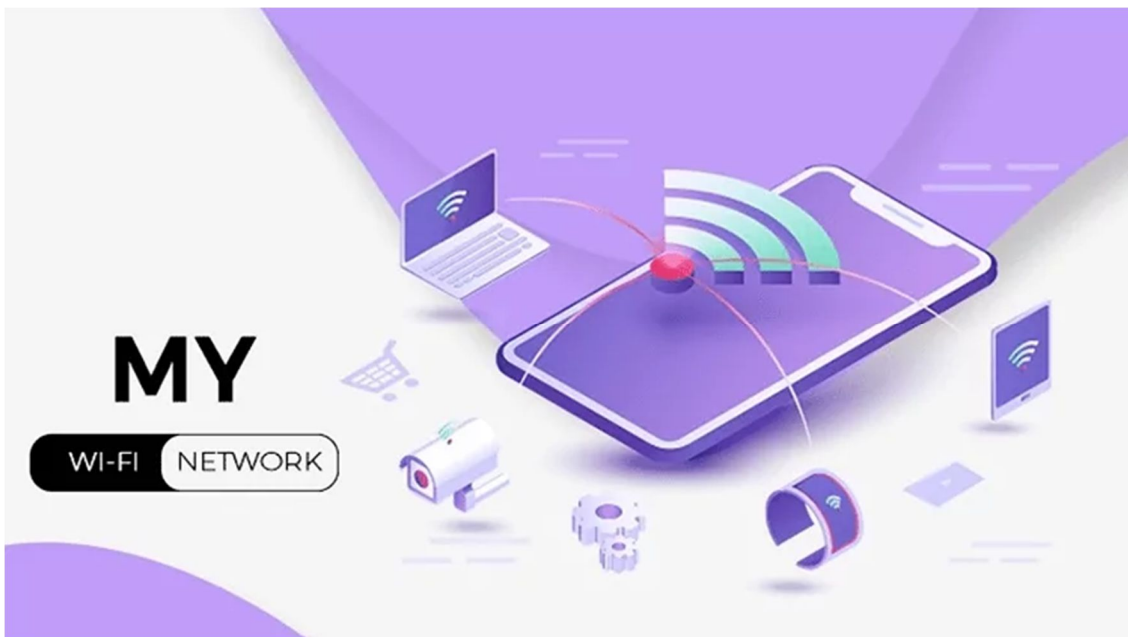


Ποιος Κλέβει το WiFi μου - Δείτε Ποιοι Συνδέονται στο Router

Εάν έχουμε παρατηρήσει ότι η σύνδεσή μας στο ίντερνετ είναι πιο αργή απ' ό,τι συνήθως, τότε ενδέχεται να μην φταίει ο πάροχος, αλλά κάποιος που κλέβει το WiFi, είτε από απροσεξία μας, είτε εκμεταλλευόμενος κάποιο κενό ασφαλείας στο router μας. Από τη στιγμή που μία άγνωστη συσκευή έχει πρόσβαση στο ασύρματο δίκτυο μας, ο κίνδυνος να εκτεθούμε ανεπανόρθωτα είναι σοβαρός. Δείτε πώς εντοπίζουμε ποιοι συνδέονται στο router εν αγνοία μας, και πώς να προφυλαχτούμε αποτελεσματικά.



Τα αναγνωριστικά των συσκευών μας στο ασύρματο δίκτυο

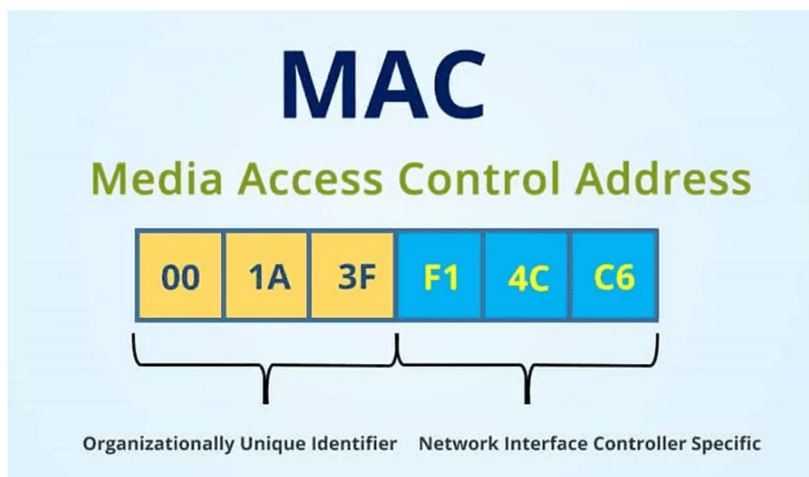
Στις μέρες μας, οι περισσότερες ηλεκτρονικές συσκευές μπορούν να συνδεθούν ασύρματα στο δίκτυο.

Φορητοί υπολογιστές, tablet, smartphone, ψηφιακές φωτογραφικές μηχανές, εκτυπωτές, κονσόλες παιχνιδιών, έξυπνες οικιακές συσκευές, και πολλά άλλα, μπορούν να συνδεθούν μεταξύ τους και στο διαδίκτυο μέσω WiFi.

Έτσι, για να διαπιστώσουμε αν κάποιος όντως κλέβει το WiFi μας, θα πρέπει πρώτα να γνωρίζουμε με ακρίβεια ποιες είναι οι δικές μας συσκευές που συνδέονται στο router, ώστε να απομονώσουμε την άγνωστη συσκευή, λαμβάνοντας άμεσα μέτρα.

Διεύθυνση MAC

Κάθε κάρτα δικτύου, εσωτερική, εξωτερική, ή ενσωματωμένη σε οποιαδήποτε συσκευή, έχει έναν μοναδικό αριθμό που είναι η ταυτότητά της. Ο αριθμός αυτός ονομάζεται **διεύθυνση MAC** (Media Access Control).



Η MAC address, ή αλλιώς φυσική διεύθυνση (Physical Address), είναι προκαθορισμένη και αποθηκευμένη στην κάρτα δικτύου του υπολογιστή από το εργοστάσιο. Δεν αλλάζει όταν μεταφέρουμε έναν υπολογιστή από ένα δίκτυο σε ένα άλλο.

Γνωρίζοντας τις διευθύνσεις MAC των συσκευών μας (υπολογιστής, κινητό, tablet), έχουμε κάνει το πρώτο βήμα για να διαπιστώσουμε αν υπάρχει κάποια άγνωστη συσκευή που μας κλέβει το WiFi.

Διεύθυνση IP

Εκτός από την διεύθυνση MAC, υπάρχει και η διεύθυνση IP (Internet Protocol address). Είναι ένας αριθμός ο οποίος εκφράζει τη μοναδική διεύθυνση της συσκευής μας στο δίκτυο που είναι συνδεδεμένη.

Έτσι, όλες οι συσκευές μας που συνδέονται μέσω router έχουν μία εσωτερική IP στο δίκτυο. Συνήθως είναι της μορφής 192.168.x.x, που δεν επαναλαμβάνεται στο ίδιο τοπικό δίκτυο LAN.

