DEO 1: INTERNET

POGLAVLJE 1: INTERNET

1.1. Koncepti i pojmovi

1.1.1 Šta je Internet?

Svi oko vas pričaju o Internetu, ali bi veoma mali broj ljudi mogao da vam kaže šta je zaista Internet. Jedan od razloga za to sasvim je jednostavan – veoma je teško precizno definisati nešto tako promenljivo kao što je Internet.

Internet je mreža koja povezuje računarske mreže širom sveta. To je globalna računarska mreža. Male mreže se međusobno povezuju i čine ovu strukturu. Internet se sve češće naziva globalnom mrežom informacija (velika internacionalna globalna baza podataka). Količina informacija na umreženim serverima je ogromna, i teško je realno proceniti i prikazati kolika je ona zaista.

Internet, kao globalni sistem međusobno povezanih računarskih mreža, koristi standardni protokol, tj. skup pravila koja svi mrežni uređaji prate kada šalju ili primaju podatke. Svaki računar koji je povezan na Internet koristi protokol **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

Internet je revolucionarno promenio način na koji ljudi pristupaju informacijama za poslovne ili privatne svrhe, način na koji pojedinci kupuju proizvode i usluge, te način na koji ljudi komuniciraju s prijateljima, kolegama i drugima.

Internet je nova komunikaciona tehnologija, koja utiče na naš život isto kao telefon (naročito mobilni) i televizija. Neki čak veruju da je u oblasti širenja informacija Internet najznačajniji pronalazak posle Gutenbergove štamparske mašine. Ako koristite telefon, pišete pisma, čitate novine i časopise, bavite se nekim poslom ili obavljate bilo kakvo istraživanje, Internet može radikalno izmeniti vaš pogled na svet. Mnogi kažu: „Ono čega nema na Internetu, to i ne postoji“.

Dakle, Internet koriste poslovni ljudi, učenici, studenti, penzioneri, domaćice – jednom rečju, ljudi svih zanimanja i životnih doba smatraju da upotreba Interneta unapređuje njihov život i rad. Na primer, predavači na univerzitetima koriste Internet za pronalaženje stručnih članaka i podataka za svoja predavanja i istraživanja. Procene iz 2009. godine govore da četvrtina zemaljske populacije koristi usluge Interneta.

Internet kao svetska mreža nema nikakvih prepreka. Dostupna je na svakom mestu, naravno, uz odgovarajuću opremu. Da biste pristupili ovoj mreži, pored računara morate imati jedan od sistema za komunikaciju kao što su: telefonska linija, ISDN, ADSL, kablovska Internet veza, bežični Internet itd.

Pored toga, morate da imate davaoca Internet usluga (**Internet Service Provider, ISP**) o čemu će biti reči u odeljku 1.1.3, i program za pregled Web stranica, tj. čitač Weba (**Web Browser**) o čemu će biti reči u odeljku 1.1.5.

1.1.2 Šta je World Wide Web?

Izrazi *Internet* i *World Wide Web* (WWW ili W3), koji se obično naziva samo Web, često se koriste u svakodnevnom govoru kao sinonimi. Međutim, Internet i Web nisu isto.

Kao što je objašnjeno u prethodnom odeljku, Internet je hardverska i softverska infrastruktura preko koje su računari povezani, tj. on je globalna mreža računarskih mreža nastala 1969. godine.

S druge strane, Web je rođen 1989. i jedna je od usluga za komunikaciju preko Interneta – predstavlja sistem međusobno povezanih Web strana kojima možete pristupiti preko Interneta. Proteklih godina, Web je (uz elektronsku poštu) postao najčešće korišćeni deo Interneta, a danas je to još i više.

Na Internetu ima još mnogo toga što nije Web, kao što su sistemi za razmenu trenutnih poruka, višekorisničke igrice i klasična elektronska pošta.

Web sadrži veliku kolekciju dokumenata (stranica) koje su na raspolaganju u određenom formatu. U tim dokumentima, tekst je kombinovan sa slikama, zvukom ili čak animacijom i filmom. Ti dokumenti, koji se nazivaju Web strane, nalaze se na Web lokacijama širom sveta.

Da zaključimo: World Wide Web je niz dokumenata objavljenih na Webu u formatu koji omogućava njihovo prikazivanje pomoću čitača Weba. Taj format se zove **html**, po jeziku za označavanje hiperteksta (**HyperText Markup Language, HTML**). HTML je prilično jednostavan jezik, koji ima jednu važnu prednost nad drugim programskim jezicima – nije mu potreban određen računar da bi se izvršavao. To znači da možete pregledati HTML stranice na bilo kom računaru na koji je instaliran čitač Weba.

Softver koji prikazuje World Wide Web dokumente (*Web stranice*) zove se *čitač Weba* ili Web čitač (**Browser**) ili program za pregledanje Web stranica. Najpopularniji čitači su: Windows Internet Explorer (o kome će biti više reči u odeljku 1.1.5), Mozilla Firefox, Google Chrome, Safari i Opera.

1.1.3 Definisanje i razumevanje pojmova: davalac Internet usluga, jedinstvena adresa resursa, hiperveza

1.1.3.1 Davalac Internet usluga

Da biste koristili Internet, morate se povezati s njim. To obično znači da treba da koristite kapacitete nekog od davalaca Internet usluga. *Davalac Internet usluga* (**Internet Servis Provider, ISP**) jeste kompanija koja svojim korisnicima pruža uslugu priključivanja na Internet i odgovarajuće servise. U kolokvijalnom govoru upotrebljava se i izraz *provajder.*

Pristup Internetu može biti: modemski, kablovski, ADSL itd. Osim pristupa Internetu, davaoci Internet usluga najčešće nude još i usluge slanja i primanja elektronske pošte, prostor na svojim serverima za postavljanje Web prezentacija, registraciju domena i drugo.

Veliki broj davalaca Internet usluga (u Srbiji su 164 firme registrovane da se bave ovim poslom)[1] nudi širok spektar usluga. Pojedinac ili firma moraju uzeti u obzir nekoliko parametara kada biraju davaoca Internet usluga, uključujući:

- Brzinu i propusni opseg veze.
- Vrstu veze i cenu usluge.
- Dostupnost korisničke službe i tehničke podrške.

Brzina Internet veze zavisi od propusnog opsega, tj. kapaciteta komunikacionih kanala.

Propusni opseg Internet veze definiše količinu podataka koji se mogu preneti u određenoim vremenskom periodu i meri se u bitovima u sekundi (**bits per second, bps**). Početkom 2010. godine, na primer, u našoj zemlji su to sledeće brzine:

- od 32 do 112 kbps, pri povezivanju preko telefonske linije, i
- od 256 kbps do 16 Mbps pri povezivanju preko ADSL-a.

Kao što je već rečeno, brzina prenosa je samo jedan od faktora koje morate uzeti u obzir kada birate davaoca Internet usluga. Morate obratiti pažnju na to kako ćete fizički povezati svoj računar na Internet – da li preko telefonske, ADSL, kablovske ili bežične veze. Svaki od ovih načina povezivanja sa Internetom ima prednosti i nedostatke koji se odnose na brzinu, cenu, opcije i pogodnosti.

Mnogi davaoci Internet usluga nude kompletne usluge, uključujući i modeme, elektronsku poštu (skraćeno: e-poštu), i prostor za smeštaj Web strana na mreži.

Korisnička služba i tehnička podrška koju nudi određeni davalac Internet usluga važan su faktor i trebalo bi da budu dostupne 24 časa dnevno, sedam dana u nedelji.

Kada poredite cene, morate znati da nacionalni davalac Internet usluga, koji možda naplaćuje više od sličnog lokalnog davaoca, ima dodatnu prednost zbog toga što su mu na raspolaganju lokalni pristupni brojeve za veće gradove, koji vam mogu zatrebati ako često putujete, a potreban vam je Internet tokom putovanja.

[1] Izvor ovih podataka je RATEL (Republička agencija za telekomunikacije).

1.1.3.2 Jedinstvena adresa resursa

Jedinstvena adresa resursa, tj. URL adresa (**Uniform Resource Locator, URL**) identifikuje pojedinačne Web stranice ili druge resurse (lokacije) na Webu.

Web server i Web stranice na serverima moraju imati jedinstvene adrese kako bi ih računar koji ih traži mogao pronaći. Jednoznačni identifikator umreženog uređaja je IP (Internet Protocol) adresa, a jednoznačni identifikator izvora podataka je URL koji otkriva gde se nalazi server, na kojoj lokaciji na serveru su traženi podaci i kojeg je tipa datoteka koja sadrži određeni dokument. Evo primera URL adrese (koja se naziva i Web adresom):

http://www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-351-9

1.1.3.3 Hiperveze

Web lokacija je kolekcija povezanih Web strana kojima upravlja pojedinac ili organizacija. Dakle, potrebne su vam odgovarajuće veze ukoliko hoćete da među milionima strana dokumenata na Internetu pronađete informacije koje tražite.

Veze između Web strana su specijalna vrsta elektronskih veza koje se zovu *hiperveze* (**Hyperlinks**), a dokumenti sačinjeni pomoću hiperveza zovu se *hipertekst* (**Hypertext**) ili *hipermedija* (**Hypermedia**) ako su dodati zvuk, grafika ili video.

Sledeća slika prikazuje jednu Web stranu: delovi teksta u drugoj boji (što nećete videti na crno-beloj slici) predstavljaju vezu ka drugim Web stranama. Hipertekst, koji pokreće Web, jedna je od onih jednostavnih ideja čiji su efekti veći nego što možete i da zamislite.

Sistem hiperteksta omogućuje stvaranje veza između pojedinih informacija na takav način da se srodne informacije mogu direktno pronaći. Ako pratite takve veze, ubrzo ćete shvatiti da one čine složenu mrežu. Web je izuzetan zato što povezuje informacije sa svih krajeva planete, s raznih računara i iz raznih baza podataka, i to gotovo nevidljivo.

