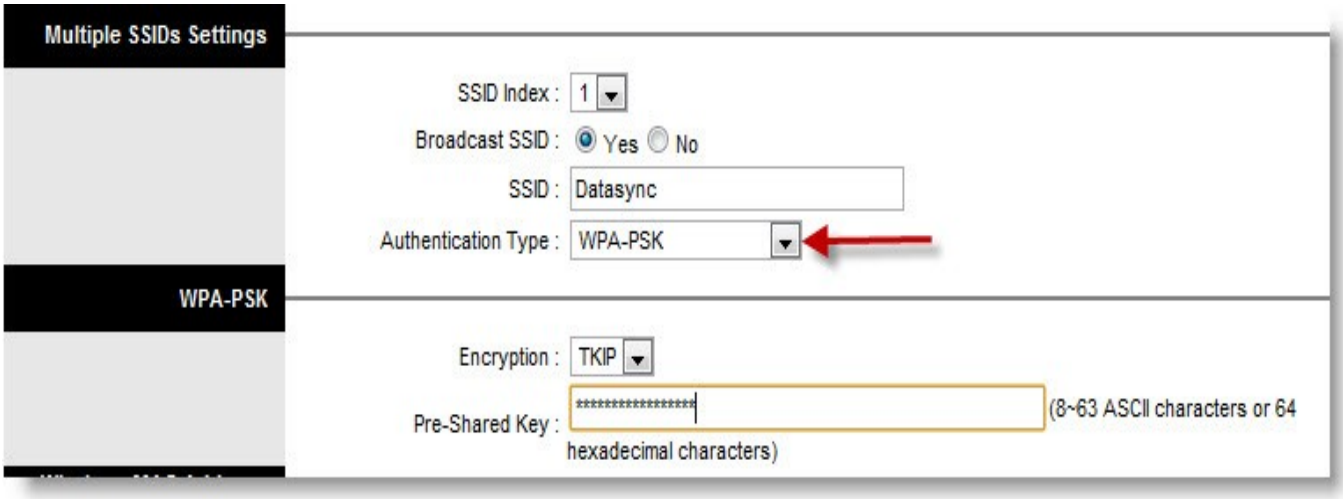


2. Προστατεύστε την ασύρματη σύνδεση με κωδικό WPA

Είναι ίσως η πιο σημαντική ρύθμιση για την ασφάλεια του ασύρματου δικτύου σας. Εάν η ασύρματη σύνδεση σας προστατεύεται με ένα κωδικό πρόσβασης, τότε θα έχουν πρόσβαση μόνο όσοι το ξέρουν.

Τα περισσότερα routers δίνουν δύο μεθόδους κρυπτογράφησης του κωδικού σας, ο ένας είναι ο Wired Equivalent Privacy **(WEP)** και ο άλλος είναι ο Wi-Fi Protected Access **(WPA).** Οι κωδικοί με κρυπτογράφηση WEP μπορούν να "σπάσουν πιο έυκολα" και γι' αυτό προτείνουμε να χρησιμοποιήσετε WPA κρυπτογράφηση.

Τις ρυθμίσεις για την κρυπτογράφηση του κλειδιού σας θα τις βρείτε συνήθως στο WLAN Settings.



3. Αναβάθμιση του Firmware του router σας

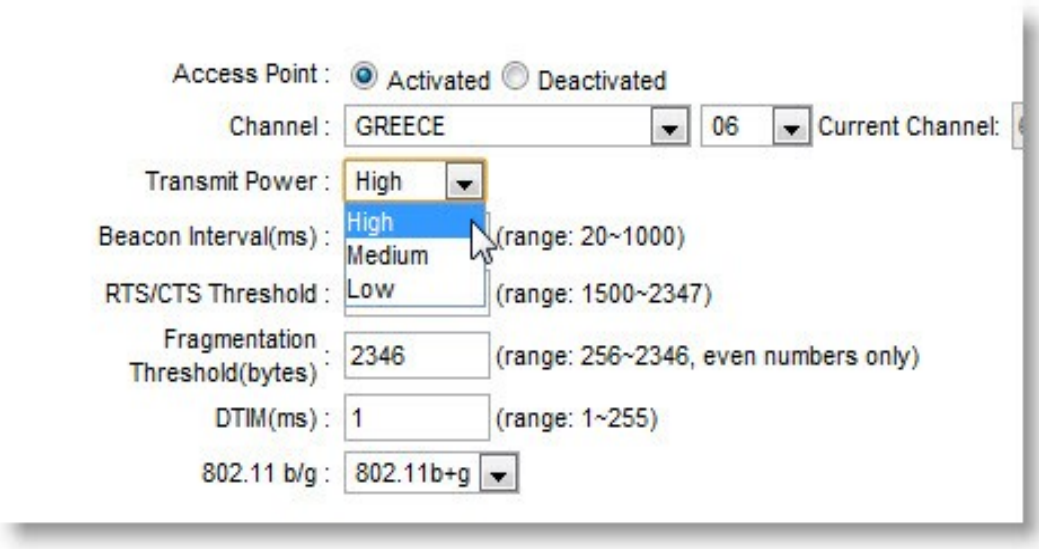
Το να κρατάτε ενημερωμένο το firmware του router σας είναι πολύ σημαντικό. Οι αναβαθμίσεις συνήθως φέρνουν περισσότερες επιλογές ασφαλείας αλλά και διορθώνουν τυχών bugs του router.

