

Koliko Vam je računalo sigurno?

Danas u doba Interneta i globalne povezanosti, računala postaju sve ranjivija na razne opasnosti, koji ih vrebaju na svakom koraku. Stalno se smisljavaju novi načini za uništavanje ili krađu podataka. Mašta hakera i Internet kriminalaca je sve veća, a apetiti organiziranog krimanala sve više ulaze i u ovu domenu života. Nažalost ili na sreću bez Interneta više ne možemo. Kako se obraniti od virusa i drugih Intenet prijetnji, koji se množe eksponentijalnom brzinom?

Često kupovinom brand računala dobijemo predinstaliran neki zaštitni program. To znači da ga besplatno možete koristiti 1-3 mjeseca, a onda ga morate kupiti ili je beskoristan. Takvi programi Vas svakih malo, podsjećaju na to. Kako je kod nas uvriježeno mišljenje, da je trošak za legalni software glupost, često se ostane bez ikakve zaštite ili se stavi neka besplatna. A kada je nešto besplatno onda to i nije ono pravo. Takve verzije u pravilu nude osnovnu zaštitu, te jednostavno brišu zaražene i oštećene datoteke, čime računalo postaje sve sporije, duže je vrijeme podizanja i shut downa, često smrzava, pa na kraju mu je potrebna reinstalacija Windowsa. Ako nemate bolje rješenje skinite makar jednu takvu besplatnu verziju AVG 8.5 sa www.avg.com stranice.

Većina programa radi na sličan način. Provjerava pristiglu e-mail poštu ili datoteku prilikom otvaranja, spremanja ili kopiranja. Slično se dešava i kod surfanja Internetom. Gotovo svaka stranica Vam smješta na Vaš hard disk nekog špijuna ili kolačić, pokušavajajući Vama olakšati ponovno učitavanje te stranice, ali i kontrolirati što radite. Postoje razni nivoi zaštite, ovisno čemu služi računalo. Visok nivo zaštite se očekuje za poslovna računala, dok ona namijenjena klincima će skupiti svega i svačega svakako veoma brzo. Visok nivo zaštite na takvim računalima neće dozvoliti mnoge radnje, koje su neophodne za pokretanje nekog programa, igrice i slično. Zaštitni program će svako malo tražiti dopuštenje za pokretanje neke datoteke. Kako većina nas nema pojma, da li je to baš ta datoteka ili neke parazitna, olako će se dati dozvola za pokretanje i na taj način opet zaobići zaštitni program.

SPAM

Spam ili neželjena pošta je drugi problem i postaje sve veći i veći. Internet je postao veoma jeftino sredstvo za promidžbu mnogih proizvoda. Po nekim ispitivanjima preko 90% svega prometa na Interentu je spam. Često ga generiramo i sami, proslijedujući kojekave poruke. Zar zaista mislite da ćete dobiti Nokia mobitel, kada mail koji ste dobili trebate poslati samo na 9 e-mail adresa u cilju Nokia kampanje? Zar ćete zaista pomoći djetetu koje umire od raka i osigurati donaciju neke kompanije, proslijedujući e-mail na 7 adresa. Glupost nad glupost. Slanje toliko mailova u kratkom vremenu samo će zagušti promet na Internetu. Pokretanje takvih mailova je čak kažnjivo u nekim zemljama. Jedinu korist od svega toga vidjeti će možda netko tko na takav način može prikupiti tisuća e-mail adresa za novo spam bombardiranje marketinškim materijalima. Ne dajte svoj pristanak i e-mail adresu da Vam se na nju šalju propagandne poruke, osim stvarno tamo onoga što želite. Spam mailovi su najčešći uzrok virusnih infekcija.

Ako su Vam dosadili mailovi gdje Vam se nudi viagra ili diploma na sveučilištu u Americi ili nešto slično možete nešto poduzeti. U borbi protiv spama prvi korak je Vaš Intenet provider. Naprimjer često dobijete poruku od T-COM-a da je e-mail upućen se određene e-mail adrese možda spam ili virus. Ako mislite da nije, možete to provjeriti. Provjerom u pravilu ustanovite da se radi o spamu. Vjerojatno je svaki takav mail spam. Pa zašto ga šalju onda? Boje se da će na taj način proglašiti spicom zaista neke mailove, koje želite primati. Na korisničkim stranicama T-COM-a možete definirati nivo zaštite za e-mail adrese tipa marko.markovic@ri.t-com.hr , pa ne dobivati niti takve mailove upozorenja da je spam. Stoga posjetite www.tportal.hr i kliknite na **korisni čke stranice**, te unesite svoje **korisničko ime i lozinku** za pristup Intenetu. U glavnom izborniku kliknite na **Sigurnosna zaštita**, te izaberite **napredna zaštita** umjesto preporučena i kliknite na gumb **Postavi razinu e-mail zaštite**. Više gotovo da nećete dobivati spam poruke niti poruke sa virusima.

Za Iskon korisnike i e-mail adrese marko.markovic@inet.hr na stranici www.iskon.hr/korisnicki_centar , nakon unosa **korisničkog imena i lozinke**, kliknite na **Antivirus/Antispam zaštita** i izaberite **Spam cleaner**. Te kliknite na gumb **Prihvati**.