Hiperveze omogućavaju pronalaženje informacija na jedinstven način – kada mišem pritisnete hipervezu, prikazuje se dokument na koji ona upućuje. Na sledećoj slici istaknuta je veza ka Web stranici jednog dela knjige. Ako tu vezu pritisnete mišem, prikazuje se nova Web strana koja zamenjuje onu koja je trenutno na ekranu.

Kad pokazivač miša u obliku strelice postavite iznad hiperveze, on se pretvara u šaku s ispruženim kažiprstom.

Kad pritisnete hipervezu levim tasterom miša, automatski ćete:

- preći na drugi deo tekuće Web strane,
- preći na neku drugu stranu tekuće Web lokacije (slučaj na prethodnoj slici),
- preći na neku drugu Web lokaciju,
- prebaciti datoteku s Web servera na svoj računar,
- pokrenuti aplikaciju, čuti zvuk ili prikazati video snimak.

Prethodna slika prikazuje deo Web lokacije izdavača ove knjige; tekst koji promeni boju kad iznad njega postavite pokazivač miša predstavlja hipervezu. Tekstualne hiperveze su najčešće plave i podvučene.

Veze možete da koristite zato što svi dokumenti na Webu imaju jedinstven URL. To je samo komplikovaniji način da se kaže da svaki dokument ima jedinstvenu adresu koja pokazuje gde se on nalazi na Internetu. Kao što vam kućne adrese pomažu da dođete do nečije kuće, URL adrese vam olakšavaju pronalaženje dokumenata na Internetu.

1.1.4 Sastav i struktura Web adrese

Drugi naziv za Web adresu (koji zvuči više tehnički) jeste jedinstvena adresa resursa (URL). Dakle, prava Web adresa prikazana na prethodnoj slici i u primeru u odeljku 1.1.3.2 glasi:

http://www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-351-9

Svaka Web adresa sastoji se od sledećih delova:

- Prvi deo Web adrese je **http://**. Reč ispred dvotačke je oznaka protokola koji se koristi za prenos Web strane od Web servera do čitača Weba. Mada je definisano desetak protokola, na Internetu se najčešće koristi **http** (protokol za prenos hiperteksta). Da bi svi računari u mreži mogli da razmenjuju informacije, moraju „govoriti istim jezikom“, to jest, moraju koristiti isti protokol. Protokol definiše pravila komuniciranja izmedu računara, tj. pravila za uspostavljanje, održavanje i prekid komunikacije.

HTTP je daleko najzastupljeniji protokol na World Wide Webu – pomoću njega komuniciraju Web čitač i Web server. Komunikacija se odvija u dve faze: faze zahteva i faze odgovora. Server obrađuje zahtev i izvršava ga šaljući Web stranicu ili ga odbija. Jezici kojima se računari sporazumijevaju u mreži zovu se protokoli. Iza dvotačke dolaze dve kose crte (uvek dve obične kose crte, nikad obrnute).

- Drugi deo je osnovna adresa Web strane. Sastoji se od dodatne oznake Web protokola, **www**, imena domena – **mikroknjiga**, i oznake domena – u ovom slučaju, oznake nacionalnog domena, **.rs**. Oznaka domena može da označava i o kakvoj se organizaciji radi (na primer, .com je komercijalna firma, .edu je obrazovna ustanova, .org je neprofitna organizacija, .gov je deo državne uprave itd.). Iza osnovne oznake sledi još jedna kosa crta.
- Treći deo označava lokaciju na serveru na kojoj se dokument nalazi, tj. sadrži putanju. U glavnom direktorijumu mogu biti i poddirektorijumi. U našem primeru, putanja je **store/prikaz.php?**.
- Četvrti deo je ime datoteke sa zatraženom Web stranicom. U našem primeru, ime datoteke je **ref=978-86-7555-351-9**. Ako nema imena, podrazumeva se ime **index.html**.

Kada unosite Web adresu u čitač Weba, protokol i odrednica **www** su opcioni. Na primer, ako unesete **http://www.mikroknjiga.rs** ili samo **mikroknjiga.rs**, čitač će učitati početnu stranu Web lokacije „Mikro knjiga“.

1.1.5 Programi za pregledanje Web stranica – čitači Weba

Program za pregledanje Web strana često se naziva čitač Weba ili samo čitač. Koristi se za pristupanje Web stranama i za njihovo pregledanje. Kad ne bi postojali čitači, ne bi postojao ni Web kakvog ga znamo.

Čitači Weba (**Web Browsers**) računarski su programi koji omogućavaju čitanje Web strana i njihovo prikazivanje na ekranu monitora. Ako imate Windows (XP, Vista ili 7), neki Mac ili bilo koji računar s pristupom Internetu, onda verovatno već imate čitač Weba.

Najčešće korišćeni čitač Weba za kućne i kancelarijske personalne računare jeste Windows Internet Explorer (ranije se zvao Microsoft Internet Explorer), ili skraćeno **IE**, koji ćemo opisati u nastavku. Drugi čitači su Mozilla Firefox, Safari, Opera i Google Chrome. Sledi kratak opis dva najpopularnija čitača.

1.1.5.1 Windows Internet Explorer 8

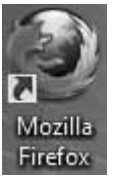
Na sledećoj slici prikazan je prozor Windows Internet Explorera 8 (IE8). U pitanju je poslednja verzija (objavljena 19.03.2009), koja se može besplatno preuzeti s Microsoftove Web lokacije. Može se koristiti kao nadogradnja za Windows XP i Windows Vistu, a isporučuje se zajedno s Windowsom 7. Već se razvija nova verzija, IE9, ali se trenutno ne zna kada će biti objavljena.

Windows Internet Explorer 8 je najpopularniji program za pregledanje Web strana; dostupan je i na srpskom jeziku. Web čitač koji koristi oko 55% korisnika računara širom sveta dobio je izdanje koje je potpuno lokalizovano za tržište Srbije: pored prikazivanja svih komandi i menija na srpskom jeziku, i to na oba pisma – ćirilici i latinici, korisnicima iz Srbije na raspolaganju su i dodaci za Windows Explorer 8 koji su razvijeni specijalno za domaće tržište.

IE8 donosi korisnicima bolje iskustvo u pregledanju Web strana. U poređenju s prethodnim verzijama, bezbedniji je, lakše se koristi i sadrži poboljšanja koja će korisnicima omogućiti da vreme provedeno na mreži iskoriste na najbolji mogući način.

Ugrađeni mehanizmi bolje štite korisnike od napada sa Interneta, virusa i zlonamernih aplikacija, a novi Internet Explorer 8 će vas upozoriti ako posećujete lokaciju koja se smatra nebezbednom ili opasnom po vašu privatnost ili podatke.

1.1.5.2 Mozilla Firefox 3.6



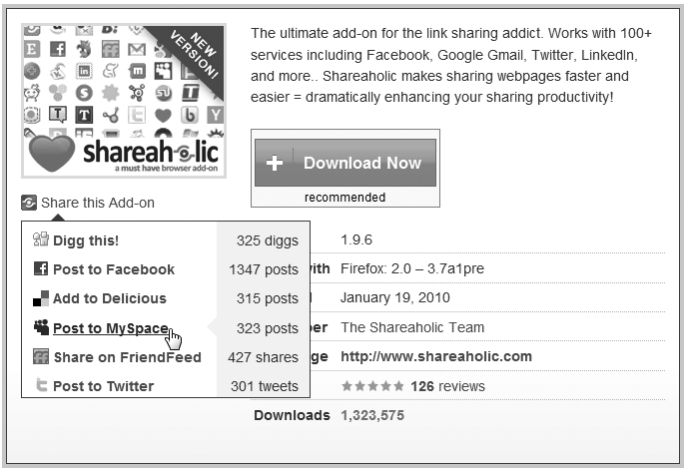
Mozilla Firefox (tekuća verzija je 3.6) takođe je veoma popularan. Postoji verzija i na srpskom jeziku. Pošto je dostigao drugu poziciju, ustoličivši se kao najpopularnija alternativa Internet Exploreru, Firefox je uspeo čak i da ugrozi gotovo apsolutnu dominaciju koju je Microsoftov čitač do sada uživao. Danas Firefox drži oko 31% svetskog tržišta, a Internet Explorer oko 55%.

To je Web čitač otvorenog koda, veličine 8,9 MB (objavljen 21.01.2010). Evo par osobina koje karakterišu Firefox 3.6:

- Velika stabilnost.
- Povećana sigurnost (u odnosu na njegove ranije verzije).
- Učitavanje stranica u pojedinačne kartice (učitavanje više stranica unutar jednog prozora).
- Ugrađena alatka za skidanje podataka (**Download Manager**).
- Dodaci koje korisnik po potrebi može ugraditi u čitač (nekoliko dodataka se odnose i na Vikipediju).
- Proširenja (**Extensions**) – dodaju nove ili menjaju postojeće funkcionalnosti.
- Teme (**Themes**) – služe za izmenu izgleda samog programa.
- Priključci (**Plugins**) – za pregled Web sadržaja u formatu koji nije **HTML**.
- Podrška za Web kanale (**Web Feed**).
- Ponovno učitavanje aktivnih stranica nakon „pucanja“ čitača.
- Zaštita od pokušaja preuzimanja ličnih podataka (**Phishing**).

Korisnici Firefoxa mogu i sami značajno da unaprede ili promene njegovu funkcionalnost. Na primer, mogu pridružiti nove funkcije pokretima miša (**Mouse Gestures**), dodati opcije koje se odnose na jezičke, blokirati reklame ili izvršavanje skriptova.

Mogu se dodati čak i čitave mini aplikacije, na primer za kalendar ili **FTP**[1] prenos. Postoji i dosta proširenja vezanih za vikipediju i za brojne druge popularne Web lokacije. Takođe, postoji i nekoliko proširenja koja se odnose na srpski jezik.



[1] **FTP** (**File Transfer Pprotocol** – protokol za prenos datoteka) najčesće je koriscen protokol za prenos podataka izmedu dva računara na mreži.

