LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

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

Pagină albă

CUPRINS

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

1. Spam

SPAM - ce reprezintă

Definiţie: 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 obţinerea de date confidenţiale.

Oricare dintre aceste tipuri de mesaje reprezintă o pierdere de timp, energie şi resurse pentru destinatari, furnizorii de servicii şi comunitatea utilizatorilor de Internet. Orice deţinator 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 poştă electronică. RCS&RDS a decis să ia măsuri atât pentru a proteja utilizatorii cât şi propria reţea. Măsurile includ instalarea de software dedicat antivirus, antispam şi toleranţă minimă faţă de aceste practici.

Are mai multe forme:

- un necunoscut vă propune să vizitaţi un site sau să faceţi o afacere, cel mai probabil ilegale
- o listă de trimitere de mesaje pe care aţi fost înscris fără ştirea dumneavoastră şi primiţi mesaje prin care sunteţi invitat să comandaţi diverse produse sau servicii

Sinonime:

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

Consecinţe:

- umplerea căsuţei cu mesaje nedorite

- pierderea de timp cu citirea mesajelor şi 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 terţi care folosesc reţeaua RCS&RDS le este interzis şi nu trebuie să permită la rândul lor să folosească reţeaua RCS&RDS pentru a trimite SPAM-uri şi 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 obţinută şi va considera abuzivă utilizarea reţelei.

Procedura de răspuns la plângeri

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

- La primirea plângerii este realizată evaluarea acesteia şi se anunţă 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 permie 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 protejati?

- Folosiţi software specializat pentru a vă securiza calculatorul.

- Marea majoritate a utilizatorilor ce abuzează de servicii nu au cunoştinţă de faptul că pe sistemul lor există un virus, robot sau troian.

- Actualizaţi sistemul de operare şi programele la ultimele versiuni disponibile; instalaţi update-urile de securitate pentru a avea un calculator neinfectat.

- Nu răspundeţi mesajelor ce vă trezesc suspiciunea; veţi arăta astfel că adresa dumneavoastră de mail este validă.

Cine practică spamul şi de ce este atât de răspândit?

Trimiterea unui mesaj la milioane de persoane este simplă şi benefică financiar pentru cei ce desfăşoara acest gen de activităţi. Chiar dacă numărul de persoane care şterg mesajul este mare, cei ce cumpară produsul fac ca această activitate să fie profitabilă.

Există mai multe metode de trimitere:

- o metodă folosită în proporţii industriale presupune deturnarea calculatoarelor utilizatorilor (folosind un virus sau alte programe maliţioase) şi 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 îşi promovează produsele)

Liste de mesaje – a nu se confunda cu spamul!

Dacă sunteţi abonat al unei companii şi aţi acceptat să primiţi informaţii legate de această companie sau produsele ei, puteţi fi destinatarul unor oferte comerciale. În acest caz nu este vorba de spam, adresa de mail fiind obţinută cu acordul dumneavoastră. Puteţi, în general, să vă dezabonaţi în orice moment şi să nu mai primiţi 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 protejeaza de mesajele de tip SPAM atât pe dvs, cât şi pe cei cărora le trimiteţi e-mail-uri. SPF este o metodă de prevenire a falsificării adresei de e-mail a expeditorului unui mesaj.

Datorită acestui tip de protectie, este posibil ca unele dintre mesajele trimise de pe adresa numeledvs@rdslink.ro prin alte servere de mail decât cele oferite clienţilor de către RCS& RDS, să fie interpretate de serverele care găzduiesc adresele la care trimiteţi e-mail-uri, drept SPAM. Unele servere şterg automat aceste SPAM-uri.
Dacă doriţi să transmiteţi e-mail-uri prin alte servere decât cele oferite de RCS& RDS fără riscul ca ele să fie interpretate drept SPAM, vă rugăm faceţi urmatoarea setare în clientul dvs. de e-mail (Outlook Expres de ex.):

- în câmpul FROM: tastaţi adresa de pe care doriţi să trimiteţi 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 siguranţa la destinaţie.

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 şi propria reţea, permiţând accesul doar la propriile servere SMTP.

De ce aţi luat această masură?

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

Ce trebuie să fac eu?

În cazul în care folosiţi pentru trimiterea mesajelor serverele RCS&RDS nu este nevoie să faceţi absolut nimic, beneficiind fără nicio întrerupere sau schimbare de configuraţie 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?

