



GHID

Securitatea utilizatorului final

Ghid realizat de către:

RCS & RDS

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO

BE AWARE, BE SECURE.

www.enisa.europa.eu/cybersecmonth

www.cert-ro.eu/tag/ecsm

Pagină alba

CUPRINS

1. SPAM	4
2. BLOCAREA PORTULUI 25 (SMTP)	7
3. VIRUȘI.....	8
4. PHISHING	11
5. SPYWARE	12
6. SECURITATEA ÎN REțeleLE WI-FI	13

Scopul prezentului document este de a familiariza cititorii cu noțiunile de bază privind tipurile de amenințări informatice, precum și de a propune o serie de practici menite să protejeze sistemul și datele personale, în timpul navigării pe internet.

1. Spam

SPAM - ce reprezintă

Definiție: SPAM (în limba engleză), desemnează în general mesaje electronice trimise către o multitudine de destinatari în scopuri publicitare sau nelegale fără acordul acestora.

Ce intră în această categorie:

- mesaje publicitare nesolicitate
- mesaje ce urmăresc realizarea unei fraude prin obținerea de date confidențiale.

Oricare dintre aceste tipuri de mesaje reprezintă o pierdere de timp, energie și resurse pentru destinatari, furnizorii de servicii și comunitatea utilizatorilor de Internet. Orice deținător al unui cont de email a observat că acest fenomen a scăpat de sub control. Statisticile realizate de RCS&RDS arată că în ultimul an mesajele nesolicitate reprezintă aproximativ 70% din totalul traficului de poștă electronică. RCS&RDS a decis să ia măsuri atât pentru a proteja utilizatorii cât și propria rețea. Măsurile includ instalarea de software dedicat antivirus, antispam și toleranță minimă față de aceste practici.

Are mai multe forme:

- un necunoscut vă propune să vizitați un site sau să faceți o afacere, cel mai probabil ilegale
- o listă de trimitere de mesaje pe care ați fost înscris fără știrea dumneavoastră și primiți mesaje prin care sunteți invitat să comandați diverse produse sau servicii

Sinonime:

- mesaje nesolicitate
- mesaje comerciale nesolicitate
- mesaje trimise în masă

Consecințe:

- umplerea căsuței cu mesaje nedorite
- pierderea de timp cu citirea mesajelor și stergerea lor

Politica antispam a RCS&RDS

RCS&RDS are o politică împotriva mesajelor nesolicitate; conform politicii de utilizare a serviciului:

Beneficiarilor RCS&RDS sau oricăror terți care folosesc rețeaua RCS&RDS le este interzis și nu trebuie să permită la rândul lor să folosească rețeaua RCS&RDS pentru a trimite SPAM-uri și de a abuza de ea. În cazul în care se trimit email-uri în masă, expeditorii trebuie să păstreze date ce atesta aprobarea fiecărui destinatar de a primi astfel de mesaje înainte ca mesajele să fie trimise. Dacă astfel de dovezi nu există, RCS&RDS poate considera după propria sa apreciere că aprobarea nu a fost obținută și va considera abuzivă utilizarea rețelei.

Procedura de răspuns la plângeri

Iată pașii urmați dacă s-a primit o plângere referitoare la mesaje nesolicitate trimise de un abonat.

- La primirea plângerii este realizată evaluarea acesteia și se anunță abonatul de violarea politicii de utilizare a serviciului.
- Conexiunea sau serviciul sunt suspendate temporar, până la rezolvarea problemelor. RCS&RDS poate decide dacă va continua sau nu contractul cu abonatul responsabil de abuzuri.
- Reconectarea se realizează în urma trimiterii unui fax în care se specifică modalitatea de rezolvare a problemei.

Cum încearca să prevină RCS&RDS SPAM-ul?

Software-ul folosit de RCS&RDS nu permite utilizatorilor relay prin alte servere de mail. Impune, de asemenea, anumite limite pentru numărul de mesaje trimise într-o perioadă de timp definită. Ca urmare, trimiterea unui număr mare de mesaje prin intermediul serverelor RCS&RDS este aproape imposibilă.

Cum vă protejați?

- Folosiți software specializat pentru a vă securiza calculatorul.
- Marea majoritate a utilizatorilor ce abuzează de servicii nu au cunoștință de faptul că pe sistemul lor există un virus, robot sau troian.
- Actualizați sistemul de operare și programele la ultimele versiuni disponibile; instalați update-urile de securitate pentru a avea un calculator neinfecat.
- Nu răspundeți mesajelor ce vă trezesc suspiciunea; veți arăta astfel că adresa dumneavoastră de mail este validă.