Na sledećoj slici prikazan je izgled Firefoxovog prozora, instaliranog pod OS Windows 7.

1.1.6 Šta je pretraživač Weba?

Na Internetu je dostupna ogromna količina informacija. Upravo zbog te količine informacija vrlo je teško pronaći dokument koji nam je potreban. Gotovo je nemoguće znati postoji li neki dokument, a ako i postoji, gde se nalazi. Da bi se taj problem rešio, razvijen je određen broj programskih rešenja koji ubrzavaju traženje informacija na Internetu.

Zadatak pretraživanja je da što efikasnije vrati što kvalitetniji rezultat. Efikasnost se meri brzinom koja protekne od pritiska dugmeta do pojave rezultata, a kvalitet se meri sa brojem rezultata (stranica) koje pretraživač Weba vrati i njihovom relevantnošću. (Pretraživač Weba ili samo pretraživač često se pominje i pod nazivom mašina za pretraživanje – **Search Engine**). Za brzinu je zadužen proces indeksiranja i algoritmi koji sortiraju podatke. Broj rezultata zavisi od broja indeksiranih stranica, to jest od broja stranica koje pretraživač poseti i preuzme u bazu. Relevantnost je povezanost sadržaja Web lokacije s traženim pojmom i zavisi od kvaliteta algoritama koje pretraživač koristi.

Proces pretrage počinje kada na stranici pretraživača Weba unesete neku reč ili izraz. Kada pritisnete dugme Pretraga (**Search**), fraza se prosleđuje pretraživaču koji traži frazu na Internetu.

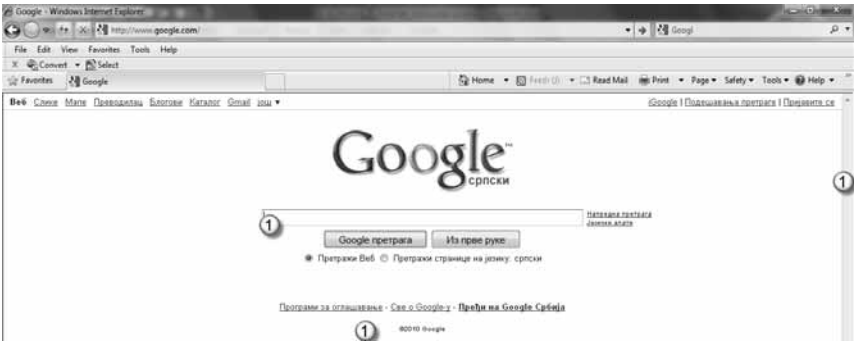
Rangiranje rezultata je proces sortiranja na osnovu relevantnosti. Najpre se za svaki dokument koji sadrži tražene reči broji pojavljivanje fraze. Zatim se za svako pojavljivanje reči gleda pozicija u dokumentu i da li je ta reč posebno naglašena (podebljana, kurzivna, podvučena).

Svaka pozicija i naglašenost reči nosi određeni težinski faktor. Sabiranjem težinskih faktora svih pojavljivanja dobija se samo delić vrednosti po kojoj se posle dokumenti sortiraju. Ostali faktori relevantnosti zavise od samog pretraživača.

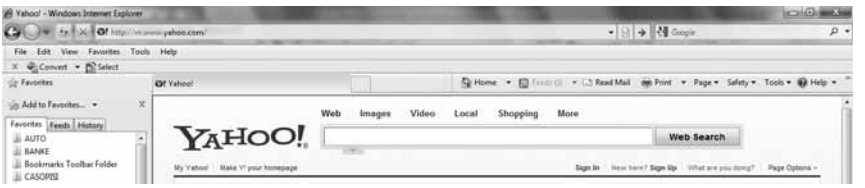
Nakon završenog sortiranja dokumenata (svih onih koji sadrže unetu frazu) po relevantnosti, pretraživač prebacuje korisnika na novu stranicu na kojoj se nalaze izlistane sortirane hiperveze ka dokumentima.

Pretraživači ne prikazuju informacije hijerarhijski jer se radi o ogromnim bazama podataka koje se pretražuju preko ključnih reči. Najpoznatija tri pretraživača Web su:

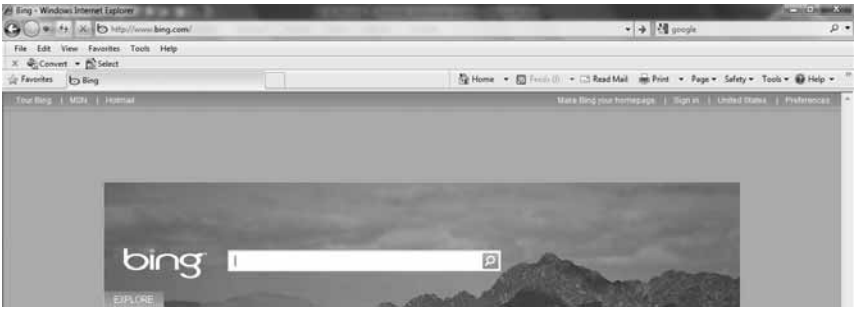
- Google (http://www.google.com ili www.google.rs) – najzastupljeniji pretraživač, sa oko 85% tržišta.



- Yahoo! (http://m.www.yahoo.com) drži oko 6% tržišta.



- Bing (http://www.bing.com) koji je Microsoft lansirao kao nov servis za pretraživanje Interneta i drži oko 6% tržišta. Novi sistem pretraživanja je, prema navodima iz Microsofta, zasnovan na „sistemu odlučivanja“ kojim se uvodi potpuno nov pristup pretraživanju Interneta.



Mnogi misle da pretraživači Weba mogu da pronađu sve Web prezentacije koje sadrže zadate reči ili fraze. Međutim, to nije tačno. Kad zadate upit, pretraživači će vam nabrojati samo one Web strane koje su registrovane na tom pretraživaču. Ukoliko zadate isti upit na različitim pretraživačima, dobićete različite rezultate.

Način na koji se prikazuju rezultati razlikuje se od jednog do drugog pretraživača. Web strana s rezultatima pretraživanja obično prikazuje listu sa 10 Web adresa koje odgovaraju zadatom kriterijumu, i kratak opis sadržaja na toj adresi.

Na kraju strane s rezultatima pretraživanja nalaze se hiperveze koje omogućavaju prikazivanje narednih i/ili prethodnih 10 Web strana.

Pored tri navedena najpopularnija pretraživača, pomenimo još dva: Altavista i Ask.

Navodimo i neke domaće pretraživače kao što su: Krstarica (http://www.krstarica.com), Pogodak (http://www.pogodak.rs), YU Search (http://www.yusearch.com), Srpko (http://www.srpko.com) i Trazim (http://www.trazim.com).

Važno je da znate da opcije i perfomanse variraju od jednog do drugog pretraživača i da se s vremenom menjaju i razvijaju. Najbolje je upoznati i koristiti više pretraživača Weba. To omogućava da u datoj situaciji upotrebite onaj koji najviše odgovara određenoj pretrazi. Kada birate pretraživače, tražite one sa sledećim osobinama:

- Lako se koriste.
- Brzo daju rezultate pretrage.
- Daju najrelevantnije rezultate za pretragu pomoću ključnih reči.
- Sadrže ograničen broj reklama ili ih uopšte ne sadrže.

Proces pretraživanja Weba sastoji se od sledećih koraka:

1. Izaberite najbolji pretraživač.
2. Formulišite upit pretrage.
3. Obavite pretraživanje.
4. Pregledajte rezultate pretraživanja.
5. Ocenite relevantnost pretraživanja.

Pretraživač Weba ima tri glavne komponente: skener, indeks i softver. Kada korisnik unese ključne reči u tekstualno polje za pretragu u pretraživaču, softver pretraživača ih poredi sa svojim indeksom, sastavlja listu Web strana koje su relevantne za zadate ključne reči i uređuje listu po određenom redosledu.

Plaćene hiperveze ne utiču na rangiranje u listi rezultata Googlea. Umesto toga, Google sve njih stavlja na vrh desnog stupca, odvojeno od rezultata pretraživanja. On ne koristi slike, banere i iskačuće reklame, čime se skraćuje vreme učitavanja i smanjuje zagušenje. Drugi pretraživači počinju da slede ovaj primer.

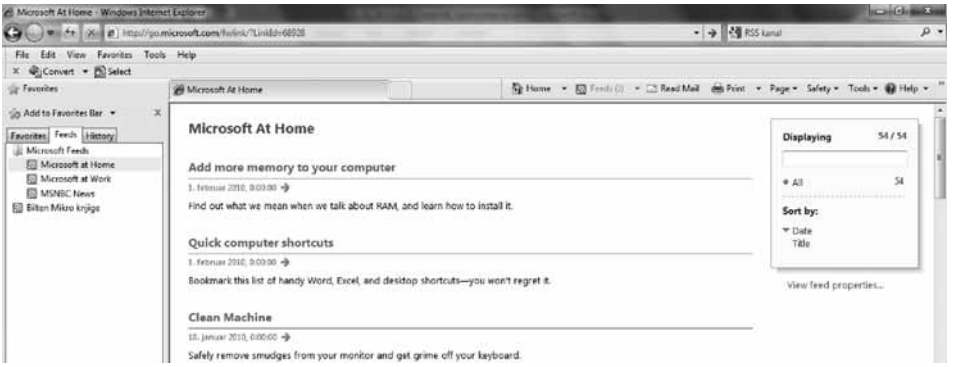
1.1.7 Šta je RSS kanal? Svrha prijavljivanja na RSS kanal

Skraćenica **RSS** zamenjuje sintagmu **Really Simple Syndication** (Zaista jednostavna distribucija), a koristi se za opis tehnologije koja se upotrebljava za brzo objavljivanje dokumenata koji se često ažuriraju (vesti, blogova, audio i video zapisa) i koji se distribuiraju preko kanala (**Feeds**). RSS je usluga (servis) putem koje dobijate informacije o ažuriranju Web lokacije. Ako često posećujete istu Web lokaciju i hoćete da vas obaveštavaju o novim informacijama na toj lokaciji, pretplatite se (**Subscribe**) na njihovu listu.