Για να αναβαθμίσετε το router σας, επισκεφθείτε την αντίστοιχη σελίδα του κατασκευαστή του.

4. Ρυθμίστε την ισχύ του σήματος που εκπέμπει το router

Εάν το router σας, δίνει την επιλογή να ρυθμίσετε την ισχύ που θα εκπέμπει το ασύρματο σήμα, τότε μπορείτε να δοκιμάσετε εάν το σήμα που εκπέμπει είναι αρκετό για να καλύψει τον χώρο σας. Με αυτό τον τρόπο μπορείτε να το ρυθμίσετε έτσι ώστε στις άκρες του σπιτιού σας, το σήμα να είναι εξασθενημένο ούτως ώστε να μην μπορούν οι γείτονες να "πιάσουν σήμα".

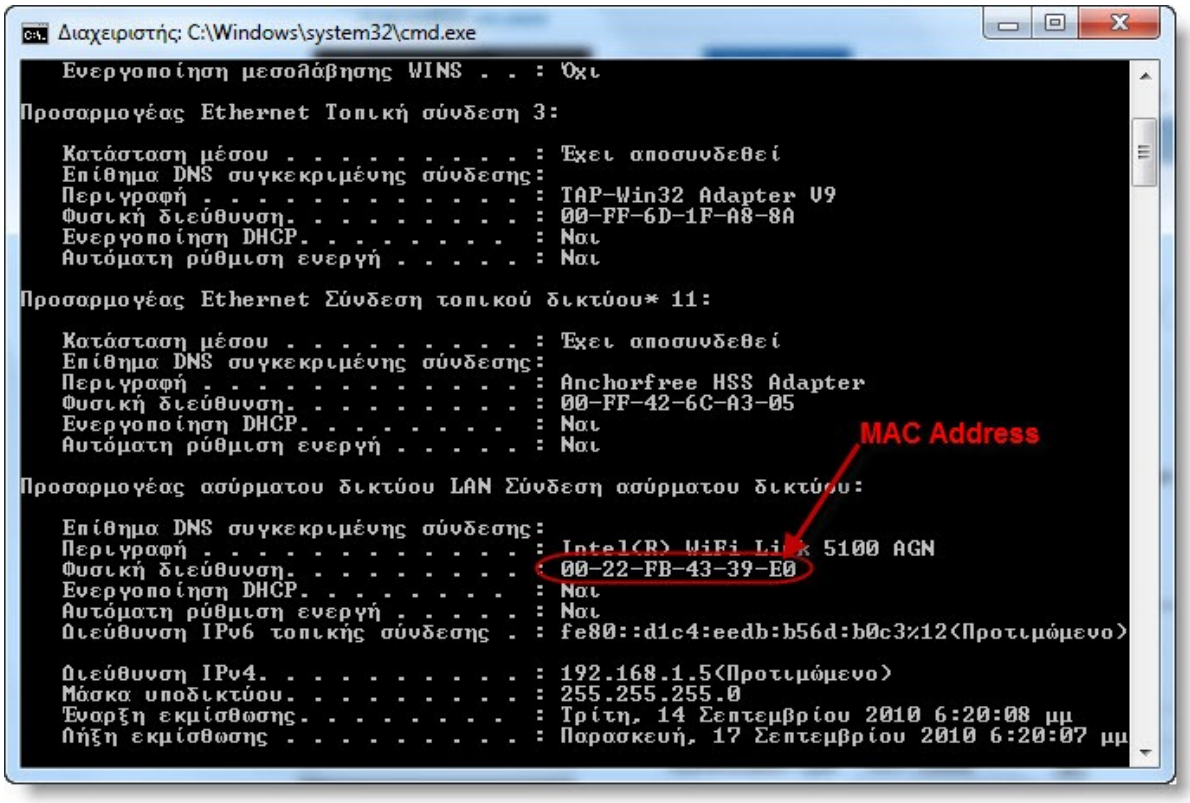
Την επιλογή συνήθως την βρίσκετε μαζί με τις υπόλοιπες ρυθμίσεις του ασύρματου δικτύου (Wireless Settings).



4. Φιλτράρισμα χρηστών βάση της MAC Adress

Κάθε υπολογιστής με κάρτα δικτύου έχει τη δική του μοναδική MAC Address ή αλλιώς Media Access Control.

Ένας ακόμη τρόπος προστασίας της ασύρματης σύνδεσης σας είναι να ρυθμίσετε το router να συνδέεται μόνο με συσκευές με συγκεκριμένες MAC Address. Για να δείτε την MAC Address ενός υπολογιστή, πληκτρολογείστε στο πεδίο της αναζήτησης του μενού έναρξης "cmd.exe" και κάντε κλίκ στο πρώτο αποτέλεσμα. Μόλις ανοίξει η κονσόλα, πληκτρολογείστε "ipconfig/all" και πατήστε enter. Το αποτέλεσμα θα είναι όπως φαίνεται στην εικόνα που ακολουθεί.



Σημειώστε κάπου τη MAC Address, και στις ρυθμίσεις "Wireless Settings" του router ενεροποιήστε το φιλτράρισμα με βάση τη MAC Address και πληκτρολογείστε τις διευθύνσεις των υπολογιστών που θέλετε να έχουν πρόσβαση στο δίκτυο σας.