Cine practică spamul și de ce este atât de răspândit?

Trimiterea unui mesaj la milioane de persoane este simplă și benefică financiar pentru cei ce desfășoară acest gen de activități. Chiar dacă numărul de persoane care șterg mesajul este mare, cei ce cumpără produsul fac ca această activitate să fie profitabilă.

Există mai multe metode de trimitere:

- o metodă folosită în proporții industriale presupune deturnarea calculatoarelor utilizatorilor (folosind un virus sau alte programe malițioase) și folosirea lor pentru a trimite un mare număr de mesaje, ascunzând astfel identitatea adevăratei persoane care face trimiterea (sistemele respective poartă numele de 'zombie'). Spamul trimis în acest fel ajunge la 4/5 din totalul mesajelor nedorite trimise în Internet
- restul este reprezentat de mesaje trimise de persoane al căror profil nu este bine definit (mesaje care promovează un site sau companii care își promovează produsele)

Liste de mesaje – a nu se confunda cu spamul!

Dacă sunteți abonat al unei companii și ați acceptat să primiți informații legate de această companie sau produsele ei, puteți fi destinatarul unor oferte comerciale. În acest caz nu este vorba de spam, adresa de mail fiind obținută cu acordul dumneavoastră. Puteți, în general, să vă dezabonați în orice moment și să nu mai primiți aceste mesaje.

Ce trebuie să fac pentru ca mesajul meu să nu fie "confundat" cu un SPAM ?

RCS& RDS a implementat instrumentul Sender Policy Framework (SPF), care vă protejează de mesajele de tip SPAM atât pe dvs, cât și pe cei cărora le trimiteți e-mailuri. SPF este o metodă de prevenire a falsificării adresei de e-mail a expeditorului unui mesaj.

Datorită acestui tip de protecție, este posibil ca unele dintre mesajele trimise de pe adresa numeledvs@rdslink.ro prin alte servere de mail decât cele oferite clienților de către RCS& RDS, să fie interpretate de serverele care găzduiesc adresele la care trimiteți e-mail-uri, drept SPAM. Unele servere șterg automat aceste SPAM-uri. Dacă doriți să transmiteți e-mail-uri prin alte servere decât cele oferite de RCS& RDS fără riscul ca ele să fie interpretate drept SPAM, vă rugăm faceți următoarea setare în clientul dvs. de e-mail (Outlook Expres de ex.):

- în câmpul FROM: tastați adresa de pe care doriți să trimiteți e-mail-uri, alta decât cea de pe domeniul rdslink.ro (de ex. cea de tipul numeledvs@companiaX.ro)

În acest fel, mesajul dumneavoastră care este transmis de pe o adresă diferită de cea de pe rdslink.ro, va ajunge cu siguranța la destinație.

2. Blocarea portului 25 (SMTP)

Ce înseamna blocarea portului 25 (SMTP)?

Portul 25 este folosit de serviciul de mesagerie electronică (e-mail). RCS&RDS a decis să ia măsuri pentru a proteja atât utilizatorii de internet cât și propria rețea, permițând accesul doar la propriile servere SMTP.

De ce ați luat această măsură?

Pe lângă mesajele legitime, o mare cantitate de SPAM este trimisă către diverse adrese, afectând în mod direct destinatarii și rețeaua furnizorului de unde sunt trimise. Măsura de a limita accesul la serviciul SMTP doar către serverele RCS&RDS a fost necesară pentru reducerea cantității de spam trimis prin intermediul rețelei RCS&RDS, cu încălcarea regulilor de utilizare a rețelei și/sau serviciilor RCS&RDS.

Ce trebuie să fac eu?

În cazul în care folosiți pentru trimiterea mesajelor serverele RCS&RDS nu este nevoie să faceți absolut nimic, beneficiind fără nicio întrerupere sau schimbare de configurație de serviciile de mail oferite de RCS&RDS.

Serverul SMTP folosit pentru trimiterea de mesaje este smtp.rdslink.ro.

Voi putea folosi în continuare adresa mea de mail de la yahoo.com, gmail.com, etc?

Da, RCS&RDS nu limitează accesul la serviciile webmail oferite de nici o altă companie.