Aveţi mai multe variante pentru a face acest lucru:

- Folosiţi o sesiune criptată (SMTP peste SSL) cu serverul dumneavoastră; aceasta foloseste implicit portul 465.
- Folosiţi o sesiune VPN până la locul unde funcţionează serverul. Este varianta care va permite accesul la toate resursele organizaţiei al cărei server doriţi să îl folosiţi.
- RCS&RDS pune la dispoziţia abonaţilor un sistem prin care va fi solicitat accesul la această resursă prin intermediul unei interfeţe 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 facut un abuz?

Accesul va fi restricţionat şi veţi putea face o nouă cerere doar după ce veţi dovedi că aţi remediat problema. Aveţi acces de asemenea, şi la istoricul problemelor.

Cum procedez dacă am în continuare probleme la trimiterea mesajelor?

Vă recomandăm să contactaţi departamentul suport tehnic din oraşul dumneavoastră folosind detaliile de contact.

3. Viruşi

Ce este un virus?

Un virus este un program capabil să se reproducă în mod repetat şi să cauzeze defecţiuni fişierelor (datelor personale) şi sistemului de operare aflate pe computerul infectat. Unii viruşi acţionează imediat ce au infestat calculatorul gazdă, alţii asteaptă pasivi până când sunt rulaţi (executaţi/ porniţi) de un anumit program.

Cum ne infestăm cu viruşi ?

În trecut, viruşii 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, viruşii 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 viruşii ?

- pot fi rezidenţi sau non-rezidenţi în memorie : un virus e rezident atunci când el se încarcă în memoria calculatorului şi apoi infectează calculatorul şi e non-rezident când acţionează numai dacă un anumit fişier este deschis sau o anumită comandă este executată.
- pot acţiona chiar şi dacă un fişier infectat este doar copiat – dacă un virus este rezident în memorie, el se va încărca singur în memoria calculatorului şi va acţiona apoi asupra fişierelor la care are acces.
- pot fi polimorfi – orice virus are un cod care îl defineşte, care poate fi înţeles ca o secvenţă de program care îi spune cum să actioneze; viruşii polimorfi sunt cei care îşi pot modifica secvenţele de cod, astfel ca forma sub care circulă pe internet poate varia, pentru a se camufla mai eficient (există viruşi care circulă pe e-mail şi care pot schimba titlul mailului pentru a-l face mai « atrăgător »)
- Pot fi « deghizaţi » - mai întâi se ataşează fisierelor computerului şi abia apoi

ataca, astfel viteaza cu care se răspândesc fiind mult mai mare.
- Pot fi însoţiţi şi de alţi viruşi : dacă e cazul, un virus poate veni însoţit şi de alt program nociv, dar cu altă funcţie, atunci când infectează o gazdă (computer).
- Pot modifica sistemul de operare astfel încât să nu mai semnaleze disfuncţionalităţi.

Cum modifică viruşii fişierele ?

- viruşii pot ataca toate fişierele, dar vor ataca preponderent fişierele executabile şi de sistem (.exe, .com, .bat, .pif, .sys, .bin) şi fisierele de date (word si excel).
- pot mări volumul unui fişier, după care îl pot face « hidden », astfel încât nu va fi vizibil decât dacă se face o căutare mai complexă.
- Pot distruge fişiere în mod aleatoriu, neavând o ţintă anume.
- Pot distruge fişierele executabile încărcate în memorie.
- Pot schimba extensiile fişierelor (ex: din .exe in .com).
- Pot face calculatorul să se restarteze sau să « îngheţe » (freeze)

Cum afectează viruşii calculatorul ?

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

- pot şterge fişiere.
- pot introduce diferite mesaje în fişiere şi în timpul rulării programelor.
- pot marca porţiuni de pe harddisk ca fiind defecte sau inaccesibile sau chiar bloca accesul la harddisk în întregime.
- pot bloca porturi pe care functionează 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 şi îndepărtarea viruşilor şi programelor nocive este folosirea unui program special conceput cu aceste funcţii, antivirusul.
- utilizatorii experimentaţi pot investiga pe cont propriu anumite aspecte şi pot detecta ei însăşi dacă un calculator este sau nu virusat, dar le va fi greu de determinat şi tipul de virus pe care s-ar putea să-l aibă.

