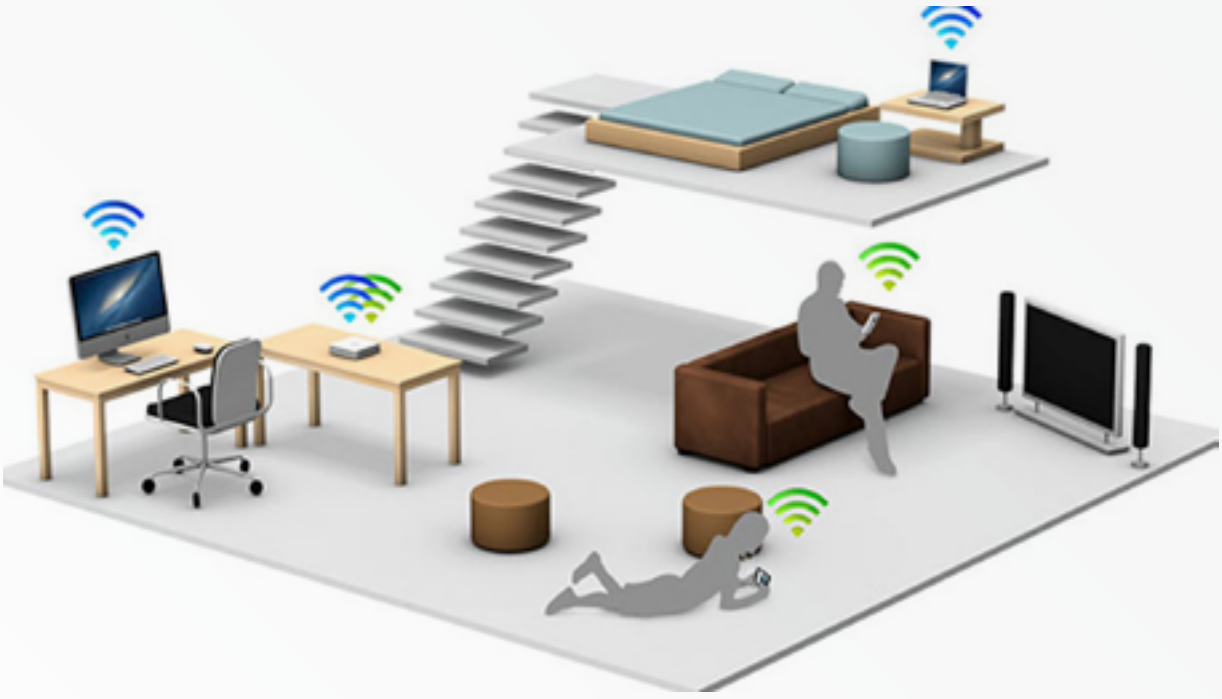
KAKO DA ZAŠTITITE SVOJU WI-FI MREŽU?
10 saveta profesionalnih mrežnih administratora

Bežične (Wi-Fi) mreže se koriste više nego ikad i nalaze se svuda oko nas. Ipak, iako je relativno lako pristupiti im i koristiti ih, Wi-Fi mreže nisu uvek i BEZBEDNE mreže.

Opasnost leži u tome što, ukoliko ne preduzmete par sigurnosnih koraka, vašoj Wi-Fi mreži mogu pristupiti drugi ljudi. A oni nekada to čine sa vrlo lošim namerama.

U manje opasnoj situaciji, na vašu mrežu bi mogao da se konektuje komšija, koji bi vam usporio internet jednostavnim korišćenjem vašeg protoka. Ali nije uvek to u pitanju; na vašu mrežu može baciti oko i online kriminalac koji želi da „prisluškuje" vaš saobraćaj ne bi li pribavio osetljive informacije, ili iskoristio vašu mrežu za vršenje zlonamernih napada.



Zbog toga je veoma važno da naučite kako da zaštitite svoju kućnu bežičnu mrežu od zlonamernih napada. A odakle drugde početi nego od maksimiziranja bezbednosti sopstvene kućne mreže?

Zato smo vam pripremili ovaj vodič sa 10 saveta profesionalnih mrežnih administratora koji se bave bezbednošću velikih korporativnih mrežnih sistema. Sigurno će vam biti od koristi.

1 PROMENITE IME VAŠE KUĆNE WI-FI MREŽE

Odmah po postavljanju vaše kućne bežične mreže, trebalo bi da promenite SSID (Service Set Identifier). Ovo je ime vaše kućne mreže, ime koje će drugi uređaji videti kada budu pokušavali da se povežu na internet koristeći bežičnu mrežu iz vašeg doma.