Folosesc alte servere SMTP. Cum le pot folosi în continuare?

Aveți mai multe variante pentru a face acest lucru:

- Folosiți o sesiune criptată (SMTP peste SSL) cu serverul dumneavoastră; aceasta folosește implicit portul 465.
- Folosiți o sesiune VPN până la locul unde funcționează serverul. Este varianta care va permite accesul la toate resursele organizației al cărei server doriți să îl folosiți.
- RCS&RDS pune la dispoziția abonaților un sistem prin care va fi solicitat accesul la această resursă prin intermediul unei interfețe web (momentan doar pentru abonatii FiberLink) aflată la adresa <https://digicare.rcs-rds.ro>.

Ce se întâmplă dacă după ce mi-a fost permis accesul se consideră ca am făcut un abuz?

Accesul va fi restricționat și veți putea face o nouă cerere doar după ce veți dovedi că ați remediat problema. Aveți acces de asemenea, și la istoricul problemelor.

Cum procedez dacă am în continuare probleme la trimiterea mesajelor?

Vă recomandăm să contactați departamentul suport tehnic din orașul dumneavoastră folosind detaliile de contact.

3. Viruși

Ce este un virus?

Un virus este un program capabil să se reproducă în mod repetat și să cauzeze defecțiuni fișierelor (datelor personale) și sistemului de operare aflate pe computerul infectat. Unii viruși acționează imediat ce au infestat calculatorul gazdă, alții asteaptă pasivi până când sunt rulați (executați/ porniți) de un anumit program.

Cum ne infestăm cu viruși ?

În trecut, virușii se raspândeau cel mai des pe dischete de date floppy, împrumutate de la un utilizator la altul. Odată ce conexiunile la internet au devenit din ce în ce mai populare, virușii se transmit mai mult prin e-mail, descărcând programe de pe internet sau folosind programe peer2peer (două calculatoare conectate unul la celălalt prin intermediul internetului).

Ce caracteristici au virușii ?

- pot fi rezidenți sau non-rezidenți în memorie : un virus e rezident atunci când el se încarcă în memoria calculatorului și apoi infectează calculatorul și e nonrezident când acționează numai dacă un anumit fișier este deschis sau o anumită comandă este executată.
- pot acționa chiar și dacă un fișier infectat este doar copiat – dacă un virus este rezident în memorie, el se va încărca singur în memoria calculatorului și va acționa apoi asupra fișierelor la care are acces.
- pot fi polimorfi – orice virus are un cod care îl definește, care poate fi înțeles ca o secvență de program care îi spune cum să acționeze; virușii polimorfi sunt cei care își pot modifica secvențele de cod, astfel ca forma sub care circulă pe internet poate varia, pentru a se camufla mai eficient (există viruși care circulă pe e-mail și care pot schimba titlul mailului pentru a-l face mai « atrăgător »)
- Pot fi « deghizați » - mai întâi se atașează fișierelor computerului și abia apoi ataca, astfel viteza cu care se răspândesc fiind mult mai mare.
- Pot fi însoțiți și de alți viruși : dacă e cazul, un virus poate veni însoțit și de alt program nociv, dar cu altă funcție, atunci când infectează o gazdă (computer).
- Pot modifica sistemul de operare astfel încât să nu mai semnaleze disfuncționalități.

Cum modifică virușii fișierele ?

- virușii pot ataca toate fișierele, dar vor ataca preponderent fișierele executabile și de sistem (.exe, .com, .bat, .pif, .sys, .bin) și fișierele de date (word si excel).

- pot mări volumul unui fișier, după care îl pot face « hidden », astfel încât nu va fi vizibil decât dacă se face o căutare mai complexă.
- Pot distruge fișiere în mod aleatoriu, neavând o țintă anume.
- Pot distruge fișierele executabile încărcate în memorie.
- Pot schimba extensiile fișierelor (ex: din .exe în .com).
- Pot face calculatorul să se restarteze sau să « înghețe » (freeze)

Cum afectează virușii calculatorul ?

Aceste simptome pot să apară și fără ca un calculator să fie virusat, dar este bine să se țină cont de ele

- pot șterge fișiere.
- pot introduce diferite mesaje în fișiere și în timpul rulării programelor.
- pot marca porțiuni de pe harddisk ca fiind defecte sau inaccesibile sau chiar bloca accesul la harddisk în întregime.
- pot bloca porturi pe care funcționează anumite componente (LPT – pentru printer) sau chiar conexiunea la internet.
- viteza de functionare a calculatorului poate scădea drastic după virusare.