Επίσης, η εξωτερική IP του router, δηλαδή η IP μας προς το ίντερνετ, είναι και αυτή μοναδική στον κόσμο, ανά πάσα στιγμή. Αυτό σημαίνει ότι μπορεί να χρησιμοποιηθεί για να εντοπίσουν τη διεύθυνση του σπιτιού μας, υπό συγκεκριμένες προϋποθέσεις.

9C-35-5B-5F-4C-D7

192.168.0.1

MAC address
and IP address

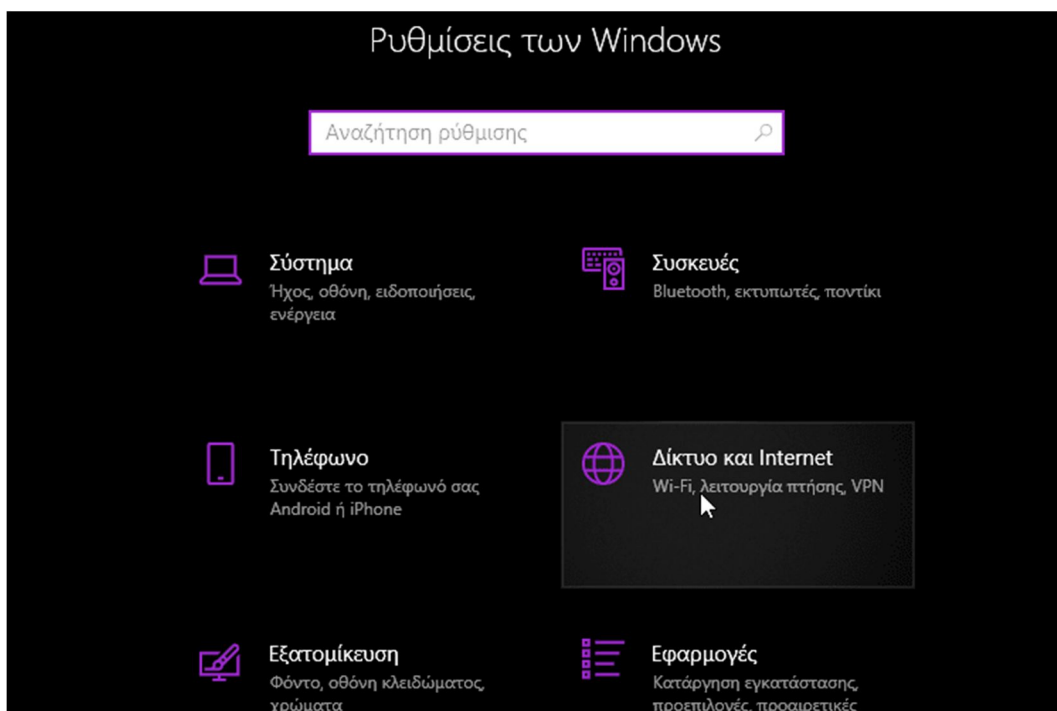
Η διεύθυνση IP είναι από προεπιλογή δυναμική σε όλες τις συσκευές, που σημαίνει πως μπορεί να αλλάζει κάθε φορά που μία συσκευή συνδέεται στο router.

Κατά συνέπεια, κάθε φορά που θα κάνουμε έλεγχο για τις συσκευές που συνδέονται στο router, ώστε να βρούμε αν κάποιος μας κλέβει το WiFi, θα πρέπει να βρίσκουμε την IP που πήρε ο υπολογιστής μας εκείνη τη στιγμή.

Ως εκ τούτου, μία καλή στρατηγική είναι να ορίζουμε σταθερή IP σε συσκευές που δεν μετακινούνται εκτός σπιτιού, ώστε να γλιτώνουμε χρόνο.

Πώς βρίσκω τη MAC & IP Address στις συσκευές

Για να εντοπίσουμε τη διεύθυνση MAC και την IP του κάθε Windows PC που διατηρούμε στο ασύρματο δίκτυο, δεν έχουμε παρά να ακολουθήσουμε μέσα από τις ρυθμίσεις τα απλά βήματα που βλέπουμε στις παρακάτω εικόνες.



🏠 Αρχική

Αναζήτηση ρύθμισης 🔍

Δίκτυο και Internet

- 🌐 Κατάσταση
- 📶 Wi-Fi
- 🖨️ Ethernet
- ☎️ Κλήση
- 🔒 VPN
- ➡️ Λειτουργία πτήσης
- 📶 Κινητό hotspot

Κατάσταση

Κατάσταση δικτύου

Ethernet
Ιδιωτικό δίκτυο

Είστε συνδεδεμένοι στο Internet

Αν έχετε ένα περιορισμένο πρόγραμμα δεδομένων, μπορείτε να κάνετε αυτό το δίκτυο μια σύνδεση ογκοχρέωσης ή να αλλάξετε άλλες ιδιότητες.

Ethernet 378.36 GB
Από τις τελευταίες 30 ημέρες

Ιδιότητες Χρήση δεδομένων

🌐 Εμφάνιση διαθέσιμων δικτύων
Προβολή των επιλογών σύνδεσης γύρω σας.

Ιδιότητες

Ταχύτητα σύνδεσης (Λήψη/Μετάδοση): 1000/1000 (Mbps)