Nije teško pogoditi razlog zašto bi trebalo da promenite ovo ime. Promena imena otežava stvar hakeru koji želi da pristupi vašoj mreži. Obično, proizvođači rutera dodele ime kompanije koja proizvodi ruter; to može biti nešto kao na primer: Linksys, Cisco ili Belkin.

U slučaju da SSID nije modifikovan, haker ima veće šanse da pristupi mreži, jednostavno zato što zna proizvođača rutera.

I još jedna stvar u vezi sa ovim korakom – ne koristite svoje ime niti prezime, kako biste izbegli da vas identifikuju kao vlasnika mreže. Ovo je još jedan detalj koji bi mogao da olakša posao potencijalnom hakeru, ili online kriminalcu koji bi mogao da pokuša postupak krađe identiteta.

2 IZABERITE JAKU I JEDINSTVENU LOZINKU ZA VAŠ BEŽIČNI INTERNET

Vaš bežični ruter već ima postavljenu šifru. Problem je u tome što je hakerima lako da provale ovu šifru, pogotovo ako znaju ime proizvođača rutera. (Pogledajte prvi korak iznad.) Kada postavljate dobru lozinku za svoj bežični internet, vodite računa da sadrži bar 20 karaktera i da uključuje brojeve, slova, kao i razne simbole.

Ovo podešavanje će sprečiti druge ljude da pristupe vašoj mreži. Iako uglavnom nije u pitanju ništa ozbiljnije od situacije da vam neki komšija „krade" brzinu, možda ćete se susresti sa drugim situacijama, kao što su online kriminalci koji pristupaju vašoj mreži kako bi „slušali" vaš saobraćaj podataka i pribavili osetljive informacije (kao što su podaci vašeg računa u banci, šifre za mejl nalog i profile na društvenim mrežama, listu svih sajtova koje ste posećivali...).

3 POVEĆAJTE BEZBEDNOST TIME ŠTO ĆETE AKTIVIRATI ENKRIPCIJU MREŽE

Postoji nekoliko popularnih opcija za enkripciju bežičnih mreža, kao što su WEP, WPA i WPA2. Ovaj poslednji vid enkripcije – WPA2 – jeste opcija koja se preporučuje zbog veće bezbednosti, pogotovo ako imate kućnu mrežu.

Opcija enkripcije saobraćaja je korisna ako vam je potrebno da učinite svoje komunikacione signale neupotrebljivim za svaki neovlašćeni tuđi softver.

U ovom trenutku, svi bežični uređaji koji su u opticaju podržavaju ovu tehnologiju i opšte je poznato da je poželjno koristi WPA2, koji ima veći stepen bezbednosti.

4 DEAKTIVIRAJTE BEŽIČNU MREŽU KADA NISTE KOD KUĆE

Mnogi je zanemaruju, ali ova opcija je veoma korisna, pogotovo kada napuštate dom na duže vreme, recimo ako idete na odmor ili jednostavno nećete biti kod kuće par dana.

Ova bezbednosna mera, pored toga što vam pomaže da smanjite utrošak energije, sigurno će sprečiti hakere da vam „slušaju" mrežni saobraćaj ili mu pristupe iz zlonamernih razloga.

5 PRONAĐITE BEZBEDNU POZICIJU ZA RUTER

Bilo bi dobro da stavite vaš bežični ruter što bliže sredini doma. Ne samo zato da bi svako mesto i svaka prostorija imali isti pristup internetu već i zato što ne želite da vaš bežični signal dopire previše van doma, gde hakeri lako mogu da ga uhvate.

Zbog ovoga, nemojte ga stavljati previše blizu prozora, gde bi se signalu lako moglo pristupiti spolja, čak i sa izvesne udaljenosti, a tu je i naše četvrto pravilo kojeg se takođe možete pridržavati – da deaktivirate ruter kada napuštate dom.

6 IZABERITE JAKU LOZINKU ZA ADMINISTRATORA MREŽE

Da biste podesili bežični ruter, obično vam je potreban pristup admin stranici, gde možete promeniti podešavanja svoje mreže.

Kao što je dobro poznato, normalno je da nađete ruter sa default postavkama kao što su „admin" i „password". A hakerima nije naročito teško da provale ove podatke.

Kad nešto menjamo na admin stranici, obično se radi o stvarima poput postavljanja jake lozinke za bežičnu mrežu i promene imena mreže, a obe promene se prave da bi se osigurao veći stepen zaštite od zlonamernih radnji online kriminalaca.

Međutim, ako IT kriminalac može da pristupi administratorskoj platformi, i pristupi opcijama za postavljanje i konfiguraciju vaše mreže, to je definitivno nešto što vam može pokvariti dan.