Cum detectam un virus ?

- metoda recomandată pentru detectarea și îndepărtarea virușilor și programelor nocive este folosirea unui program special conceput cu aceste funcții, antivirusul.
- utilizatorii experimentați pot investiga pe cont propriu anumite aspecte și pot detecta ei înșiși dacă un calculator este sau nu virusat, dar le va fi greu de determinat și tipul de virus pe care s-ar putea să-l aibă.

Dar dacă... :

Dacă doar am downloadat un fișier pe calculator nu risc să fiu infectat

Fals : dacă doar copiați conținutul virusat al unei dischete sau dacă descărcați un fișier de pe internet, calculatorul poate fi infectat. Există viruși rezidenți în memorie care se « încarcă » singuri odată ce au ajuns într-un calculator (harddisk sau dischetă)neinfectat

Dacă nu descarc nimic de pe internet, calculatorul nu se poate infecta

Fals : chiar dacă majoritatea companiilor deținătoare de site-uri scanează conținutul pus la dispoziție utilizatorilor pentru a nu fi infectat, există posibilitatea ca unii proprietari de site-uri să nu o facă. În plus, există mulți creatori de site-uri care construiesc un site tocmai pentru a răspândi fișiere virusate, spyware, troieni și alte programe nocive.

Dacă doar citesc mailul, nu pot fi infectat

Fals : Sunt viruși care se răspândesc tocmai cu ajutorul mailului. Fișierele infectate se pot atașa mailului, aceasta fiind de altfel cea mai comună modalitate de răspândire a virușilor în acest moment.

Dacă nu intru pe internet, nu am cum să fiu infectat

Fals : virușii pot ajunge în calculator și prin intermediul unui CD infectat.

Pot lua viruși dacă doar vizitez pagini web

Fals : cu toate acestea, dacă se descarcă un fișier infectat, posibilitatea virusării există. Există însă structuri de programe care se execută doar vizitând o pagină: spyware. Aceste programe sunt concepute pentru a trimite informații private despre utilizatorul de internet infectat (violarea intimității).

Dacă formatez harddisk-ul sau șterg tot conținutul, scap de viruși?

In cele mai multe situații, da. Sunt însă viruși care se instalează pe toate partițiile harddisk-ului, pe driver-ele adiacente (floppy, de exemplu) sau în datele pentru care se face back-up, reinfestând calculatorul cu prima ocazie.

Există posibilitatea scanării calculatorului online, pentru a detecta viruși ?

Da. Dar aceasta metodă nu previne infectarea, ci doar detectează dacă un calculator este deja infectat. Pentru a preveni infectarea, este recomandat să se folosească un program special conceput și instalat pe calculator. Pentru scanarea online, este indicat ca scriptul ActiveX să fie activat, și de asemenea este recomandată folosirea browserului Internet Explorer, în cazul în care în mod obișnuit se folosește alt program pentru navigarea pe Internet.

O listă cu site-uri care permit scanarea online:

<http://us.mcafee.com/root/mfs/default.asp>
<http://security.symantec.com/>
<http://housecall.trendmicro.com/>

4. Phishing

Ce este phishingul?

Phishingul constă în trimiterea de e-mailuri care au ca și expeditor fals diverse instituții cu care potențiala victimă are anumite relații (de ex: bănci, magazine on-line etc). Aceste e-mailuri de obicei direcționează userii către anumite site-uri unde sunt rugați să-și actualizeze diverse informații sau să introducă date personale.

Aceste site-uri imită foarte bine structura celor originale însă sunt găzduite de către persoane rău intenționate care urmăresc obținerea de foloase materiale.

Ce trebuie să știm despre phishing?

La prima vedere tentativele de phishing pot trece neobservate însă sunt câteva lucruri de care ar trebui să ținem cont atunci când primim un e-mail ce pare a fi de la una din insituțiile cu care colaborăm. De regulă toate urmează aceeași structură.

Introducerea

Salutul este generic, de exemplu : “Stimate client”. De obicei companiile cu care colaborați, personalizează e-mailurile cu numele dumneavoastră.

Avertizarea

Vi se transmite faptul că în urma unor investigații au fost descoperite câteva nereguli la conturile dumneavoastră și vi se cer informațiile personale. Majoritatea companiilor nu procedează așa, este puțin probabil ca un colaborator de-al dumneavoastră să vă solicite informații confidențiale prin e-mail.