Dar dacă... :

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

Fals : dacă doar copiaţi conţinutul virusat al unei dischete sau dacă descărcaţi un fişier de pe internet, calculatorul poate fi infectat. Există viruşi rezidenţi în memorie care se «

încarcă » singuri odată ce au ajuns într-un calculator (harddisk sau dischetă)neinfestat

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

Fals : chiar dacă majoritatea companiilor deţinatoare de site-uri scanează conţinutul pus la dispoziţie utilizatorilor pentru a nu fi infectat, există posibilitatea ca unii proprietari de site-uri să nu o facă. În plus, există mulţi creatori de site-uri care construiesc un site tocmai pentru a răspândi fişiere virusate, spyware, troieni şi alte programe nocive.

Dacă doar citesc mailul, nu pot fi infectat

Fals : Sunt viruşi care se răspândesc tocmai cu ajutorul mailului. Fişierele infectate se pot ataşa mailului, aceasta fiind de altfel cea mai comună modalitate de răspândire a viruşilor în acest moment.

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

Fals : viruşii pot ajunge în calculator şi prin intermediul unui CD infectat.

Pot lua viruşi dacă doar vizitez pagini web

Fals : cu toate acestea, dacă se descarcă un fişier infestat, posibilitatea virusării există. Există însă structuri de programe care se executa doar vizitând o pagină : spyware. Aceste programe sunt concepute pentru a trimite informaţii private despre utilizatorul de internet infestat (violarea intimităţii).

Dacă formatez harddisk-ul sau şterg tot conţinutul, scap de virusi?

In cele mai multe situatii, da. Sunt însă viruşi care se instalează pe toate partiţiile 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 viruşi ?

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 şi instalat pe calculator. Pentru scanarea online, este indicat ca scriptul ActiveX să fie activat, şi de asemenea este recomandată folosirea browser-ului Internet Explorer, în cazul în care în mod obişnuit se foloşeste 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/sscv6/default.asp?productid=symhome&langid=ie&venid=sym
http://housecall.trendmicro.com/

4. Phishing

Ce este phishingul?

Phisingul constă în trimiterea de e-mailuri care au ca şi expeditor fals diverse instituţii cu care potenţiala victimă are anumite relaţii (de ex: bănci, magazine on-line etc). Aceste e-mailuri de obicei direcţionează userii către anumite site-uri unde sunt rugaţi să-şi actualizeze diverse informaţii sau să introducă date personale.

Aceste site-uri imită foarte bine structura celor originale însă sunt găzduite de către persoane rău intenţionate care urmăresc obţinerea de foloase material.

Ce trebuie să ştim despre phishing?

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

Introducerea

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

Avertizarea

Vi se transmite faptul că în urma unor investigaţii au fost descoperite câteva nereguli la conturile domneavoastră şi vi se cer informaţiile personale. Majoritatea companiilor nu procedeaza aşa, este puţin probabil ca un colaborator de-al dumneavoastră să vă solicite informaţii confidenţiale prin e-mail.

În cazul în care nu urmaţi instrucţiunile din e-mail într-un interval de timp destul de scurt sunteţi ameninţat cu dezactivarea conturilor, pierderea banilor etc.

Redirecţionarea

Vi se cere să intraţi imediat pe o anumită pagină web, accesând un link din cadrul e-mailului. Pe pagina respectivă ar trebui să introduceţi informaţii cu caracter general ca numele dumneavoastră însă şi cele cu caracter privat: coduri pin, coduri numerice personale, adrese detaliate, numere de telefon etc.

Retineţi faptul că nu toate paginile care arată a fi “oficiale”, chiar sunt. Linkurile pe care ar trebui să daţi click sunt mai lungi în comparaţie cu cele obişnuite şi adesea conţin

simbolul @.

Cum ne putem proteja?

Persoanele din spatele phisingului se bazează pe naivitatea utilizatorilor. Nu există o metodă de protecţie 100% sigură atâta timp cât totul depinde de factorul uman. Practic orice utilizator de e-mail este o potenţiala victimă. Cunoscând cele câteva reguli esenţiale despre comunicarea prin e-mail şi luându-ne toate măsurile de precauţie, 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 şi reclame nesolicitate, când PC-ul merge din ce în ce mai încet. Fără a ştii 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 vulnerabilităţile unui sistem în folosul unei terţe persoane. Termenul vine de la « a spiona », adică a culege informaţii despre activitatea calculatorului şi a le trimite unui server sau unei persoane. Spyware-ul poate face calculatorul să funcţioneze greoi, îl poate face vulnerabil la infestarea cu viruşi şi poate culege informaţii confidenţiale cum ar fi nume de utilizator pentru diferite aplicaţii, parole şi informaţii despre cărţi de credit/ conturi bancare.