Oni vam po postavljanju novog unosa na njihovu Web lokaciju (vest, blog itd.) šalju informaciju (**Feed, Web Feed**) sa delimičnim ili potpunim sadržajem novog unosa.

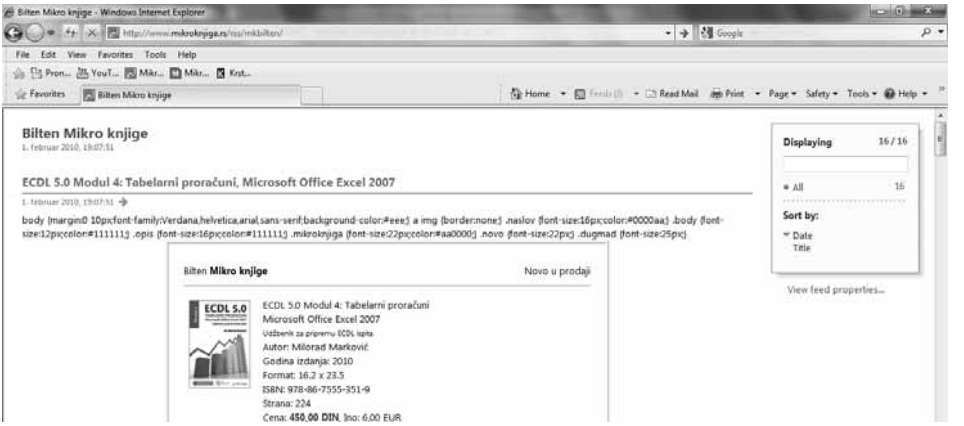
Ne postoji na svakoj Web lokaciji mogućnost dobijanja vesti (RSS kanala). Na lokacijama gde postoji ta mogućnost, obično se u čitaču Weba prikazuje narandžasta ikonica RSS-a, kao na slici desno.

Kod RSS kanala s delimičnim unosom sadržaja, na jednom mestu ćete pregledati naslove, a kada vas neki naslov zainteresuje, pritisnite ga i on vas vodi na Web stranicu na kojoj je nalazi ceo tekst vesti, članka, bloga, kao što je prikazano na slici.



Velika prednost ovakve vrste RSS kanala nad „običnim“ pregledom Web stranice, počiva upravo u njegovoj brzini i jednostavnosti promene – ne morate pristupati nekoj stranici da biste videli najnovije izmene (vesti i slične informacije, koje se menjaju svakih nekoliko minuta) već je dovoljno da „preletite“ preko najnovijih izmena na nekoliko Web lokacija u roku od nekoliko sekundi. RSS čitači to obično rade automatski (u određenim vremenskim intervalima) i „prijave“ vam najnovije izmene.

RSS kanal s potpunim sadržajem takođe je zanimljiv; primer takvog kanala prikazan je na sledećoj slici. U pitanju je RSS kanal izdavača ove knjige koji vas sa potpunim sadržajem obaveštava o svojim novim izdanjima. Da biste pročitali primljene informacije, dovoljan vam je noviji čitač Weba, kao što je IE8, jer on podržava RSS kao i njegov prethodnik, IE7.



Postoje i namenski RSS čitači kao što su **RSSReader** i **FeedReader**, ali oni nisu neophodni ukoliko koristite novije Web čitače koji podržavaju RSS kanale.

Kada se pretplatite na RSS, ispravke možete pratiti na kartici **Feeds** s trake **Favorites** (Omiljene lokacije). Da biste se pretplatili na RSS i pratili ga na traci **Favorites**, pogledajte korake iz odeljka 2.4.1.2.

1.1.8 Šta je podkast? Svrha prijave na podkast

Podkast je digitalna datoteka koja sadrži audio ili audio-video zapis koji se distribuira preko Interneta pomoću RSS tehnologije, a namenjen je gledanju (ili slušanju) na računaru, digitanom prenosnom plejeru poput iPoda ili televizije uz korišćenje uređaja poput Apple TV. Izvorni naziv **Podcast** složenica je od reči **POD (Personal On Demand)** i engleske reči **Broadcast** (Emitovanje).

Iako su na početku podkasti bili isključivo audio datoteke, najčešće u formatu .mp3, danas se za podkast često smatraju video-sadržaji. Video-podkast se još naziva i vidkast (**Vidcast**), a osobe koje se bave podkastingom nazivaju se podkasteri. RSS agregatori specijalizovani za skidanje podkasta zovu se podkečeri (**Podcatchers**). Podkečer, ili podkast klijent, jeste program koji se koristi za preuzimanje različitih medijskih sadržaja preko RSS kanala.

Podcast je vrsta ličnog Internet radija ili videa. Za razliku od uobičajenog Internet radija (ili Internet TV-a) koji slušate, odnosno gledate prema unapred definisanom programu, podkast slušate (odnosno gledate) po svom izboru; odaberete podkast koji vam je interesantan, preuzimate ga na lokalni čvrsti disk i posle po želji slušate (odnosno gledate) kod kuće na računaru ili ga prebacujete na mp3 (odnosno mp4) plejer i slušate (odnosno gledate) van kuće.

Ta tehnologija je jako mlada (razvoj je počeo 2001. u SAD). Prvi podkečer razvijen je krajem 2003. i postao je popularan u 2004. Kad je firma Apple dodala podkasting u svoj softver **iTunes**, odmah je postao najpopularniji program za preuzimanje medijskih sadržaja.

iTunes je digitalni plejer koji se koristi za reprodukciju i organizovanje muzičkih i video datoteka. On je istovremeno i interfejs preko kojeg upravljate sadržajem na Appleovim proizvodima: iPodu (digitalnom plejeru), iPhoneu (mobilnom telefonu) i iPadu (tabličnom računaru). Uz to, **iTunes** se može povezati preko Interneta sa prodavnicom iTunes da biste kupili i preuzeli: muziku, muzički video, TV serije, aplikacije, igrice za iPod, audio knjige, podkastove, dugometražne filmove itd. Primer prozora **iTunesa** prikazan je na slici.

1.2 Bezbednost

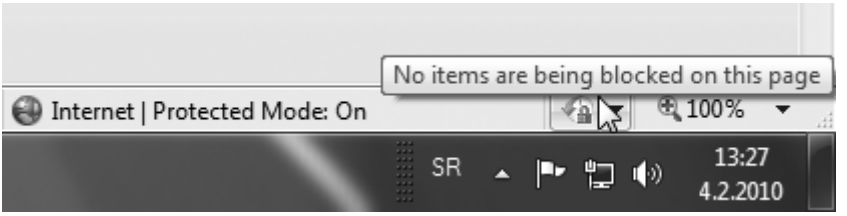
1.2.1 Prepoznavanje zaštićene Web lokacije: https, oznaka katanca

Zaštićene Web lokacije ograničavaju pristup. Neke kompanije omogućavaju pristup delovima svoje lokacije samo klijentima koji plaćaju; druge od korisnika zahtevaju da se predstave pre nego što im dozvole pristup, tako da mogu bolje reklamirati svoje proizvode i usluge.

Za pristup zaštićenoj Web lokaciji najčešće treba da date svoje lične podatke, tj. da se registrujete tako što ćete uneti korisničko ime (**User Name**) i lozinku (**Password**). Većina kompanija na taj način štiti Web lokacije koje su namenjene samo za njene klijente i/ili zaposlene.

Drugi primer su komercijalne Web lokacije gde morate da se pretplatite kako biste videli njihov sadržaj.

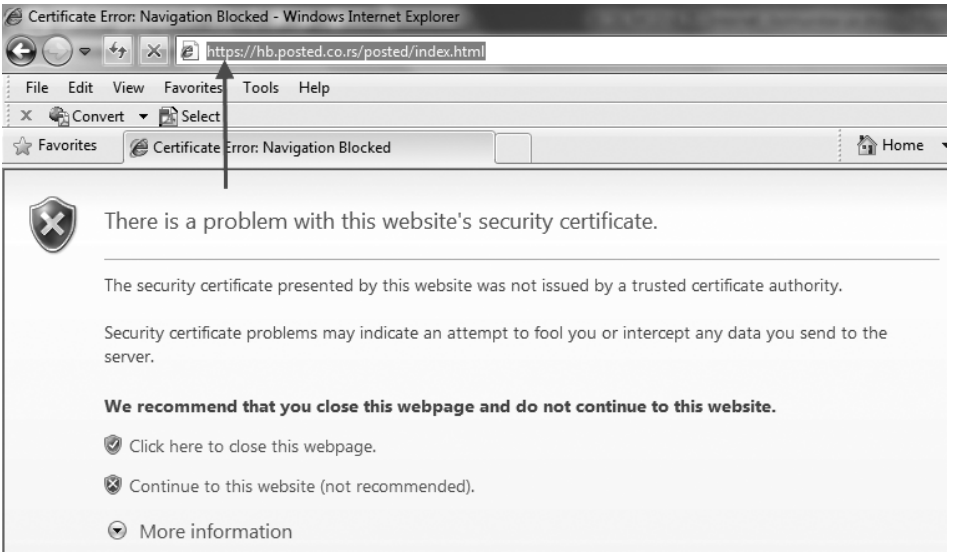
Zaštićene Web lokacije imaju na statusnoj traci ikonicu u vidu katanca, kao na slici.



Posebna vrsta zaštićenih Web lokacija jesu lokacije banaka, zbog tzv. elektronskog bankarstva. Bez namere da se ovde bavimo tom temom, samo ukazujemo na tu vrstu zaštite koja je višeslojna i s dodatnim uređajima za zaštitu podataka banke i klijenta. Na sledećoj slici je prikazan primer početne stranice zaštićene Web lokacije jedne banke.

Treba uočiti da se u Web adresi zaštićenih Web lokacija koristi protokol **HTTPS** (**Hypertext Transfer Protocol Secure**), a ne **HTTP**. On je kombinacija protokola **HTTP** s protokolom **SSL/TLS** i obezbeđuje zaštitu i sigurnu komunikaciju sa serverom.