Τοπική διεύθυνση σύνδεσης IPv6: fe80::98d1:3bcf:b864:939e%20

Διεύθυνση IPv4: 192.168.1.6

Διακομιστές DNS IPv4: 192.168.1.1
192.168.1.1

Επίθημα πρωτεύοντος DNS: home

Κατασκευαστής: Realtek

Περιγραφή: Realtek PCIe GBE Family Controller

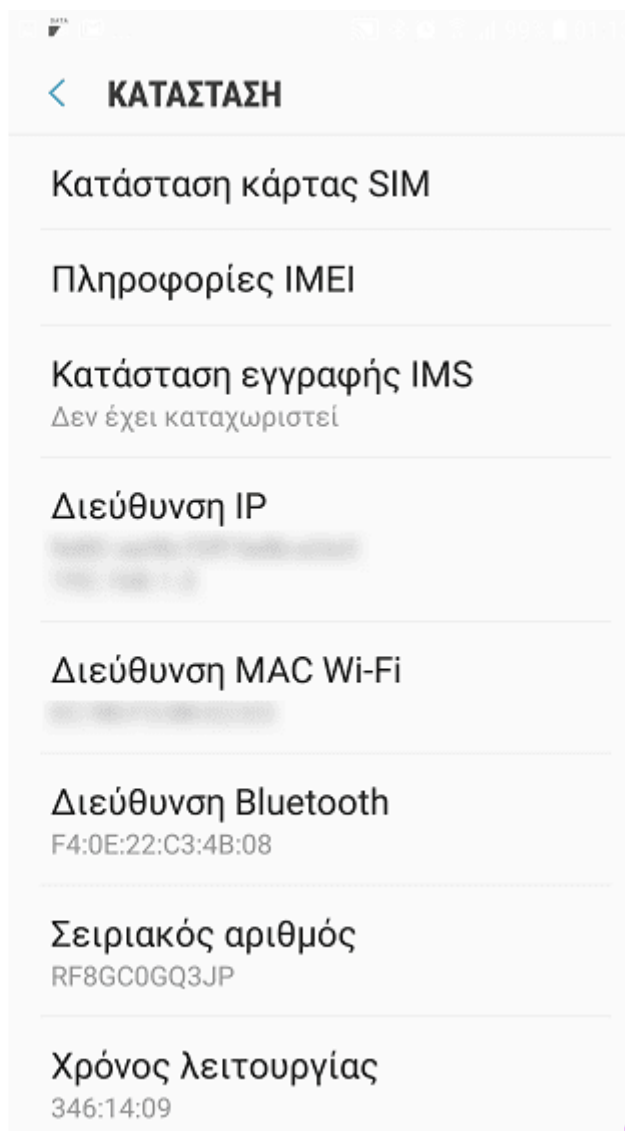
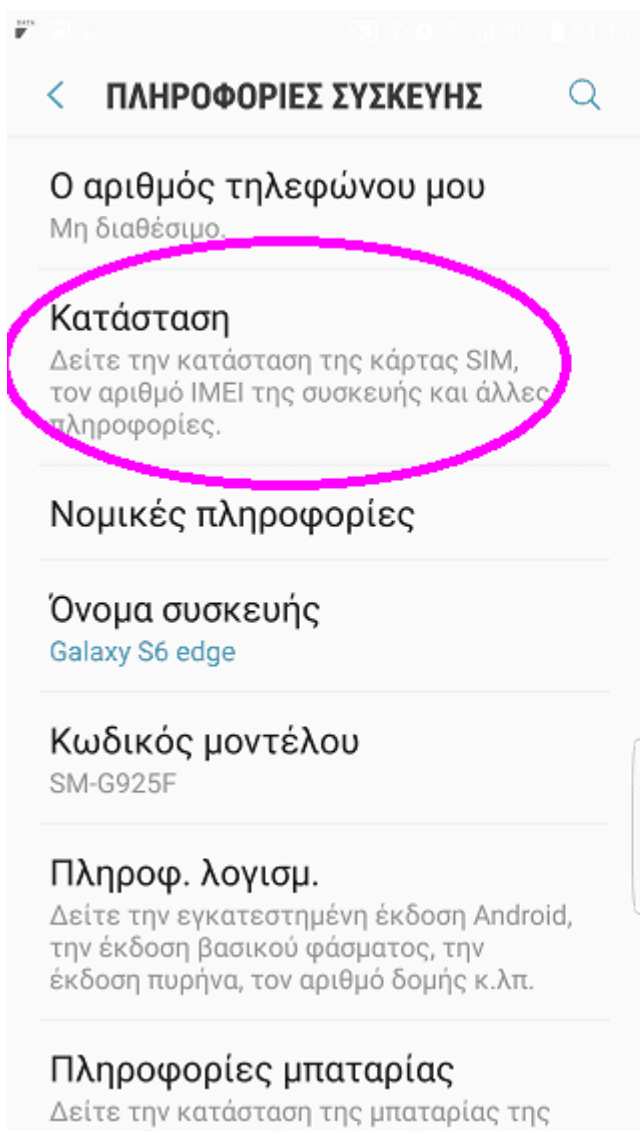
Έκδοση προγράμματος οδήγησης: 10.10.714.2016

Φυσική διεύθυνση (MAC): 98-EE-(...)

Αντιγραφή

🔊 Λήψη βοήθειας

Στο Android και στο iOS, θα χρειαστεί να πάμε Ρυθμίσεις -> Σχετικά με τη συσκευή ή Πληροφορίες συσκευής -> Κατάσταση.



Γιατί ο έλεγχος είναι σημαντικός

Το πιο κοινό σημάδι ότι κάποιος κλέβει το WiFi μας είναι η αργή σύνδεση στο ίντερνετ.

Κάθε σύνδεση στο διαδίκτυο καταλαμβάνει ένα εύρος ζώνης. Αν κάποιος το χρησιμοποιεί για λήψη torrent ή παίζει διαδικτυακά παιχνίδια χωρίς την άδειά μας, τότε η επιβράδυνση είναι ένα φυσικό επακόλουθο.

Όμως, η καθυστέρηση της σύνδεσης είναι το λιγότερο που μπορεί να μας συμβεί. Αν αυτός που κλέβει το WiFi το χρησιμοποιεί για έκνομες ενέργειες, δεν αποκλείεται να βρεθούμε κατηγορούμενοι από το πουθενά.

Ο λόγος είναι ότι οι δραστηριότητες του θα φαίνονται μέσα από τη διεύθυνση IP της δικής μας σύνδεσης, και η δίωξη ηλεκτρονικού εγκλήματος θα χτυπήσει τη δική μας πόρτα. Και σε τέτοιες περιπτώσεις, είναι πολύ δύσκολο να αποδείξουμε την αθωότητά μας.

Επιπλέον, αν κάποιος έχει πρόσβαση στο δίκτυό μας, ενδεχομένως να μπορεί να έχει πρόσβαση στα προσωπικά μας αρχεία. Σε ορισμένες περιπτώσεις μπορεί ακόμη και να κλέψει διάφορους κωδικούς πρόσβασης και άλλα προσωπικά δεδομένα.


Οι μέθοδοι του ελέγχου

Έτσι λοιπόν, είναι ζωτικής σημασίας να ελέγχουμε τακτικά αν κάποιος συνδέεται στο δίκτυό μας χωρίς την άδειά μας και μας κλέβει το WiFi. Αυτό το επιτυγχάνουμε κυρίως με τη χρήση ειδικών εφαρμογών. Φυσικά, μπορούμε και μέσα από το router μας.

Έλεγχος WiFi διαμέσου Fing Desktop

Το Fing είναι ένα δωρεάν app, το οποίο διατίθεται σε iOS και Android, καθώς επίσης και σε Windows και Mac. Είναι ιδανικό για να ανιχνεύσουμε με πολύ εύκολο τρόπο όλες τις συσκευές που είναι συνδεδεμένες στο WiFi του χώρου.