În cazul în care nu urmați instrucțiunile din e-mail într-un interval de timp destul de scurt sunteți amenințat cu dezactivarea conturilor, pierderea banilor etc.

Redirecționarea

Vi se cere să intrați imediat pe o anumită pagină web, accesând un link din cadrul emailului. Pe pagina respectivă ar trebui să introduceți informații cu caracter general ca numele dumneavoastră însă și cele cu caracter privat: coduri pin, coduri numerice personale, adrese detaliate, numere de telefon etc.

Retineți faptul că nu toate paginile care arată a fi “oficiale”, chiar sunt. Linkurile pe care ar trebui să dați click sunt mai lungi în comparație cu cele obișnuite și adesea conțin simbolul @.

Cum ne putem proteja?

Persoanele din spatele phishingului se bazează pe naivitatea utilizatorilor. Nu există o metodă de protecție 100% sigură atâta timp cât totul depinde de factorul uman. Practic orice utilizator de e-mail este o potențială victimă. Cunoscând cele câteva reguli esențiale despre comunicarea prin e-mail și luându-ne toate măsurile de precauție, ne putem feri de astfel de răufăcători.

5. Spyware

Ce se întâmplă cu PC-ul meu ?

Prima întrebare pe care ne-o adresăm când nu mai putem folosi browser-ul, când ne apar pe ecran mesaje ciudate și reclame nesolicitate, când PC-ul merge din ce în ce mai încet. Fără a ști ce este spyware-ul e greu de răspuns la asemenea întrebări.

Ce este spyware-ul ?

Spyware-ul este în general definit ca un program care profita de vulnerabilitățile unui sistem în folosul unei terțe persoane. Termenul vine de la « a spiona », adică a culege informații despre activitatea calculatorului și a le trimite unui server sau unei persoane. Spyware-ul poate face calculatorul să funcționeze greoi, îl poate face vulnerabil la infestarea cu viruși și poate culege informații confidențiale cum ar fi nume de utilizator pentru diferite aplicații, parole și informații despre cărți de credit/ conturi bancare.

Ce sunt Adware, Malware, Trackware ?

Adware este o sub-categorie a spyware-ului și este un program cu ajutorul căruia se face reclamă unor produse sau servicii. Deseori aceste reclame apar chiar și după ce programul a fost deinstalat. Aplicațiile gratuite cum ar fi Kazaa sau diferite playere media sunt însoțite la instalare și de o parte de ad-ware.

Malware reprezintă orice program care are ca funcție să producă daune la nivel software sau hardware unui calculator (ex: viruși).

Trackware sunt programele care se folosesc de unele vulnerabilitati ale browserului de web pentru a trimite unui server sau persoane informații despre siteurile accesate, informațiile căutate și obiceiurile de navigare ale utilizatorului.

Care e diferența între spyware și viruși ?

Virușii au ca scop să afecteze cât mai multe calculatoare personale, în timp ce spyware-ul are ca scop răspândirea în internet.

Virușii au de obicei o încărcătură periculoasă, vor să cauzeze daune calculatorului infectat, în timp ce spyware-ul doar încetinește procesele calculatorului, adaugă popup-uri și destabilizează browserul și are alte efecte « enervante ».

Cum aflu daca PC-ul meu are spyware ?

Cea mai eficientă metodă e scanarea lui cu un program dedicat acestui serviciu. Orice program anti-spyware are o versiune gratuită (de mediatizare) care poate fi descărcată de pe site-urile oficiale.

Folosesc un anti-spyware cunoscut dar lucrurile nu au revenit la normal, ce fac ?

În mod normal o singură scanare cu un program anti-spyware foarte bun ar trebui să fie suficientă pentru calculatorul utilizatorului obișnuit. S-ar putea să fie totuși nevoie de un al doilea program care să scaneze din nou același conținut pentru a înlătura programele spyware și adware ce n-au fost detectate cu primul program.

Programele anti-spyware conțin o listă de acțiuni tipice spyware-ului pe care acesta le poate identifica, ataca și înlătura. Odată cu evoluția programelor spyware și adware, și acțiunile pe care acestea le desfășoară se pot înmulți și diversifica. Este imposibil ca un singur program anti-spyware să recunoască toate aceste acțiuni, mai ales dacă nu este ultima versiune lansată sau dacă nu este cu update-urile la zi, de aceea în cazurile mai deosebite se recomandă folosirea de programe separate pentru scanare.