HTTPS veze se često koriste za novčane transankcije na Webu i za osetljive transakcije u korporativnim informacionim sistemima. **HTTPS** ne treba mešati sa **Secure HTTP** (**S-HTTP**).



Transport Layer Security (**TLS**) i njegov prethodnik, **Secure Sockets Layer** (**SSL**), jesu protokoli za šifrovanje (kriptografiju) koji omogućuju bezbednu komunikaciju preko mreža kao što je Internet.

1.2.2 Digitalni sertifikat

Ako hoćete nekome da pošaljete šifrovanu poruku, morate prvo dobiti njegov javni ključ. Međutim, kako možete biti sigurni da je to zaista njegov ključ? Taj problem se rešava upotrebom digitalnih sertifikata. Možemo ih nazvati i digitalnom ličnom kartom, jer oni zaista to i jesu – digitalna lična karta u Web prostoru, sredstvo kojim ćete vi ili osoba s kojom komunicirate dokazati identitet na Internetu.

Pošto na Internetu nema policije koja bi proverila vaše podatke i izdala vam ličnu kartu, pojavile su se kompanije koje imaju ulogu 'treće strane' – **CA** (**Certificate Authority**) čija je uloga da provere i utvrde nečiji identitet i nakon toga mu izdaju digitalni sertifikat.

Kako to funkcioniše u praksi? Na primer, podnesete zahtev za izdavanje sertifikata CA kompaniji (kod nas je prvo registrovano sertifikaciono telo Pošta Srbije – www.ca.posta.rs). CA proverava vaš identitet na osnovu ličnih dokumenata koje ste im prikazali pri podnošenju zahteva.

Ako je sve u redu, prosleđujete im svoj javni ključ za koji CA izradi digitalni potpis i nakon toga izdaje sertifikat kojim se potvrđuje da taj javni ključ zaista pripada vama. Ako vi kasnije želite da komunicirate s nekim, pri prvom kontaktu mu šaljete digitalni sertifikat i svoj javni ključ. Pošto svi poznatiji komunikacioni programi u sebi već imaju uključene javne ključeve CA kompanija kojima se veruje, primalac po prijemu ove poruke lako utvrđuje validnost vašeg sertifikata.

Svi ovi podaci formiraju sertifikat koji se na kraju šifruje tajnim ključem CA. Ako korisnik ima poverenja u CA i ima CA javni ključ, može biti siguran u ispravnost sertifikata.

Digitalni sertifikati i tajni (privatni) kriptografski ključevi mogu da se čuvaju na sledećim medijima:

- Čvrsti disk računara, disketa, CD ili USB memorijski token.
- **PKI** (**Public Key Infrastructure**) smart kartica (slika levo).

- **PKI** (**Public Key Infrastructure**) USB memorijski token (slika gore desno).

Najviši nivo sigurnosti postiže se ukoliko se kao mediji za digitalne sertifikate i tajne (privatne) kriptografske ključeve koriste PKI smart kartice i PKI USB memorijski token. Kvalifikovani digitalni sertifikati i tajni (privatni) kriptografski ključevi mogu da se čuvaju isključivo na PKI smart karticama i PKI USB memorijskim tokenima koji su sredstvo za formiranje kvalifikovanog digitalnog potpisa (**Secure Signature Creation Device, SSCD**).

Digitalni sertifikat služi i za šifrovanje podataka s vaše kreditne kartice prilikom kupovine preko Interneta.

1.2.3 Pojam šifrovanja

Kad se lične, finansijske, vojne informacije ili informacije državne bezbednosti prenose preko Interneta, do njih mogu da dođu neovlašćena lica. Takvi problemi se mogu izbeći šifrovanjem podataka.

Pri kupovini na Internetu, osnovnu zaštitu pruža šifrovanje podataka; tako niko ne može da pročita broj vaše kreditne kartice i da ga kasnije zloupotrebi.

Šifrovanje je postupak preuređivanja izvornih podataka tako da niko tokom njihovog putovanja Internetom ne može da ih pročita. Ako neovlašćena osoba čak i uhvati te podatke tokom prenosa, neće moći da ih protumači i izmeni. Šifrovanje se obavlja na zaštićenim (bezbednim) serverima, koji šifruju svu komunikaciju s vama.

U kriptografiji, šifra je algoritam za šifrovanje i dešifrovanje – niz precizno definisanih koraka koji slede jedan za drugim. U netehničkoj upotrebi, šifra i kôd predstavljaju sinonime, ali su u kriptografiji to različiti pojmovi. U klasičnoj kriptografiji, šifra je odvojena od koda. Načelno, u kodu se zamenjivanje vrši na osnovu obimne knjige kodova, u kojoj se reči i fraze zamenjuju slučajnim nizom znakova.

Originalna informacija je poznata kao otvoreni tekst, a šifrovani oblik kao šifrovani tekst ili šifrat. Šifrovana poruka sadrži sve informacije iz otvorenog teksta, ali nije u obliku koji čovek ili računar mogu čitati bez primene odgovarajućeg mehanizma za dešifrovanje – treba da predstavlja nasumične znakove za sve kojima nije namenjena.

Operacija šifrovanja obično zavisi od dodatne informacije zvane ključ. Procedura šifrovanja varira u zavisnosti od ključa, koji menja detalje algoritma. Ključ mora da se izabere pre šifrovanja poruke. Bez poznavanja ključa trebalo bi da je teško, ili skoro nemoguće, dekriptovati šifrat u čitljiv otvoreni tekst.

Treba razlikovati termine dešifrovanje i dekriptovanje:

- Dešifrovanje je pretvaranje šifrata u otvoreni tekst kad je ključ poznat; obavlja ga osoba kojoj je poruka namenjena.
- Dekriptovanje je pokušaj pretvaranja šifrata u otvoreni tekst kad ključ nije poznat – obavljaju ga osobe kojima poruka nije namenjena. Dekriptovanje je deo kriptoanalize.

Postoji više tipova šifrovanja. Algoritmi koji su se koristili u prošlosti značajno se razlikuju od modernih metoda, a moderna šifra može da se klasifikuje prema načinu rada i da li koristi jedan ili dva ključa.

Moderne metode šifrovanja mogu da se podele po dva kriterijuma: po tipu korišćenog ključa i tipu ulaznih podataka.

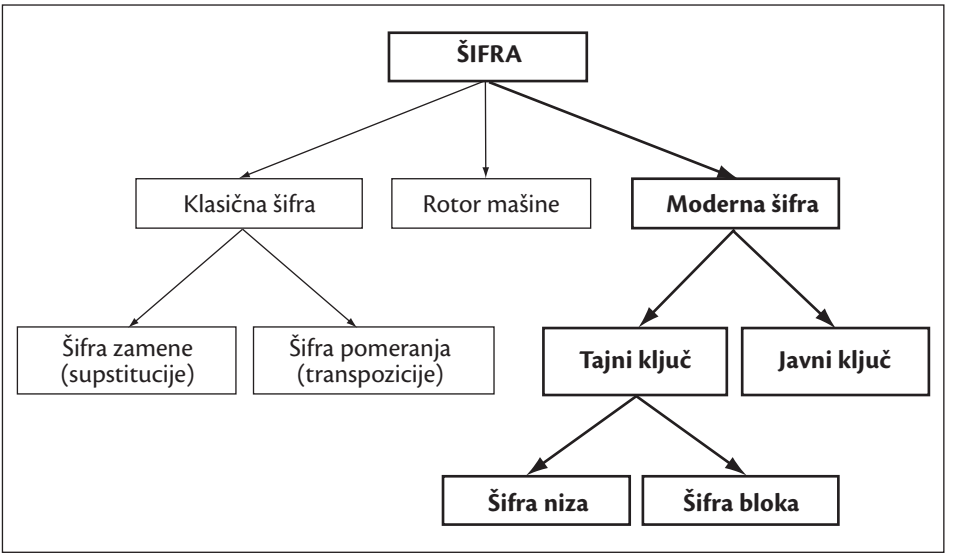
Po tipu ključa, šifre se dele na:

- Algoritme simetričnog ključa (kriptografija s tajnim ključem), gde se isti ključ koristi i za šifrovanje i za dešifrovanje.
- Algoritme asimetričnog ključa (kriptografija s javnim ključem), gde se koriste dva različita ključa za šifrovanje i dešifrovanje.

  U algoritmu simetričnog ključa (**DES** i **AES**), pošiljalac i primalac moraju da imaju isti ključ, koji je unapred pripremljen i koji mora da bude tajan za sve kojima nije namenjen – pošiljalac koristi taj ključ za šifrovanje, a primalac isti taj ključ za dešifrovanje. U algoritmu asimetričnog ključa (npr. **RSA**), postoje dva posebna ključa: „javni ključ“ se objavljuje i omogućava pošiljaocu da šifruje sadržaj poruke, dok „tajni ključ“ primalac čuva kao tajnu i koristi ga da ispravno dešifruje poruku.

Po tipu ulaznih podataka, šifre se mogu svrstati u dve grupe:

- Šifra bloka, kojom se šifruje blok podataka fiksne dužine, i
- Šifra niza, kojom se šifruje kontinualni niz podataka.



Pomenimo i to da se u svetu najčešće koristi algoritam **DES** (**Data Encryption Standard**). **DES** je dugo bio sinonim za sigurno šifrovanje.

Danas se za šifrovanje i dešifrovanje e-pošte najčešće koristi program **Pretty Good Privacy (PGP)**, pa vam predlažem da ga isprobate, ukoliko imate potrebe za zaštitom prepiske.

Šifrovanje i digitalni potpis su kriptografske tehnike koje se koriste da bi se zaštitile informacije.