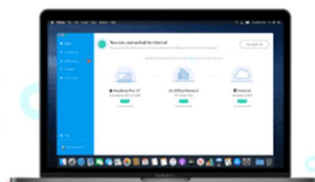


FING ACCOUNT 

Download Fing Desktop

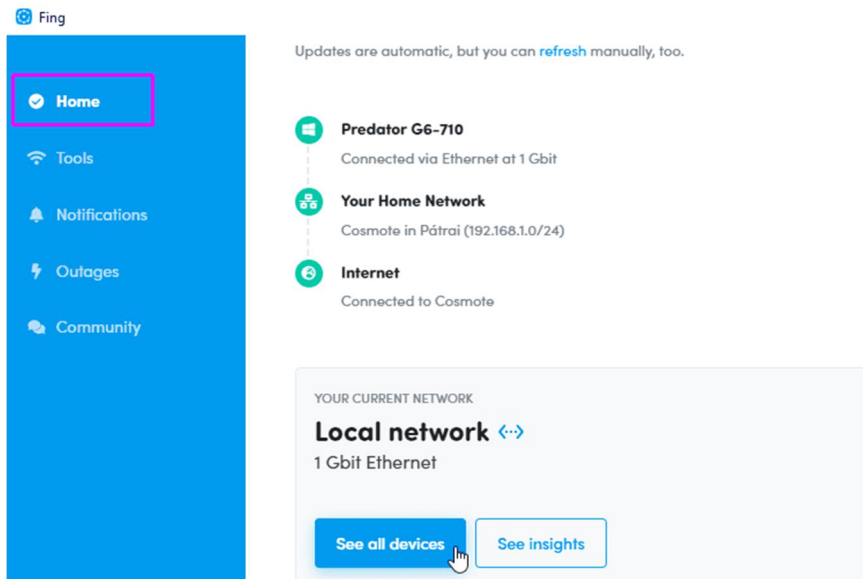
Get the free Fing Desktop for continuous connectivity health checks, advanced speed tests, level 1 troubleshooting features, notifications of connectivity issues and widespread Internet outages for your Home ISP.

Send yourself an e-mail with the [download link](#).



Το αρχείο εγκατάστασης είναι περί τα 70MB και δεν κρύβει προγράμματα τρίτων. Μόλις ολοκληρωθεί η εγκατάσταση, το Fing Desktop θα τρέχει αυτόματα με την εκκίνηση του PC, κάτω δεξιά στην γραμμή εργασιών.

Μόλις το τρέξουμε για πρώτη φορά, θα μας ζητήσει να ανοίξουμε έναν λογαριασμό μέσω Google ή Facebook. Κατόπιν, το μόνο που έχουμε να κάνουμε είναι να πατήσουμε στο "See all devices" στη κεντρική του καρτέλα.



Αναγνώριση συσκευών

Από εκεί και μετά, το Fing Desktop προσφέρει με αυτόματο τρόπο την καλύτερη μέθοδο αναγνώρισης συσκευών που θα μπορούσαμε να έχουμε. Μας δείχνει με ξεκάθαρο τρόπο ποιες είναι οι δικές μας, και ποιες ενδεχομένως όχι.

Όπως παρατηρούμε στη παρακάτω εικόνα, η εφαρμογή εμφανίζει την διεύθυνση MAC και IP των συσκευών, μία ακριβή περιγραφή, τον τύπο και την κατηγορία της συσκευής, ακόμη και το λειτουργικό σύστημά της, έτσι ώστε να είμαστε απόλυτα βέβαιοι ότι είναι η δικιά μας.

Type	IP Address	MAC Address	Name	DStails	Changed
	192.168.1.1	60:CE:86	speedport		
	192.168.1.2	C0:48:E6	[TV] Samsung 7 Seri...		6:54 PM
	192.168.1.3	EC:9B:F3	Samsung Galaxy S6...	Android Nou...	1:14 PM
	192.168.1.4	70:85:C2	AKISPC	Windows	12:21 PM
	192.168.1.5	6C:21:A2	TV BOX		8:05 PM
	192.168.1.6	98:EE:CB	PREDATOR: akistiga...	Windows 10 H...	1:14 PM
	192.168.1.7	50:3E:AA	WIN-6D2JOO033M4	Windows	5:14 PM
	192.168.1.8	10:1C:0C:	iPad	iOS	6:54 PM

Εφόσον εντοπίσουμε μία συσκευή που δεν ανήκει σε εμάς και θεωρούμε ότι μπορεί να κλέβει το WiFi, πρέπει αμέσως να αλλάξουμε τους κωδικούς πρόσβασης, το λεγόμενο WLAN key.

Όταν αλλάξει ο κωδικός πρόσβασης στον router, την ίδια στιγμή αποσυνδέονται όλες οι συσκευές που χρησιμοποιούν τον παλιό κωδικό πρόσβασης.

Σε αντίθετη περίπτωση, η νέα σάρωση δικτύου θα προσθέσει ξανά την άγνωστη συσκευή στη λίστα, καθώς η διαγραφή της συσκευής που διαθέτει το Fing δεν θα εμποδίσει τον επίμονο επιτήδειο να συνεχίσει να κλέβει το WiFi μας.

Home

Tools

Notifications

Outages

Community

★ Upgrade Account

📄 Fing 2.0.0

👤 akis tigas

↑ Online • 20 hours ago

🏠 Add placement

Edit Delete Recognize Events Favorite Important

Info

IP Address	192.168.1.7
MAC Address	50:3E:AA:B3:B5:24 [TP-Link]
Hostname	WIN-6D2JOO033M4-001
First seen	16 Thu, 12:53 AM
Last change	16 Thu, 5:14 PM

Notifications

★ Premium

Η ιδέα στο δωρεάν πρόγραμμα είναι να εντοπίσουμε τυχόν άγνωστες συσκευές που είναι συνδεδεμένες στο τοπικό μας δίκτυο για να πάρουμε άμεσα τα μέτρα μας.

Αν θέλουμε τον οριστικό αποκλεισμό άγνωστων συσκευών που έχουν συνδεθεί στο ασύρματο δίκτυο μας, πρέπει να αγοράσουμε το Fingbox, μία ειδική συσκευή που συνεργάζεται με το πρόγραμμα. Βέβαια, αυτό είναι σχετικά υπερβολικό για έναν απλό χρήστη.

Επίσης, πατώντας στο "Edit" ή στο "Recognise", το Fing Desktop μας επιτρέπει να δώσουμε πιο αναλυτική περιγραφή σε όποια συσκευή εμφανίζεται.

Έτσι, σε κάθε έλεγχο, θα έχουμε ακόμη πιο άμεση και ξεκάθαρη εικόνα ότι είναι η δικιά μας, χωρίς να χρειαστεί να ανατρέξουμε στη MAC address.

Automatic
Manual

You can manually enter product details for this device by searching in Fingpedia.

It is suggested to type brand, type and specific model name of the device, then click on the best result to choose it.