7 ISKLJUČITE PRISTUP NA DALJINU

Uobičajeno je da možete pristupiti interfejsu vašeg rutera sa uređaja povezanog na vašu mrežu, ali neki ruteri omogućavaju pristup čak i sa udaljenih sistema. U smislu sprečavanja da online hakeri pristupe podešavanjima vašeg rutera, isključivanje ove opcije u podešavanjima vašeg rutera je dobra bezbednosna ideja.

Da napravite ovu izmenu, pristupite admin panelu i potražite „Remote access" ili „Remote administration".

8 AŽURIRAJTE SOFTVER RUTERA

Posmatrajte softver svog rutera kao bilo koji drugi softver koji imate na svom računaru. Recimo, vaš antivirus program, ili uostalom bilo koja druga aplikacija u sistemu. Ruterov firmware, kao i svaki drugi softver, ima nedostatke koji mogu postati velike slabosti ukoliko se brzo ne poprave kroz apdejte koje objavljuje proizvođač.

Problem je u tome što većina rutera nema opciju automatskog instaliranja poslednjih bezbednosnih verzija i potrebno je da s vremena na vreme proverite zvanični sajt radi bezbednosnog ažuriranja.

Ne treba zaboraviti da je do nekih od najgorih zabeleženih napada došlo zahvaljujući nezakrpljenim bezbednosnim rupama u programima i operativnim sistemima.

9 POSTARAJTE SE DA IMATE DOBAR FIREWALL

Neki ruteri imaju sopstveni firewall koji pomaže u sprečavanju hakera da pristupe vašem računaru.

U slučaju da vaš ruter ne poseduje takav firewall, postarajte se da instalirate dobar firewall u svoj sistem, kako bi pazio na zlonamerne pokušaje pristupa vašoj bežičnoj mreži.

U današnje vreme, većina ljudi koristi firewall rešenje koje nudi njihov operativni sistem, što je dobra opcija. U slučaju da koristite bezbednosni softver koji sadrži firewall, dobra opcija je uključiti ga.

10 ZAŠTITITE UREĐAJE KOJI SE NAJČEŠĆE POVEZUJU NA VAŠU BEŽIČNU MREŽU

Zatvorite sva vrata online kriminalcima!

Iako ste možda osigurali ruter i bežičnu mrežu, treba da obratite pažnju da niste napravili neki bezbednosni propust koji IT kriminalci mogu iskoristiti. Stoga, pratite neke opšte i uobičajene smernice kako biste se držali dalje od online opasnosti, na primer, imajte instaliran najnoviji softver i najnovije sigurnosne dodatke, kako nijedna bezbednosna rupa ili propust ne bi bili izloženi online predatorima.

Takođe, što je još važnije, proverite koji se uređaji najviše povezuju na vašu kućnu mrežu i vodite računa da imaju instaliran sigurnosni softver protiv virusa i spywarea.

I na kraju, koristite specijalizovan sigurnosni softver da biste zaštitili svoje uređaje od zlоćudnog softvera za krađu novca i podataka, cyber kriminalaca i zlоćudnih hakerskih servera.

ŽELITE STABILAN POSAO?
Administrator mreža je pouzdan izbor

Školovanjem na odseku Administration na ITAcademy, bićete spremni za rad na celokupnom procesu planiranja, projektovanja, konfigurisanja, implementacije, održavanja i zaštite kompletne mrežne infrastrukture pod operativnim sistemima Microsoft Windows Server ili Linux.

Po završetku ovog programa moći ćete da radite u savremenom poslovnom svetu u širokom spektru poslova, od početnog nivoa administratora do vrhunskog sistemskog i mrežnog projektanta, a vašu stručnost potvrdiće i međunarodni sertifikati svetski poznatih kompanija i organizacija sa kojima ITAcademy sarađuje: Microsoft, CompTIA, Cisco, MikroTik i Linux Professional Institute.

Da saznate sve o školovanju na ITAcademy i načinima da se usavršite za jedno od najpopularnijih zanimanja današnjice idite na www.it-akademija.com.

ITAcademy™

Za profitabilnu IT karijeru:
Po zvaničnom ovlašćenju ispitnog odeljenja Kembridž Univerziteta i tri vodeće IT kompanije, jednogodišnje stručno IT školovanje naprednog programa za računarske i dizajn tehnologije

CAMBRIDGE International Examinations
Cambridge International School

ITAcademy je ovlašćena od ispitnog odeljenja Kembridž Univerziteta

Microsoft Partner
Silver Learning

ITAcademy obezbeđuje zvanična stručna zvanja Microsoft korporacije

MikroTik

ITAcademy je akreditovani MikroTik trening centar za obuku mrežnih administratora.

ITAcademy • Cara Dušana 34, 11080 Zemun, Beograd • +381 (0)11 7856 100 (GMT + 01:00) • www.it-akademija.com

Copyright © ITAcademy