1.2.4 Sigurnosne pretnje: virusi, crvi, trojanski konji, špijunski programi. Pojam malvera

1.2.4.1 Pojam malvera

Malver (**Malware**) je složenica od engleskih reči **Malicious** i **Software**; u prevodu „maliciozni“ ili „zlonamerni“ softver. Osim klasičnih računarskih virusa, obuhvata sve vrste softvera koji na bilo koji način mogu da ugroze računarski sistem ili računarsku mrežu, kao što su: trojanci (**Trojan Horses**), računarski crvi (**Worms**), rutkit (**Rootkits**), zadnja vrata (**Backdoor**), različite vrste špijunskih programa (**Spyware**), advera (**Adware**), dajlera (**Dialers**), krimvera (**Crimeware**) i drugog štetnog softvera.

1.2.4.2 Virusi

Virus je program ili kôd koji se sam umnožava u drugim datotekama s kojima dolazi u kontakt. Može zaraziti bilo koji program, sektor za podizanje računara i dokument koji podržava makroe, tako da promeni sadržaj te datoteke i u nju kopira svoj kôd.

Računarski virus se obično sastoji od dva dela:

- Prvi deo je samokopirajući kôd koji omogućava razmnožavanje virusa.
- Drugi deo je informacija koja može biti bezopasna ili opasna.

Neki se sastoje samo od samokopirajućeg koda.

Da bi se virus umnožio, ponekad je potrebna akcija čoveka, poput pokretanja programa koji sadrži virus ili otvaranja zaražene datoteke.

Vrste računarskih virusa:

- boot sektor virusi – napadaju sektor za podizanje sistema (**Master Boot**),
- parazitski – zaraze izvršne datoteke tako što dodaju svoj sadržaj u strukturu programa,
- svestrani virusi – napadaju **boot** sektore i izvršne programe,
- virusi pratioci – naprave `.com` datoteku koristeći ime postojećeg `.exe` programa i ugrade u nju svoj kôd.
- link virusi – u trenu inficiraju napadnut računarski sistem; mogu da izazovu pravi haos na disku,
- makro virusi – mogu da sami sebe kopiraju, brišu i menjaju dokumente.

Podela virusa prema mestu u memoriji:

- virusi u privremenoj memoriji – ostaju u memoriji računara nakon aktiviranja koda virusa.
- virusi koji nisu u privremenoj memoriji.

Virusi se mogu prenositi na mnogo načina; u današnje vreme, skoro svi virusi se prenose preko Interneta, a mogu se prenositi i preko USB fleš memorija, izmenjivih diskova, CD-ova i drugi prenosivih medija.

1.2.4.3 Računarski crvi

Računarski crvi (**Worms**) jesu programi koji umnožavaju sami sebe. Pri tome koriste računarske mreže da bi se kopirali na druge računare, često bez uticaja čoveka. Za razliku od virusa, svojim delovanjem ne moraju inficirati druge programe.

Mogu stići i kao datoteka u e-pošti te im pristup računaru omogućuju propusti u operativnim sistemima i aplikacijama. Crvi otežavaju rad mreže, a mogu oštetiti podatke i smanjiti sigurnost računara.

Vrste računarskih crva:

- Crv – može oštetiti podatke i smanjiti sigurnost računara.
- **Mailer** i **mass-mailer** – sami se šalju elektronskom poštom.
- Mešane pretnje – za svoje pokretanje, prenos i širenje napada kombinuju karakteristike virusa, crva i trojanskih konja s propustima u softveru.

Crvi i virusi su napravljeni za prenos korisnih podataka (**Payload**) na računar. **Payload** služi za obavljanje određenih funkcija kao što su brisanje ili promena podataka, instalisanje softvera na računar i izradu stražnjih vrata koja napadač može kasnije upotrebiti da bi dobio neovlašćen pristup računaru. Internet crvi i virusi stvaraju probleme inficiranim računarima, ali crvi mogu napraviti veću štetu zbog mrežnog prometa koji generišu prilikom širenja Internetom.

Najbolja zaštita od virusa i crva je antivirusni softver. On može da spreči instaliranje virusa, a može i da otkrije, izoluje i ukloni crve i viruse s računara koji su se provukli kroz odbrambene mehanizme. Ipak, antivirusni softver može da vas zaštiti samo od poznatih virusa, a od onih za koje se ne zna (novih virusa) teže se zaštititi. Metode zaštite su i zaštitni zidovi (**Firewall**), neotvaranje neobičnih ili neočekivanih poruka e-pošte i redovno ažuriranje softvera. O tim temama govorićemo u narednim odeljcima.

1.2.4.4 Trojanski konji

Trojanskim konjem (trojancem) označavaju se u računarskom žargonu zlonamerni programi, koji su „maskirani“ kao korisni ili se proširuju „prikačeni“ na druge korisne programe. Trojanci obično sprovode neželjene akcije u računaru i to u pozadini i prikriveno. Najčešća od tih neželjenih akcija je otkrivanje korisničkih lozinki, bankovnih podataka i drugih poverljivih informacija „prisluškivanjem“ razmene podataka ili čitanjem odgovarajućih datoteka, i prosleđivanje podataka „vlasniku“ trojanskog konja.

Postoje i trojanski konji u službi policije, koji se bave prikupljanjem informacija s ciljem otkrivanja krivičnog dela (**Remote Forensic Software**). Taj oblik špijuniranja građana je u nekim zemljama zakonit i vrši se po sudskom nalogu (npr. SAD, Australija), a u nekima je, i pored sukoba sa ustavom, u fazi pripreme.

Trojanci se šire pri instaliranju ili ažuriranju komercijalnih operativnih sistema i drugih softverskih i hardverskih komponenata računara, kao i preko davalaca Internet usluga, infiltriranjem u postojeće mehanizme prenosa podataka; davaoci Internet usluha takvu mogućnost u svojim proizvodima i uslugama, na zahtev dotične države, moraju predvideti.

Poznati trojanci su: Back Orifice, Netbus, Subseven i Zenux.

1.2.4.5 Špijunski programi

Špijunski program (**Spyware**) široka je kategorija malicioznog softvera čija je namena da presreće ili delimično preuzima kontrolu nad radom na računaru, bez znanja ili dozvole korisnika. Sam naziv sugeriše da je reč o programima koji nadgledaju rad korisnika, ali je to danas široka paleta programa koji zloupotrebljavaju korisnički računar za sticanje koristi za neku treću osobu.

Špijunski program se razlikuje od virusa i od crva po tome što se obično ne umnožava. Kao mnogi novi virusi, špijunski program iskorišćava zaražene računare za komercijalnu dobit. Tipične taktike su prikazivanje netraženih iskačućih reklama; krađa ličnih informacija (uključujući i financijske informacije kao što su brojevi kreditnih kartica i lozinke); praćenje aktivnosti na Internetu za marketinške svrhe; ili preusmeravanje HTTP zahteva na reklamne stranice. U nekim slučajevima, špijunski program se koristi za proveru poštovanja uslova licence za korišćenje programa.

Zaraza se u najvećem broju slučajeva događa prilikom posete stranicama sa ilegalnim ili pornografskim sadržajem.

1.2.5 Ažuriranje antivirusnog softvera kao najbolja zaštita od sigurnosnih pretnji

Antivirusni softver je softver koji se koristi za identifikaciju i uklanjanje računarskih virusa, i svakog drugog softvera koji može da ošteti ili nanese štetu računarskom softveru, i koji se jednim imenom naziva malver.

Za razliku od prvobitnih antivirusnih programa koji su se zasnivali isključivo na tretiranju računarskih virusa, moderni antivirusni softver štiti sistem od što većeg broja različitih mogućih malvera, kao što su crvi, trojanci, špijunski programi, napadi pecanjem (**Phishing**), zadnja vrata, rutkit itd.

Postoji nekoliko metoda koje antivirusni softver koristi za identifikaciju mejlvera. U zavisnosti od softvera može se koristiti i više metoda:

- *Detekcija zasnovana na potpisima* – najčešće je korišćena metoda za identifikaciju mejlvera (štetni softver u e-pošti). Da bi pronašao virus ili drugi mejlver, softver upoređuje sadržaj datoteke sa sadržajem kataloga potpisa virusa. Pošto virus može biti ugnežđen u samu datoteku, proverava se i njen sadržaj, te sadržaj svih njenih sastavnih delova, ako se radi o složenoj ili komprimovanoj datoteci.
- *Detekcija štetnih aktivnosti* – antivirusni softver nadgleda softver u okruženju s kojim računarski sistem komunicira. Ukoliko otkrije sumnjive aktivnosti nekog softvera, dodatno ga detaljno proverava koristeći neku od metoda detekcije. Ova metoda je pogodna za detekciju novih i nepoznatih virusa.
- *Heuristička metoda* – slično metodi detekcije štetnih aktivnosti, ova metoda se može upotrebiti za otkrivanje novih i nepoznatih virusa. Može se koristiti na dva načina: analiza datoteka i emulacija datoteka. Analiza datoteka je proces traganja za sumnjivim komandama u datotekama. Ako, recimo jedna datoteka sadrži komandu: formatiraj disk C, heuristički softver će detaljno proveriti tu datoteku. Slabost ove metode je to što ona može znatno usporiti računarski sistem proveravajući veliki broj datoteka.

  Emulacija datoteka je metoda koja izvršava program u virtuelnom okruženju i beleži sve akcije tog programa. Analizom zabeleženih akcija može se utvrditi da li program može ugroziti računarski sistem.

Alati za uklanjanje virusa (**Virus Removal Tools**) predstavljaju softver za uklanjanje specifične vrste virusa. Za razliku od kompletnih antivirusnih programa, oni su namenjeni samo za određenu grupu virusa, ali ih zato uklanjaju znatno efikasnije. Pošto napadi zlonamernih programa (malvera) postaju sve češći, pažnja se pomera od virusa i špijunskog softvera ka zaštiti od zlonamernih programa, pa su razvijeni programi za borbu protiv njih.