Device TP-Link Computer

Type	Brand	Model	Code	Market Share
Wi-Fi	TP-Link	TP-Link		
Mobile	TP-	Link		
	TP-	TP mini		

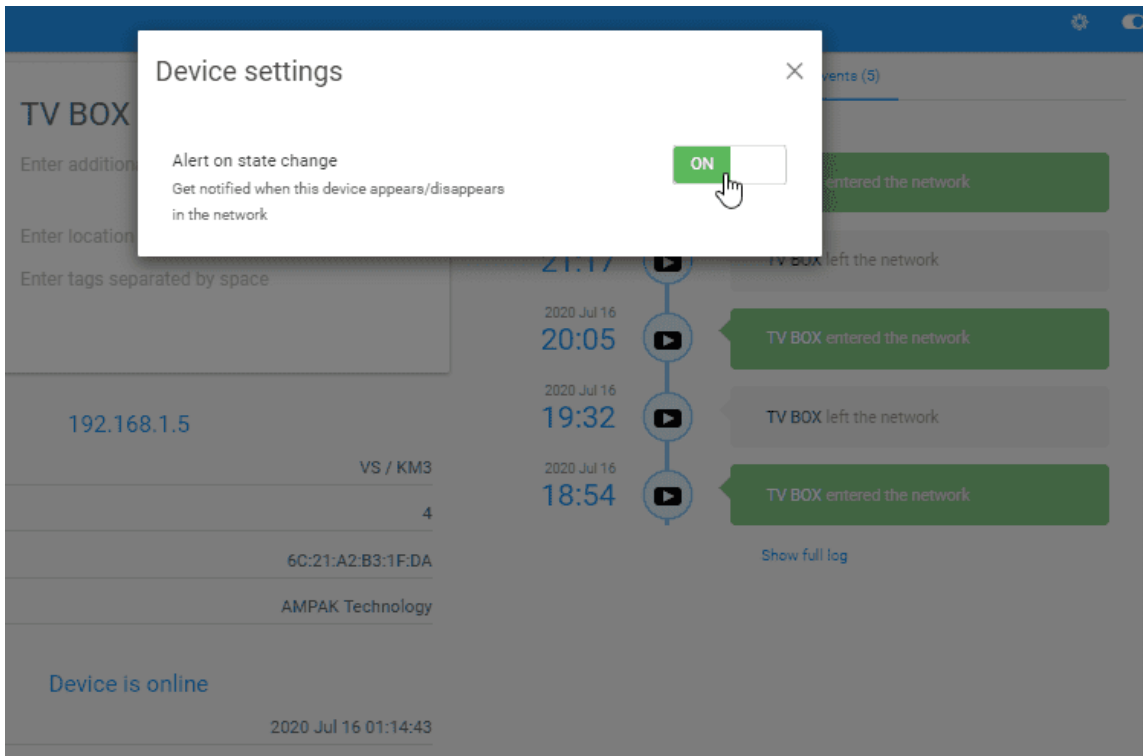
Το Fing δεν περιορίζεται μόνο για να δούμε ποιος κλέβει το WiFi. Προσφέρει πολλές ακόμη δωρεάν λειτουργίες, όπως έλεγχο για κενά ασφαλείας σε UPnP και NAT-PMP, την πραγματική μας ταχύτητα, κ.α.

Απομακρυσμένος έλεγχος ασύρματου δικτύου

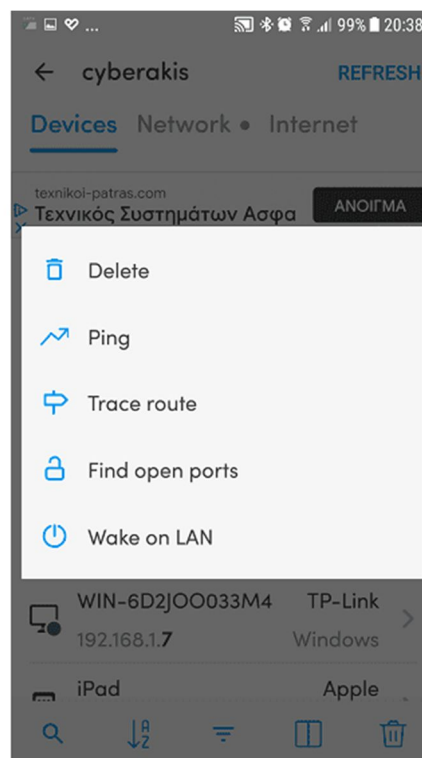
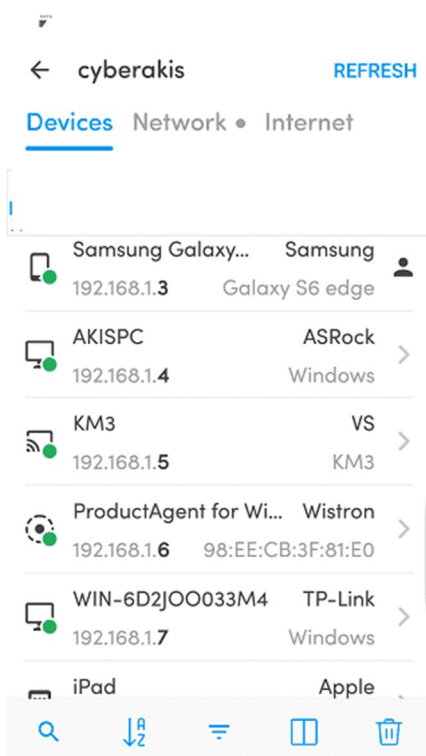
Άλλη μία χρήσιμη δυνατότητα είναι ότι μας επιτρέπει να ελέγχουμε απομακρυσμένα μέσω του λογαριασμού μας στον browser, αν κάποιος κλέβει το WiFi στην οικία, στο γραφείο, ή σε οποιοδήποτε άλλο απομακρυσμένο προσωπικό μας χώρο που έχουμε router και ασύρματο δίκτυο.

Cosmote in Pátrai (192.168.1.0...)			
8	Computer	Samsung	
Discovered	Most popular of 7 types	Most popular of 7 vendors	
	192.168.1.1	speedport.ip	Router Sercomm / Speedport
	192.168.1.2	[TV] Samsung 7 Series (49)	Television Samsung / NU7100 Ultra HDR Smart 4K TV
	192.168.1.3	Samsung Galaxy S6 edge	Mobile Samsung / Galaxy S6 edge
	192.168.1.4	AKISPC	Computer
	192.168.1.5	TV BOX	Alerted Media Player VS / KM3
	192.168.1.6	PREDATOR: [blurred]	Desktop Acer / Predator G6-710
	192.168.1.7	WIN-6D2J00033M4	Computer
	192.168.1.8	iPad	Tablet Apple / iPad

Επιπλέον, μπορούμε να ειδοποιούμαστε για τυχόν αλλαγές στις συνδεδεμένες συσκευές του ασύρματου δικτύου που παρακολουθούμε απομακρυσμένα. Αρκεί να έχουμε εγκαταστήσει και τρέξει το Fing σε κάποια συσκευή αυτού του δικτύου.



Αν δεν θέλουμε να κατεβάσουμε το πρόγραμμα στο PC, οι ενέργειες του ελέγχου για άγνωστες συσκευές στο συγκεκριμένο ασύρματο δίκτυο που βρισκόμαστε εκείνη τη στιγμή είναι παρόμοιες και στο Android και iOS app. Η μόνη διαφορά είναι κάποιες διαφημίσεις.



Έλεγχος με το WNetWatcher

Το Wireless Network Watcher είναι ένα πολύ μικρό πρόγραμμα της εταιρείας Nirsoft. Μας επιτρέπει να ελέγξουμε τις συσκευές που συνδέονται στο router και αν κάποιος μας κλέβει το WiFi.

Καλό είναι να κατεβάσουμε την συμπιεσμένη μορφή, καθαρά για λόγους απλότητας και ευχρηστίας του προγράμματος. Αποσυμπιέζουμε το .zip αρχείο και είμαστε έτοιμοι να το εκτελέσουμε.