6. Securitatea in rețelele Wi-Fi

“**Wi-Fi** (pronunțat în engleză /'waɪfaɪ/) este numele comercial pentru tehnologiile construite pe baza standardelor de comunicație din familia **IEEE 802.11** utilizate pentru realizarea de rețele locale de comunicație (**LAN**) fără fir (*wireless*, **WLAN**) la viteze echivalente cu cele ale rețelilor cu fir electric de tip **Ethernet**.” (surse: Wikipedia)

Majoritatea utilizatorilor de internet folosesc conexiunea Wi-Fi , cu ajutorul unui laptop, telefon, etc. și în multe cazuri dacă aceste rețele nu sunt securizate oricine se poate conecta fără probleme (necurizat – fără parolă de acces).

Ținând cont că majoritatea hotspot-urilor nu folosesc criptare, ar trebui să fiți conștienți că traficul de internet poate fi văzut de oricine. Există echipamente de tip “pirat” cu nume clasice (SSID clasic : dlink , netgear), folosite pentru a captura informațiile de logare sau alte informații private.

Obs: Securizați-vă pc-ul, laptop-ul, etc. cu ajutorul unui firewall, opriți serviciul de file-sharing. Verificați înainte să faceți plăți bancare sau orice tip de plată, dacă sunteți la o adresă securizata: să aibă în colț stânga sus : *https* .

Routerile/acces-pointurile în general pot fi accesate pentru partea de configurare (manage-administrare echipament) intrând pe adresa “192.168.1.1” din browser, cu un utilizator și o parolă (clasică), ce pot fi verificate și aici: <http://www.routerpasswords.com/> , sau: <http://www.cirt.net/passwords> .

Obs: ar trebui să schimbați parola de acces pentru configurarea echipamentului cu una cât mai solidă, care să conțină minim 8 caractere, caractere speciale :\$#*&, cifre, litere mari și mici. Anumite echipamente Wi-Fi oferă posibilitatea administrării via wireless și cel mai bine ar fi să blocați acest feature pentru o securitate mai ridicată.

Pentru evitarea conectării altor persoane pe rețeaua dvs. Wi-Fi, ar trebui să activați criptarea : WEP (wired equivalency privacy) sau WPA & WPA2(Wi-Fi protected acces).

Cel mai bine ar fi să activați WPA sau WPA2, deoarece criptarea WEP este depășită și poate fi ușor de spart. Dacă alegeți WPA2 aveți posibilitate să alegeți o parolă cât mai complexă (cât mai greu de ghicit) pentru a limita accesul. Majoritatea echipamentelor noi au posibilitatea alegerii unei criptări : WPA + WPA2 , avantaj fiind compatibilitatea cu adaptoarele WPA.

Obs: Să alegeți o criptare WPA, WPA2 sau WPA + WPA2, o parolă de minim 10 caractere (cât mai complex și schimbarea ei la o perioadă de 3-6 luni) pentru o securitate mai ridicată.

Echipamentele Wi-Fi, de obicei au by default SSID-ul (un identificator unic) pentru a evita interferențele dintr-o rețea wireless. De multe ori când găsești dispozitive cu SSID-uri clasice : dlink, netgear20 , etc. te poți gândi că acesta nu a fost securizat pe partea de management a echipamentului.

Obs: Cel mai sigur ar fi să schimbați SSID-ul clasic cu ceva diferit (nu trebuie să aibă neaparat numele Dvs ca să vă dezvaluiți identitatea printr-un echipament wireless). De asemenea, pentru o protecție mai ridicată, este indicat să debifați opțiunea SSID broadcast, astfel existența disponibilității conexiunii WIFI în zona de acces să nu fie vizibilă.

Accesul la Wi-Fi se poate securiza și mai mult cu ajutorul setărilor din echipamentul avut.

Obs: Filtrarea după adresa MAC a echipamentului de la care doriți să aveți acces. Limitarea DHCP pentru controlul numărului de ip-uri care doriți să le permiteți accesul la rețeaua wireless.

Un alt sfat pentru o securitate mai bună a echipamentului Wi-Fi, ar fi poziționarea acestuia în casă cât mai central, cât mai departe de fereastră ca să nu poată fi accesat din exterior (semnalul să fie cât mai slab, sau inexistent).