Anti-malver programi se bore protiv malvera na dva načina:

- U realnom vremenu štite računar od instaliranja zlonamernih programa. Ova vrsta zaštite od špijunskog softvera radi na isti način kao zaštita od virusa tako da anti-malver softver skenira sve dolazne mrežne podatke na zlonamerni softver i blokira svaku pretnju koja nailazi.
- Anti-malver programi se mogu koristiti samo za otkrivanje i uklanjanje zlonamernih programa koji su već instalirani na računaru. Ova vrsta zaštite od zlonamernih programa mnogo se lakše koristi, pa je i popularnija. Ti programi skeniraju sadržaj baze registara (**Registry**), datoteke operativnog sistema i instaliranih programa na računaru i daju listu pronađenih pretnji, dozvoljavajući korisniku da izabere datoteke koje će da obriše ili sačuva, ili da uporedi tu listu sa listom poznatih zlonamernih programa i ukloni odgovarajuće datoteke.

Zaštita u realnom vremenu od zlonamernih programa radi identično kao antivirusna zaštita u realnom vremenu: datoteke na disku skeniraju se tokom preuzimanja i blokiraju se aktivnosti komponenata koje predstavljaju zlonamerni softver. U nekim slučajevima, to može takođe da zaustavi pokušaje zlonamernog softvera da instalira stavke za pokretanje ili da modifikuje podešavanja u čitaču Weba.

Anti-malver mora redovno da se ažurira kako bi bio efikasan protiv novih zlonamernih programa. Većina tih programa se automatski ažurira, ali ih možete ažurirati i ručno.

1.2.6 Zaštitni zid pomaže da se računar zaštiti od upada

Zaštitni zid (**Firewall**) jeste hardver i/ili softver koji u sklopu računarske mreže može da spreči nepropisan ili neželjen prenos podataka preko mreže koji je zabranjen na osnovu sigurnosne politike postavljene na mreži.

Zaštitni zid ima zadatak da kontroliše (dozvoljava ili odbija) protok podataka između različitih zona u računarskoj mreži. Zone se dele na osnovu stepena poverenja u bezbednost nekog dela mreže.

Obično se zona Interneta smatra nesigurnom, dok se lokalna mreža smatra relativno sigurnom. Najbitniji cilj je ostvarivanje normalnog odnosa između ove dve zone, tako da jedna ne naškodi drugoj.

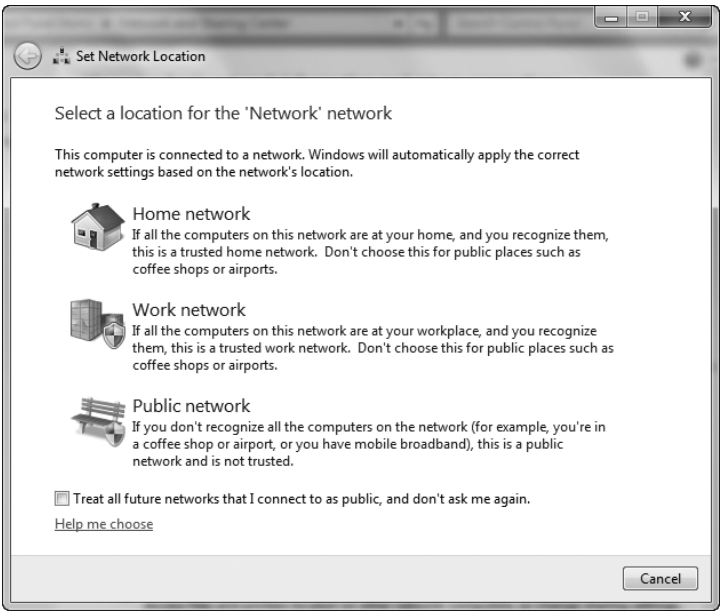
Najčešće, zaštitni zid se brine da sa globalne mreže, Interneta, na računar ne dospe štetan kôd (virus, crv itd.). Zaštitni zid sprečava viruse da dospeju na računar, ali ih ne leči, to jest ne uklanja.

Zaštitni zid ne može raditi sam, i najčešće zahteva iskusnijeg korisnika koji će odobravati ili zabranjivati pristup nekoj mrežnoj aktivnosti. Zaštitni zid je najosnovnija komponenta koja čini sigurnu računarsku mrežu, i uslov je normalnog rada – kako na Internetu, tako i na lokalnoj mreži.

Mnogi noviji anti-malvare programi imaju ugrađen zaštitni zid. Windows takođe sadrži zaštitni zid **Windows Firewall** (**Start ➪ Control Panel ➪ Windows Firewall**) i **Windows Defender** (**Start ➪ Control Panel ➪ Windows Defender**), namenjen blokiranju špijunskih programa. Sledeća ilustracija pokazuje kako funkcioniše zaštitni zid. Kao što zid od cigle može da predstavlja fizičku prepreku, zaštitni zid je prepreka između Interneta i računara.

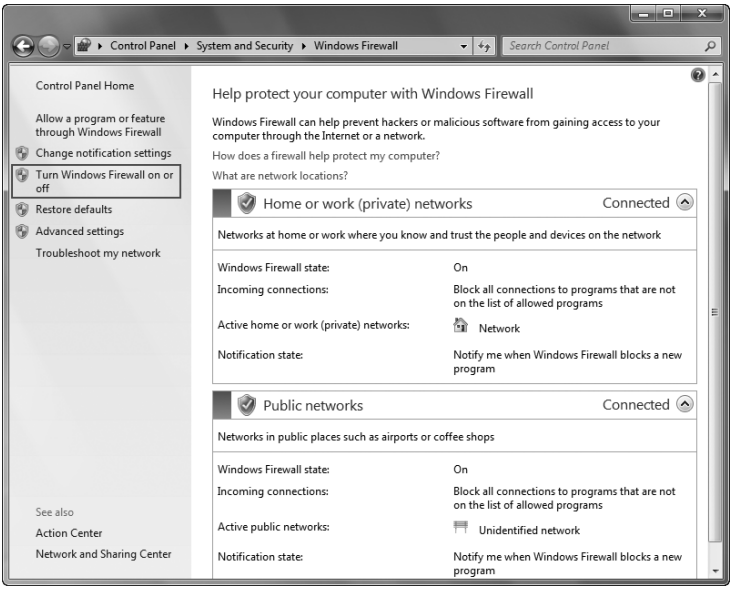
Windows Firewall može doprineti zaštiti računara od hakera i zlonamernog softvera. U operativnom sistemu Windows 7 on je i dalje moćan – ali je fleksibilniji i lakše se koristi. Na primer, sada možete precizno podesiti željenu zaštitu i obaveštenja za svaki mrežni profil – **Home network** (Kućna mreža), **Work network** (Poslovna mreža) i **Public network** (Javna mreža). Kada ste povezani s javnom mrežom, kao što je biblioteka ili kafić, možete da blokirate sve dolazne veze. Kod kuće ili na poslu, to bi moglo biti preterano.

Bez obzira na to koji nivo zaštite odaberete za profile, moći ćete lako da se prebacujete s jednog profila na drugi (sledeća slika).

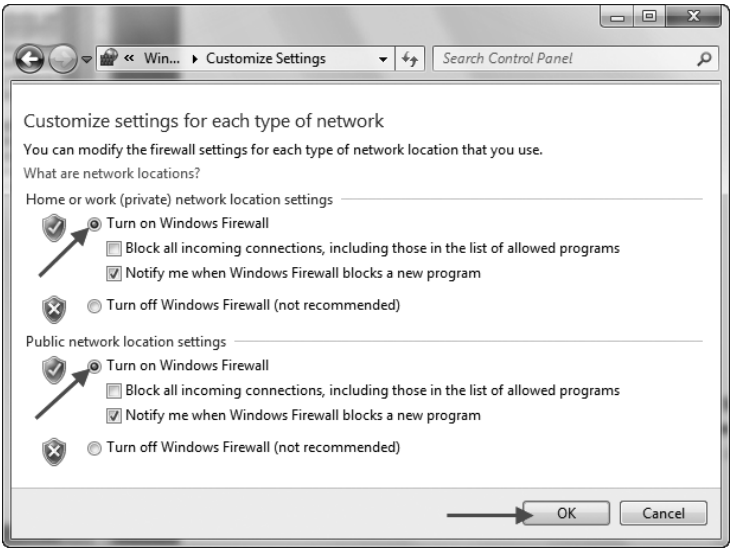


U Windowsu 7, zaštitni zid je podrazumevano uključen. Kako biste se uverili da on nije isključen, sledite ove korake:

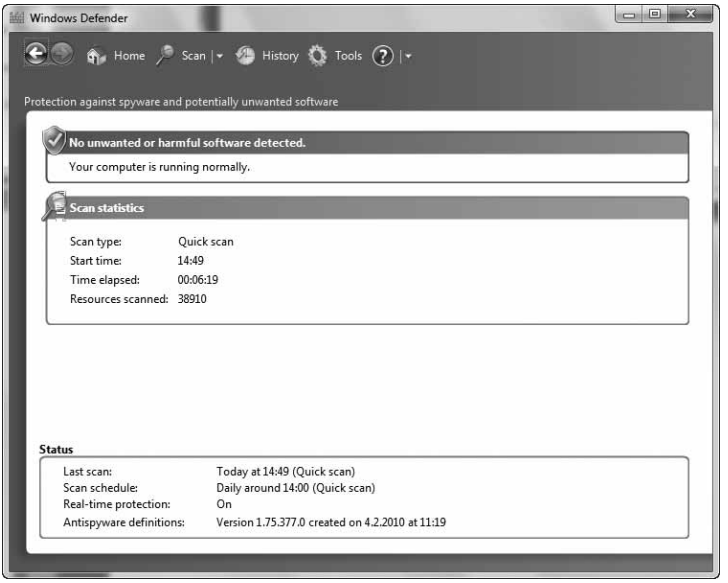
1. Otvorite Windowsov zaštitni zid tako što ćete pritisnuti **Start ➪ Control Panel ➪ Windows Firewall**.
2. U levom oknu izaberite stavku **Turn Windows Firewall on or off** (Uključi ili isključi Windowsov zaštitni zid).