Feedback

If you have any problem, suggestion, comment, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com

[Download Wireless Network Watcher \(In Zip file\)](#)

[Download Wireless Network Watcher with full install/uninstall support \(wnetwatcher_setup.exe\)](#)

[Check Download MD5/SHA1/SHA256 Hashes](#)

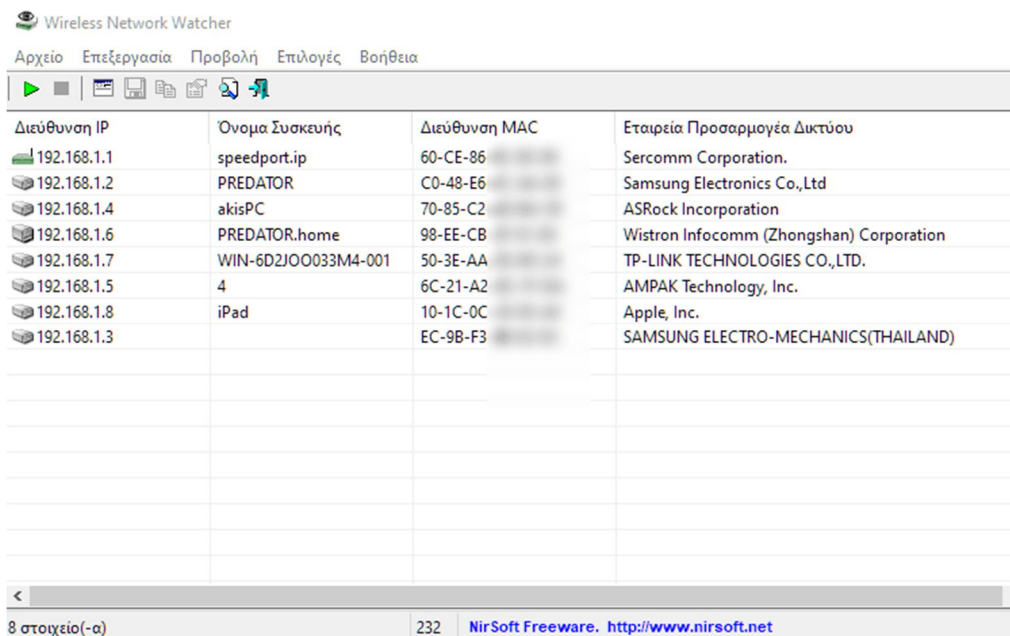
Επιπλέον, έχουμε τη δυνατότητα να επιλέξουμε την ελληνική έκδοση του προγράμματος, αποσυμπιέζοντας το .ini αρχείο στον ίδιο φάκελο. Με άλλα λόγια, μεταφέρουμε το αρχείο της γλώσσας μέσα στον φάκελο με το όνομα WNetWatcher.

French	Eric FICHOT,Largo	24/01/2018	2.16
German	«Latino» auf WinTotal.de	21/06/2020	2.22
Greek	Θανάσης Κατσαγιώργης	20/05/2012	1.45
Gujarati	Jay Simmons	22/04/2019	2.20
Hebrew	Aharon Don	29/02/2020	2.21
Hellenic	Ἐπίκουρος Ἐαδούααβηῆαῖο	12/07/2011	1.00
Hungarian	tpr / Koncz László	27/04/2016	1.97
Indonesian	Ivan Dhuha Firmansyah	17/10/2016	2.02
Italian	Alessandro Viscone	09/06/2019	2.20

Όνομα	Ημερομηνία τροποποι...	Τύπος	Μέγεθος
readme.txt	20/6/2020 5:34 μμ	Εγγραφο κειμένου	20 KB
WNetWatcher.cfg	16/7/2020 1:35 μμ	Αρχείο CFG	4 KB
WNetWatcher.chm	20/6/2020 5:34 μμ	Αρχείο μεταλωτ...	19 KB
WNetWatcher.exe	20/6/2020 5:34 μμ	Εφαρμογή	371 KB
WNetWatcher_Ing.ini	20/5/2012 11:16 μμ	Ρυθμίσεις παραμέ...	4 KB

Από εκεί και μετά, μπορούμε να ανοίξουμε το πρόγραμμα και η σάρωση των συσκευών γίνεται αυτόματα. Θα δούμε αμέσως τις MAC και IP διευθύνσεις των συσκευών που συνδέονται στο router.

Μπορούμε, επίσης, να εξαγάγουμε τη λίστα συνδεδεμένων συσκευών σε αρχείο html / xml / csv / text, ή να αντιγράψουμε τη λίστα στο πρόχειρο και στη συνέχεια να την επικολλήσουμε στο Excel, ή σε άλλη εφαρμογή Office.



Διεύθυνση IP	Όνομα Συσκευής	Διεύθυνση MAC	Εταιρεία Προσαρμογέα Δικτύου
192.168.1.1	speedport.ip	60-CE-86	Sercomm Corporation.
192.168.1.2	PREDATOR	C0-48-E6	Samsung Electronics Co.,Ltd
192.168.1.4	akisPC	70-85-C2	ASRock Incorporation
192.168.1.6	PREDATOR.home	98-EE-CB	Wistron Infocomm (Zhongshan) Corporation
192.168.1.7	WIN-6D2J0O033M4-001	50-3E-AA	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.5	4	6C-21-A2	AMPAK Technology, Inc.
192.168.1.8	iPad	10-1C-0C	Apple, Inc.
192.168.1.3		EC-9B-F3	SAMSUNG ELECTRO-MECHANICS(THAILAND)

Εφόσον εντοπίσουμε μία συσκευή που δεν ανήκει σε εμάς, και θεωρούμε ότι μπορεί να κλέβει το WiFi, πρέπει αμέσως να πάρουμε τα μέτρα μας και να αλλάξουμε τους κωδικούς πρόσβασης.

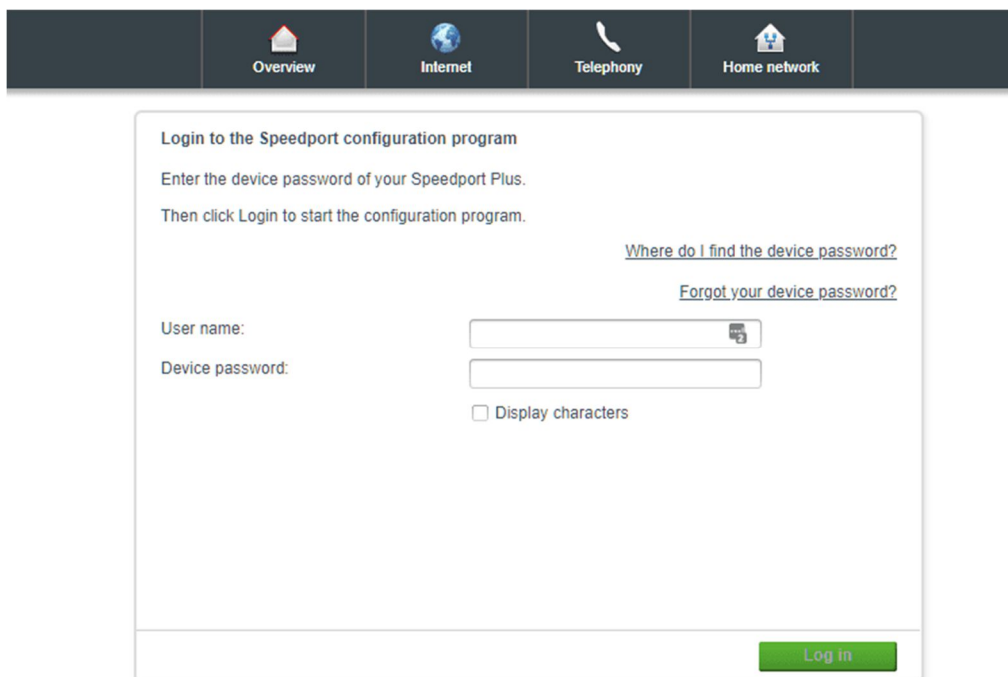
Έλεγχος μέσα από το περιβάλλον του router