Ovo se može podesiti i kod drugih Intenet davatelja usluga, a također i na mail serverima davatelja usluga hostinga za e-mail adrese tipa marko@naprimjer.hr.

Nažalost mnoge naše firme šalju propagandne materijale, koje T-COM, Iskon ili neki drugi Intenet provajder neće tretirati kao spam. Tada ostaje druga opcija. Antispam software, gdje ćete Vi sami definirati e-mail adresu, sa koje stiže takav materijal, kao spam. Čak i u Outlooku postoji opcija Junk mail,

ali to je sve tada već skinuto i nalazi se u folderu outlooka.

Riječnik pojmova

Često se na Intrenetu i u radu sa računalom srećemo sa raznim engleskim pojmovima, koji nam mnoga ne znače. Evo male pomoći oko njihovog boljeg razumjevanja, u cilju bolje zaštite.

Authentication je proces gdje računalo provjerava identitet korisnika ili drugog računala koje se spaja na Vaše računalo. Može odbiti spajanje ili prijem e-maila ako se to drugo računalo ne predstavi svojim podacima kako treba.

Dialler je program koji Vas preusmjerava sa Intrenet dial-up veze, koju obično koristite, na vezu preko nekih telefonskih brojeva u banana zemljama. Time Vaši računi za telefon i Interenet postaju veoma visoki. Pomaže ugradnja anti-dialer programa i pravilnog konfiguriranja outlooka. Kod ADSL-a nema ovaj problem.

Digital certificate je digitalni dokument-potvrda. U cilju vjerodostojnosti izdaje se od treće strane (Certificate Authority, ili CA), kako bi garantirao da se radi o traženom identitetu. Pristup na neke web stranice (npr. banaka) nije moguć bez prethodno instaliranih digitalnih cerifikata na računalu. **SSL certifikat** se često viđa na webshop stranicama. To je garancija slobodnog plaćanja na toj stranici kreditnim karticama, jer niti trgovac tu ne vidi broj kartice. Cijela transakcija se obavlja direktno preko kartičarske kuće.

Digital signature je ekvivalent potpisu na papiru, čime se svjedoči o vjerodostojnosti dokumenta.

Encryption i Decryption je način zaštite podataka kod presretanja i otuđenja. Takvi podaci su obično neupotrebljivi onome što ih se domogne.

Evil twin je lažna kopija javne Intrenet mreže ili WI-FI hot spot točke u nekom kafiću, restoranu ili slično. Spajajući se na nju ostajete bez brojeva kreditnih kartica, bankovnih računa i slično.

Firewall ili vatrogasd štiti računalo od napada hackare izvana. Kontrolira pristup korisnika i raznih programa računalu ili mreži.

Hacker je informatički veoma obrazovana i upućena osoba, koja iz raznih razloga upada u sustave, krađe ili uništava informacije.

Internet hosting je davatelj usluga smještaja web stranica, e-mail servera raznih korisnika.

Internet server je program na Intrenet hostingu.

Internet Service Provider (ISP) je davatelj usluga Interneta (T-COM, Iskon,...)

Keylogger je uređaj ili program, koji registrira svaki klik na tipkovnici. Cilj je krađa passworda (lozinke) ili brojeva kreditnih kartica.

Malware je opće ime za program napravljen za neovlaštene aktivnosti na vašem računalu, u cilju nanošenja štete.

Pharming je radnja koja Vas preusmjerava sa stranice koju želite posjetiti na lažno napravljenu web stranicu. Ona po izgledu podsjeća na onu željenu, a tada se krađu osobne informacije, pristup bankovnim računima, kreditnim karticama.

Phishing je način krađe osobnih podataka i podataka o računima i kreditnim karticama. Obično se dobije e-mail u kojem se traži potvrda i dopuna podataka. Korisnik misli da ga je uputila njegova banka, a ustvari je žrtva prevare. Spear phishing je napad na određenu tvrtku ili organizaciju.

Rootkit je program koji omogućava pristup **Trojan horse** programima, koji preuzimaju kontrolu na računalu. To su programi dizajnirani po legendi na trojanskog konja. Instalira ih korisnik sam misleći da instalira nešto korisno što mu treba. Nakon instaliranja oni onda pokazuju svoju pravu namjeru.

Sniffing je osluškivanje u komunikaciji na mreži ili Intrenetu u cilju prikupljanja povjerljivih podataka. Posebno su riskantne bežične mreže.

Spyware dolazi na računalo putem virusa, downloada ili nekog softwarea. Cilj mu je skupljanje informacija i njihovo prosljeđivanje drugome. Mogu tako i usporiti rad računala.

Za zaštitu i čišćenje od svega ovoga postoje mnogi programi i paketi programa. Čak i pored kupljene licence ne znači da ne možete imati problema. Nitko ne tvrdi da je zaštita 100%. Čišćenje nije lako i obično zahtijeva skeniranje sa više raznih programa. Čak i iskusni informatičari nekada imaju problema da očiste računalo. Nekada su i važni podaci izgubljeni. Najbolja zaštita je backup. Kod nekih računala samo pomaže formatiranje diska i ponovna instalacija Windowsa.