Ce sunt Adware, Malware, Trackware ?

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

Malware reprezintă orice program care are ca funcţie să producă daune la nivel sofware sau hardware unui calculator (ex: viruşii).

Trackware sunt programele care se folosesc de unele vulnerabilitati ale browserului de web pentru a trimite unui server sau persoane informaţii despre site-urile accesate, informaţiile căutate şi obiceiurile de navigare ale utilizatorului.

Care e diferenţa între spyware şi viruşi ?

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

Viruşii au de obicei o încărcătură periculoasă, vor să cauzeze daune calculatorului infectat, în timp ce spyware-ul doar încetineşte procesele calculatorului, adaugă pop-up-uri şi destabilizează browserul şi 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 obişnuit. S-ar putea să fie totuşi nevoie de un al doilea program care să scaneze din nou acelaşi conţinut pentru a înlătura programele spyware şi adware ce n-au fost detectate cu primul program.

Programele anti-spyware conţin o listă de acţiuni tipice spyware-ului pe care acesta le poate identifica, ataca şi înlătura. Odată cu evoluţia programelor spyware şi adware, şi acţiunile pe care acestea le desfăşoară se pot înmulţi şi diversifica. Este imposibil ca un singur program anti-spyware să recunoască toate aceste acţiuni, 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 reţelele Wi-Fi

"**Wi-Fi** (pronunţat în engleză/'waıfaı/) este numele comercial pentru tehnologiile construite pe baza standardelor de comunicaţie din familia **IEEE 802.11** utilizate pentru realizarea de reţele locale de comunicaţie (LAN) fără fir (*wireless*,WLAN) la viteze echivalente cu cele ale reţelelor cu fir electric de tip Ethernet." (surse: Wikipedia)

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

Ţinând cont că majoritatea hotspot-urilor nu folosesc criptare, ar trebui să fiţi conştienţi 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 informaţiile de logare sau alte informaţii private.

Obs: Securizaţi-vă pc-ul, laptop-ul, etc. cu ajutorul unui firewall, opriţi serviciul de file-sharing. Verificaţi înainte să faceţi plăţi bancare sau orice tip de plată, dacă sunteţi la o adresă securizata: să aibă în colţ stânga sus : *https* .

Routerele/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 şi o parolă (clasică), ce pot fi verificate şi aici: http://www.routerpasswords.com/ , sau: http://www.cirt.net/passwords .

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

Pentru evitarea conectării altor persoane pe reţeaua dvs. Wi-Fi, ar trebui să activaţi criptarea : WEP (wired equivalency privacy) sau WPA & WPA2(Wi-Fi protected acces). Cel mai bine ar fi să activati WPA sau WPA2, deoarece criptarea WEP este depaşită şi poate fi uşor de spart. Dacă alegeţi WPA2 aveţi posibilitate să alegeţi 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 alegeţi o criptare WPA, WPA2 sau WPA + WPA2, o parolă de minim 10 caractere (cât mai complex şi 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 interferenţele dintr-o reţea wireless. De multe ori când găseşti dispozitive cu SSID-uri clasice : dlink, netgear20 , etc. te poţi gândi că acesta nu a fost securizat pe partea de management a echipamentului.

Obs: Cel mai sigur ar fi să schimbaţi SSID-ul clasic cu ceva diferit (nu trebuie să aibă neaparat numele Dvs ca să vă dezvaluiţi identitatea printr-un echipament wireless). De asemenea, pentru o protecţie mai ridicată, este indicat să debifaţi opţiunea SSID broadcast, astfel existenţa disponibilităţii conexiunii WIFI în zona de accces să nu fie vizibilă.

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

Obs: Filtrarea dupa adresa MAC a echipamentului de la care doriţi să aveţi acces. Limitarea DHCP pentru controlul numărului de ip-uri care doriţi să le permiteţi accesul la reţeaua wireless.

Un alt sfat pentru o securitate mai bună a echipamentului Wi-Fi, ar fi poziţionarea 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).