Είναι γεγονός ότι ανάλογα τον κατασκευαστή και το μοντέλο, τα router έχουν διαφορετικό διαχειριστικό περιβάλλον. Επιπλέον, πολλά router ενδέχεται να μην μας παρέχουν πλήρη πρόσβαση σε αυτές τις πληροφορίες που είδαμε προηγουμένως.

Ως εκ τούτου, αυτή η μέθοδος ίσως είναι λιγότερο βολική σε σχέση με τους αυτοματισμούς του Fing και Wireless Network Watcher.

Σε κάθε περίπτωση, για να μπούμε στο web interface του router, πληκτρολογούμε την IP του router. Συνήθως είναι 192.168.0.1, 192.168.1.1, ή 10.0.0.1. Για να βρείτε την ακριβή διεύθυνση, αν δεν τη γνωρίζετε, θα βρείτε τη διαδικασία στον οδηγό μας:

Στο διαχειριστικό περιβάλλον του router θα μας ζητηθεί να εισάγουμε το username και το password για να συνδεθούμε.



Overview Internet Telephony Home network

Login to the Speedport configuration program

Enter the device password of your Speedport Plus.
Then click Login to start the configuration program.

[Where do I find the device password?](#)

[Forgot your device password?](#)

User name:

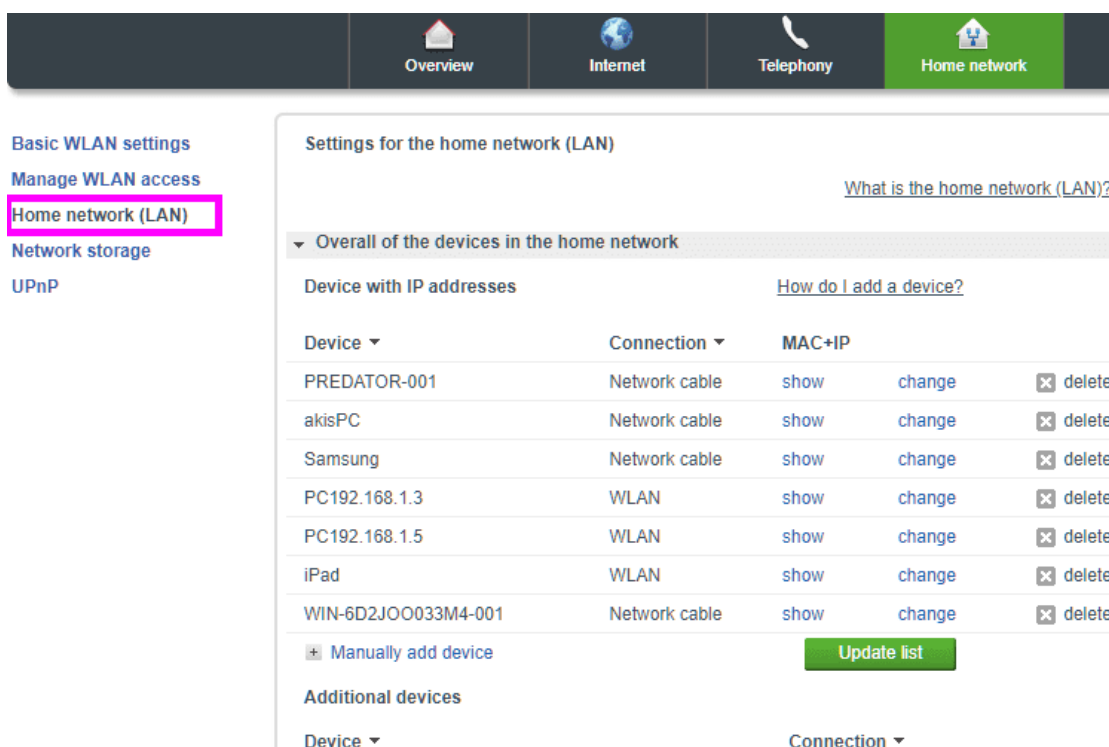
Device password:

Display characters

Log in

Αν φυσικά δεν γνωρίζουμε τον κωδικό χρήστη και το κλειδί, είμαστε αναγκασμένοι να τα αναζητήσουμε είτε στο εγχειρίδιο χρήσης του router, είτε στη σελίδα του κατασκευαστή. Δείτε περισσότερες πληροφορίες στον οδηγό για τον Κωδικό Router.

Από εκεί και μετά, για να δούμε ποιες συσκευές συνδέονται στο router, απλά ψάχνουμε από το μενού να βρούμε το LAN. Στο διαχειριστικό του router του ΟΤΕ ξεκινάμε από το Home network.



Overview Internet Telephony Home network

Basic WLAN settings
Manage WLAN access
Home network (LAN)
Network storage
UPnP

Settings for the home network (LAN)

[What is the home network \(LAN\)?](#)

Overall of the devices in the home network

Device with IP addresses [How do I add a device?](#)

Device	Connection	MAC+IP		
PREDATOR-001	Network cable	show	change	delete
akisPC	Network cable	show	change	delete
Samsung	Network cable	show	change	delete
PC192.168.1.3	WLAN	show	change	delete
PC192.168.1.5	WLAN	show	change	delete
iPad	WLAN	show	change	delete
WIN-6D2JOO033M4-001	Network cable	show	change	delete

[Manually add device](#) [Update list](#)

Additional devices

Device Connection

Τα έξτρα βήματα για την προστασία του WiFi

Δεν χωρά αμφιβολία ότι το WPA2 έχει αυξήσει σημαντικά την ασφάλεια του ασύρματου δικτύου. Χρησιμοποιεί ισχυρά πρωτόκολλα κωδικοποίησης, αποθαρρύνοντας έτσι τον επιτήδειο που θέλει να μας κλέβει το WiFi.