3. Otvoriće se nov okvir za dijalog **Customize Settings**. Ispod svakog tipa mrežne lokacije izaberite stavku **Turn on Windows Firewall** (Uključi Windowsov zaštitni zid), pa pritisnite dugme **OK**. Preporučujemo da zaštitni zid uključite za sve tipove mrežnih lokacija.



Windows Defender (Windowsov zaštitnik) predstavlja prvu liniju odbrane od špijunskog i drugog neželjenog softvera. U operativnom sistemu Windows 7, ta funkcija ima jednostavnija obaveštenja, više opcija skeniranja i manji uticaj na performanse računara.



Windows Defender je antišpijunski program koji je sastavni deo Windowsa i pokreće se automatski kada je uključen. Upotreba antišpijunskog programa može da pomogne u zaštiti računara od špijunskog softvera i ostalog potencijalno opasnog softvera. Špijunski softver može da se instalira na računaru bez vašeg znanja kad god se povežete sa Internetom i može da zarazi računar kada instalirate neke programe koristeći CD, DVD ili druge prenosive medijume. Špijunski softver se takođe može programirati da se pokreće u neočekivano vreme, a ne samo kada se instalira.

Windows Defender na dva načina sprečava da špijunski softver zarazi računar:

- *Zaštita u realnom vremenu*.Windows Defender vas upozorava kada špijunski softver pokuša da se instalira ili pokrene na računaru. Takođe vas upozorava kada programi pokušaju da promene važne postavke operativnog sistema Windows.
- *Opcije skeniranja*. Windows Defender možete koristiti da biste skenirali sistem u potrazi za špijunskim softverom koji je možda instaliran na računaru, planirali redovna skeniranja i automatski uklonili sve što se otkrije tokom skeniranja.

Kada koristite ovaj program, važno je da imate ažurne definicije. Definicije su datoteke koje se ponašaju kao enciklopedije potencijalnih softverskih pretnji, koje se stalno povećavaju. Windows Defender koristi definicije da bi vas upozorio na potencijalne rizike ako utvrdi da je otkriveni softver špijunski ili drugi potencijalno neželjeni softver.

Da bi definicije bile ažurne, Windows Defender funkcioniše sa uslugom **Windows Update** i automatski instalira nove definicije po njihovom objavljivanju. Windows Defender možete podesiti i tako da pre skeniranja proveri ima li ažurnih definicija na mreži.

1.2.7 Mreže treba da budu zaštićene korisničkim imenima i lozinkama

Računarska mreža je grupa računara međusobno povezanih elektronskim kolima ili bežično, uz primenu različitih konstrukcija i tehnologija, a u cilju razmene podataka između njih ili njihovih korisnika. Mreže se mogu klasifikovati prema svojim karakteristikama:

- *Lokalna mreža* (**Local Area Network, LAN**). Najčešće povezuje računare u jednoj kancelariji, zgradi ili grupi susednih zgrada. Računari u lokalnoj mreži mogu deliti istu vezu sa Internetom. Postoje ožičene i bežične lokalne mreže. U ožičenoj mreži, svaki računar je kablom povezan s centralnim razvodnikom (**Hub**), dok se u bežičnoj mreži umesto žica upotrebljavaju radio-signali, a centralni razvodnik se zove pristupna tačka (**Access Point**).
- *Mreža širokog područja* (**Wide Area Network, WAN**). U velikim kompanijama koriste se računarske mreže koje povezuju delove kompanije smeštene na različitim lokacijama, pa čak i u različitim državama. Takve regionalne mreže zovu se mreže širokog područja.

  U stvarnosti, mnoge mreže su veće od lokalnih, ali manje od mreža širokog područja. Iz nekog razloga, još niko nije smislio ime za njih.

Primenom Internet tehnologija na lokalne mreže (**LAN**) ili mreže širokog područja (**WAN**) nastao je tzv. *intranet*. Radi se o grupi usluga koje su dostupne samo unutar preduzeća/organizacije, na njenoj internoj mreži, gde Web serveri šalju Web strane samo osoblju unutar organizacije, kad ih neko zatraži. Intranet je neka vrsta privatnog Weba.

U svim ovim slučajevima, pristup računarskim mrežama može biti dozvoljen samo zaposlenima u tim organizacijama. Iz bezbednosnih razloga, mreže moraju da budu zaštićene, pa im možete pristupiti samo uz upotrebu korisničkog imena i lozinke koje vam dodeljuje administrator sistema (gde on postoji). Ako mrežu koristite u manjoj firmi ili porodično, svaki pojedinac mora takođe da ima svoje korisničko ime i lozinku.

1.2.8 Identifikovanje rizika pri radu na mreži: nenamerno otkrivanje ličnih podataka, maltretiranje ili uznemiravanje, napadi uljeza

Da biste bezbedno koristili Internet, morate znati pravila. Prvo pravilo je da na Internetu nikada ne otkrivate svoj identitet. Za predstavljanje upotrebljavajte samo ime, a ne i prezime, adresu, telefonski broj. I nikome nikad nemojte otkriti svoju lozinku. Niko pošten to od vas neće ni tražiti.

Podaci o nama nalaze se u mnogim bazama podataka: u bankama, osiguravajućim kompanijama, obrazovnim institucijama, a poslodavci i državni organi barataju datotekama punim ličnih podataka.

Naši datumi rođenja, adrese, bračno stanje, prihodi, istorije korišćenja kredita, obrazovanje, istorije bolesti i drugi podaci, poznati su raznim institucijama. Ponekad su podaci opšteg tipa, a ponekad su specifični. Mogu biti poverljivi i, ako dospeju u pogrešne ruke, štetni ili opasni.

Marketinška odeljenja velikih kompanija rado plaćaju velike svote za baze podataka sa imenima i adresama određenih kategorija ljudi. To im omogućava da svoje proizvode i usluge ponude ciljnoj grupi ljudi.

Zbog toga su prikupljanje, održavanje i zaštita podataka poslovi koje nikako ne treba shvatiti olako. Održavanje nečijih ličnih podataka zahteva osećaj odgovornosti i poštovanja. Tu obavezu odražavaju zakoni o zaštiti podataka.

I pored svih predostrožnosti u vezi sa zaštitom ličnih podataka, dolazi do njihovog nenamernog otkrivanja, pa morate biti svesni tog rizika koji uvek postoji.

U vezi s tim postavlja se pitanje da li je bezbedno koristiti kreditne kartice preko mreže. Mišljenja su veoma podeljena, ali je poznato da je bilo dosta slučajeva otkrivanja podataka s tih kartica i njihove zloupotrebe. Stoga mnoge banke izdaju posebne kartice za plaćanje preko Interneta na koje se samo pred plaćanje prebacuje manji iznos, dovoljan da obavite odgovarajuću transakciju; nakon tog plaćanja, stanje na tom računu je blizu nule, pa ste zaštićeni od mogućih zloupotreba.

Drugi mogući rizik vezan za aktivnosti na mreži jeste zlostavljanje ili uznemiravanje koje obuhvata upotrebu informaciono-komunikacionih tehnologija kao što su e-pošta, trenutne poruke, neprimerene lične Web lokacije, blogovi, Web lokacije na kojima se organizuju glasanja čiji je cilj da povrede druge.

„Pecanje" (**Phishing**) na mreži predstavlja način prevare korisnika računara u cilju otkrivanja ličnih ili finansijskih podataka preko e-poruke ili Web lokacije. Uobičajena prevara pecanjem na mreži počinje e-poštom koja izgleda kao zvanično obaveštenje iz pouzdanog izvora, kao što je banka, preduzeće koje se bavi kreditnim karticama ili ugledni prodavac na mreži. Primaoce e-poruka upućuje na lažnu Web lokaciju gde se od njih zahteva da unesu lične podatke, kao što su broj računa ili lozinka. Te informacije se nakon toga obično koriste za krađu identiteta.

Šta da radite ako mislite da ste uneli lične ili finansijske podatke na Web lokaciju za pecanje?

Moglo bi biti od pomoći da odmah uradite sledeće:

- Promenite lozinke i PIN kodove na svim računima na mreži.
- Postavite upozorenje o prevari na kreditne izveštaje. Posavetujte se s bankom ako niste sigurni kako to treba da uradite.
- Direktno kontaktirajte banku ili prodavca na mreži. Nemojte slediti vezu koja se nalazi u lažnoj e-poruci.
- Ako shvatite da je nekim računima pristupljeno ili da su otvoreni prevarom, odmah ih zatvorite.

1.2.9 Identifikovanje mogućnosti roditeljskog nadzora: nadgledanje, ograničavanje pristupa Web sadržaju, ograničavanje korišćenja računarskih igara, ograničavanje vremena korišćenja računara

Da bi ograničili ili kontrolisali ono što njihova deca gledaju na Webu, roditelji treba da preduzmu sledeće akcije:

- Objasne deci kako ne bi trebalo da razgovaju s nepoznatima, da nije neobično da ljudi na mreži lažu o svojim godinama, da nikada ne saopštavaju svoje pravo ime, broj telefona ili adresu.
- Investiraju u programe koji blokiraju pristup Web lokacijama namenjenim samo za odrasle. Kada se ti programi instaliraju na računar, sprečavaju decu da pristupe neprikladnim Web lokacijama. Ti programi se nazivaju blokirajući softver (**Blocking Software**) ili Internet filtri (**Internet Filters**).

I najveći pobornici blokiranja neprikladnih Web lokacija slažu se da je prvi korak uspostavljanje saradnje s decom. Ona moraju shvatiti kako da se zabave i obrazuju na Webu, ali da ne upadnu u nevolje. Evo nekoliko akcija koje roditelji treba samostalno da preduzmu:

- Postavite računar u prostoriju u kojoj cela porodica najčešće boravi. Neka Internet postane porodična aktivnost. Prijateljski razgovarajte s decom o onome što oni rade na Internetu.
- Zamolite decu da vas malo provedu kroz Internet, da vam pokažu kuda idu kada su na mreži. Istinski se zainteresujte ko su im mrežni prijatelji. Pokušajte da saznate ko su te nove, nepoznate ličnosti.
- