

# OUCH!

## NË KËTË NUMËR..

- Rrjeti juaj pa tel (Wireless)
- Pajisjet tuaja

## Mbrojtja e rrjetit tuaj të shtëpisë

### Përmbledhje

Para disa vitesh rrjetet shtëpiake ishin relativisht të thjeshtë, zakonisht nuk kishte më shume se një qendër qasjeje pa tela dhe një a dy kompjuterë që përdorëshin për t'u lidhur në internet, për të blerë diçka online apo për lojëra. Mirëpo rrjetet shtëpiake po bëhen çdoherë e më komplekse. Ne tani lidhemi në shumë më shumë pajisje në këto rrjete dhe i përdorim ato për më shumë arsye se sa thjesht shfletim i internetit apo hapja e mediave. Në këtë broshurë ne do të mbulojmë disa këshilla se si ju mund të krijoni një rrjet të sigurt në shtëpi për ju dhe familjen tuaj.

### Botuesi i ftuar

Cheryl Conley e udhëheq ekipin 'Security Education and Awareness' në Lockheed Martin, duke forcuar iniciativën The I Campaign™ e cila prek mbi 100,000 punëtorë. Kjo iniciativë përfshin grupet e aleancave dhe të avokimit të sigurisë në korporata, në vazhdimësi të programit global mbi 'phishing'-un. Ndiqeni Cheryl-in në [@conleychera](https://twitter.com/conleychera).

### Rrjeti juaj pa tel

Gati secili rrjet shtëpie fillon me një rrjet pa tel (ang. Wireless), i cili nganjëherë njihet edhe me emrin rrjeti Wi-Fi. Kjo është ajo që mundëson që ju të lidhni pa tel cilëndo nga pajisjet tuaja në internet, nga laptopët dhe tabletët te konzollat për lojëra dhe televizorët. Shumë rrjete shtëpiake pa tel kontrollohen nga ruteri juaj i internetit, që është një pajisje që operatori i internetit jua ka instaluar juve për t'ju lidhur në internet. Por në disa raste rrjeti juaj pa tel mund të kontrollohet nga një sistem tjetër i njohur si pika lidhëse pa tel (ang. Wireless access point) që lidhet me ruterin e internetit. Pa marrë parasysh se cilën mënyrë e shfrytëzoni të dyjat funksionojnë pak a shumë në të njëjtën mënyrë duket shpërndarë sinjale pa tel. Pajisjet e ndryshme në shtëpinë tuaj lidhen me rrjetin pa tel me anë të këtyre sinjaleve. Nga aty, këto pajisje pastaj lidhen në Internet, e poashtu edhe me pajisjet tjera në rrjet. Kjo nënkupton që mbrojtja e rrjetit tuaj pa tel është pikë kryesore e mbrojtjes së shtëpisë suaj. Ne ju rekomandojmë që t'i ndiqni këta hapa për ta mbrojtur atë.

- Ndërroni fjalëkalimin fillestar të administratorit me anë të cilit lidheni në ruterin e internetit apo në pikën lidhëse pa tel (ang. wireless access point). Llogaria e administratorit është ajo që ju mundëson ndryshimin e detajeve teknike për rrjetin tuaj pa tel. Problemi është se shumica e ruterëve të internetit dhe atyre pa tel kur blihen vijnë me një fjalëkalim i cili është i njohur dhe shpesh gjindet lehtë në Internet. Prandaj sigurohuni që ta ndërroni këtë fjalëkalim dhe ta bëni një të fortë, të veçantë që e dini vetëm ju.
- Ndërroni emrin fillestar të rrjetit pa tel (nganjëherë i njohur si SSID). Ky është emri të cilin do ta shohin pajisjet tuaja kur e kërkojnë rrjetin pa tel për tu lidhur. Jepini rrjetit tuaj një emër unik që vetëm ju mund ta identifikoni,

## Mbrojtja e rrjetit tuaj të shtëpisë

por sigurohuni që nuk përmban ndonjë detaj apo informatë personale. Ka pak vlerë në konfigurimin e rrjetit tuaj si të fshehur (ang. Non-broadcast) sepse shumica e pajisjeve skanuese ose ndonjë sulmues i shkathhtë mund ta gjejë fare lehtë një rrjet të fshehur.