Όμως, δεν πρέπει να ξεχνάμε ότι το ασύρματο δίκτυο λειτουργεί σαν το σπίτι μας: Μπορεί να έχουμε πόρτα ασφαλείας, αλλά πρέπει να την κλειδώνουμε για να είμαστε ασφαλείς.

Είναι πιθανό φίλοι, γείτονες, ή μέλη της οικογένειας, να έχουν μοιραστεί τα συνθηματικά του WiFi με άλλους και άτομα που δεν γνωρίζουμε. Μπορεί και εμείς οι ίδιοι να τα είχαμε δώσει σε κάποιον γνωστό μας.

Ως εκ τούτου, όλοι αυτοί θα μπορούσαν να έχουν πρόσβαση στο δίκτυό μας και στα κοινόχρηστα αρχεία μας. Επομένως, είναι απαραίτητο να προχωρήσουμε σε κάποιες ενέργειες που ίσως αμελήσαμε να τις κάνουμε ευθύς εξαρχής.

Βήμα 1 - Αλλάζω αμέσως τον εργοστασιακό κωδικό του router

Είναι γεγονός ότι πολλοί χρήστες ακολουθούν τη επικίνδυνη χρήση του εργοστασιακού κωδικού του router. Αν ανήκουμε σε αυτή την κατηγορία χρηστών και δεν έχουμε μπει ακόμη στον κόπο να τον αλλάξουμε, πρέπει να σπεύσουμε άμεσα.

Σε αντίθετη περίπτωση, είναι πολύ εύκολο κάποιος να μας κλέβει το WiFi. Ο λόγος είναι ότι υπάρχουν πολλά προγράμματα που εντοπίζουν τον εργοστασιακό κωδικό ανά μοντέλο router. Κάποια άλλα σπάνε ακόμη πιο γρήγορα και εύκολα τους κωδικούς.

Βήμα 2 - Βεβαιώνομαι ότι έχω WPA2 και AES

Όπως αναφέραμε προηγουμένως, είναι παραπάνω από απαραίτητο να χρησιμοποιούμε το πρότυπο κρυπτογράφησης WPA2 με έναν ισχυρό κωδικό πρόσβασης.

Μόλις ορίσουμε το WPA2, αν είναι παλιό το router, βεβαιωνόμαστε ότι χρησιμοποιούμε κρυπτογράφηση AES αντί για TKIP.

WLAN Name (SSID)	<input type="text" value="cyberakis"/>
WLAN name visibility	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible What does visibility of the WLAN name mean?
Enable SSID	<input checked="" type="checkbox"/>
Enable SSID Isolation	<input type="checkbox"/>
Maximum Clients	<input type="text" value="32"/> (1 ~ 32)
Encryption Type	<input type="text" value="WPA/WPA2-Personal"/> <ul style="list-style-type: none"> WPA/WPA2-Personal <li style="background-color: #e0e0e0;">WPA2-Personal (very secure) WPA/WPA2-Personal WPA2-Enterprise WPA/WPA2-Enterprise WEP (low security level) Unencrypted (not recommended)
Encryption Method	Types of encryption?
WLAN key	

Έτσι, αν μας ξέφυγε και χρησιμοποιούμε το WEP, πρέπει να το αλλάξουμε αμέσως. Το WEP είναι πολύ εύκολο να σπάσει. Ως εκ τούτου, είναι η χαρά του power user γείτονα που θέλει να το παίξει hacker και να μας κλέβει το WiFi.

Βήμα 3 - Απενεργοποιώ το WPS & UPnP

Η ιδέα πίσω από το WiFi Protected Setup (WPS) είναι να διευκολύνει τη σύνδεση νέων συσκευών στο δίκτυο με ένα πάτημα στο σχετικό πλήκτρο. Είναι μια δυνατότητα που την συναντάμε σε πολλά σύγχρονα router.



Όμως, το WPS, εφόσον διατίθεται, είναι μία άλλη πιθανή σοβαρή ευπάθεια. Μπορεί να αξιοποιηθεί εύκολα από κάποιον για να αποκτήσει πρόσβαση στο ασύρματο δίκτυο μας.

Το UPnP (Universal Plug and Play) επιτρέπει την άμεση επικοινωνία μεταξύ διαφορετικών συσκευών σε ένα ασύρματο δίκτυο. Δυστυχώς, το UPnP είναι γεμάτο

από κενά ασφαλείας και πρέπει να το απενεργοποιήσουμε το συντομότερο δυνατό στον router.

Αν χρησιμοποιούμε το Plex για απομακρυσμένη πρόσβαση στον Plex Media Server έξω από το τοπικό μας δίκτυο, η απενεργοποίηση του UPnP θα προκαλέσει αστοχίες στην πρόσβαση.

Βήμα 4 - Βάζω φράση για κωδικό πρόσβασης

Για ακόμη περισσότερο ασφάλεια, μπορούμε να εξετάσουμε μία φράση πρόσβασης που έχει σύνθετους χαρακτήρες. Με αυτόν τον τρόπο, θα είναι εξαιρετικά δύσκολο πλέον για τον οποιοδήποτε να αποκτήσει πρόσβαση στο WiFi μας.

<p>UNCOMMON (NON-GIBBERISH) BASE WORD ORDER UNKNOWN</p> <p>Tr0ub4dor &3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CATCHING A STOLEN MESH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

Βήμα 5 - Σύνδεση με Ethernet

Όπως είδαμε, η σύνδεση στον πίνακα διαχείρισης του router μας είναι ιδιαίτερα απλή. Πληκτρολογούμε μία διεύθυνση IP στον browser και εισάγουμε τα συνθηματικά μας.

Όμως, αν η σύνδεση στο router γίνεται μέσω ασύρματου δικτύου, αυτά τα διαπιστευτήρια σύνδεσης είναι ο κεντρικός στόχος αυτού που θέλει να κλέβει το WiFi. Ως εκ τούτου, αν η σύνδεση γίνεται μόνο μέσω Ethernet, μπορούμε να εξαλείψουμε αυτόν τον κίνδυνο.



Για περισσότερη ακόμη ασφάλεια, εφόσον αυτό είναι δυνατό, μπορούμε να συνδέσουμε με ένα καλώδιο Ethernet τις συσκευές που το επιτρέπουν, όπως τα laptop, TV Box, Smart TV, απευθείας στον router.

Τι άλλο να κάνω αν κάποιος κλέβει το WiFi?

Στη περίπτωση που ανακαλύψουμε ότι άγνωστες συσκευές συνδέονται στο router μας, δεν έχουμε παρά να αλλάζουμε αμέσως τους κωδικούς πρόσβασης με νέους πιο ισχυρούς για να θωρακίσουμε το δίκτυο.

Φυσικά, μπορούμε να επικοινωνήσουμε και με τη δίωξη ηλεκτρονικού εγκλήματος μέσω της ηλεκτρονικής πλατφόρμας υποβολής καταγγελιών, ή στο 11188. Θα μας καθοδηγήσουν όσον αφορά τη σχετική διαδικασία.

Το παραπάνω κείμενο αποτελεί αποδελτίωση άρθρου του [Άκη Τίγκα](#) στο περιοδικό PC STEPS