- Sigurohuni që vetëm njerëzit e besueshëm mund të lidhen dhe ta përdorin rrjetin tuaj pa tel, dhe ato lidhje janë të enkriptuara. Bëjeni këtë duke aktivizuar siguri të lartë. Për momentin opsioni më i mirë është të përdoret mekanizmi i sigurisë që quhet WPA2. Duke e aktivizuar këtë fjalëkalimi do të kërkohej gjithmonë për personat që lidhen në rrjet, dhe kur ata lidhen atëherë aktivitetet online janë të enkriptuar. Sigurohuni që nuk përdorni metoda të vjetra si WEP apo asnjë metodë sigurie, që ndryshe njihet si rrjet i hapur (ang. Open network). Rrjetet e hapura i lejojnë kujt do të lidhen në rrjetin tuaj pa tel pa asnjë autentifikim apo vërtetim autorizimi.
- Sigurohuni që fjalëkalimi që njerëzit përdorin për tu lidhur në rrjetin tuaj pa tel është fjalëkalim i fortë dhe i ndryshëm nga fjalëkalimi i llogarisë së administratorit. Mbani mend që fjalëkalimi mund të nevojitet të vendoset vetëm një herë për secilën pajisje tuaj, sepse fjalëkalimi mund të ruhet pas vendosjes së parë.
- Shumë rrjete pa tel përkrahin funksionin që quhet rrjeti për mysafirë (ang Guest Network). Kjo i lejon vizitorët të lidhen në Internet, por e mbron rrjetin tuaj të shtëpisë ashtu që ata nuk mund të lidhen në ndonjë pajisje tjetër në rrjetin e brendshëm. Nëse shtoni një rrjet për mysafirë, sigurohuni që të aktivizoni WPA2 si dhe një fjalëkalim unik për këtë rrjet.
- Çaktivizoni funksionin “WiFi Protected Setup” ose ndonjë mekanizëm tjetër që ju mundëson të lidhni një pajisje në rrjet pa e ditur fjalëkalimin apo opsionet tjera të konfigurimit
- Nëse keni vështirësi t’i mbani mend të gjithë fjalëkalimet, ne ju rekomandojmë të përdorni një menaxhues fjalëkalimesh që t’i ruajë ata për ju.



*Për ta mbrojtur rrjetin tuaj të shtëpisë sigurojeni rrjetin tuaj pa tel, përditësoni atë dhe mbroni me fjalëkalim të gjitha pajisjet në rrjet.*

Nuk jeni të sigurt si t’i realizoni këta hapa? Pyeteni operatorin e shpërndarjes së internetit, lexoni dokumentacionin me të cilin e keni pranuar ruterin e internetit apo pajisjen shpërndarëse të rrjetit pa tel, ose shihni faqen e internetit të prodhuesit.

### Pajisjet tuaja

Hapi tjetër është të dini se çka është lidhur në rrjetin tuaj të shtëpisë dhe të siguroheni që ato pajisje janë të sigurta. Kjo dikur ishte e thjeshtë sepse kishte shumë pak pajisje të lidhura. Por në botën e sotme ‘gjithmonë të lidhur’ gati çdo pajisje

## Mbrojtja e rrjetit tuaj të shtëpisë

mund të lidhet me rrjetin tuaj, duke përfshirë këtu TV, konzolat për lojëra, monitorët e fëmijëve, dëgjueset, termostati juaj e ndoshta edhe vetura juaj. Një mënyrë e thjeshtë për ta zbuluar se kush është lidhur në rrjetin tuaj të shtëpisë është të përdorni një skaner të njohur me emrin Fing. Këto aplikacione, që mund t'i instaloni në kompjuterin apo pajisjen tuaj mobile, e skanojnë rrjetin tuaj pa tel dhe ju raportojnë për secilën pajisje të lidhur në rrjet. Kur t'i keni identifikuar të gjitha pajisjet në rrjet, ju duhet të siguroheni që secila nga ato është e sigurt. Mënyra më e mirë për ta bërë këtë është të siguroheni që ato kanë të instaluar sistemin operativ të fundit. Kur është e mundur, aktivizoni përditësimin automatik. Nëse ndonjë nga pajisjet tuaja kërkon fjalëkalim, atëherë përdorni një fjalëkalim unik dhe të fortë. Në fund, sigurohuni që të hyni në faqen e internetit të shpërndarësit të internetit, sepse mund t'ju ofrojnë edhe ata ndonjë aplikacion për mbrojtjen e rrjetit tuaj të shtëpisë.

### Mëso më shumë

Regjistrohuni në buletin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen <http://www.securingthehuman.org>.

### Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyesë profesionale e gjuhës angleze në OSBE.

### Burimet

Pasfrazat:	<a href="https://securingthehuman.sans.org/ouch/2015#april2015">https://securingthehuman.sans.org/ouch/2015#april2015</a>
Menaxhuesit e fjalëkalimeve:	<a href="https://securingthehuman.sans.org/ouch/2015#october2015">https://securingthehuman.sans.org/ouch/2015#october2015</a>
Mbrojtja e tabletit tuaj të ri:	<a href="https://securingthehuman.sans.org/ouch/2016#january2016">https://securingthehuman.sans.org/ouch/2016#january2016</a>
Krijimi i hartës së rrjetit tuaj të shtëpisë:	<a href="http://l.rud.is/home-network-mapping">http://l.rud.is/home-network-mapping</a>

OUCH! botohet nga SANS Securing The Human dhe shpërndahet nën licencën [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Lejohet ta shpërndani këtë buletin ose ta përdorni për programet tuaja vetëdijësuese, për sa kohë nuk e modifikoni përmbajtjen e buletinit. Për përkthimet apo më shumë informata, ju lutemi na kontaktoni në [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org).

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis  
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano



[securingthehuman.org/blog](https://securingthehuman.org/blog)



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gpl](https://securingthehuman.org/gpl)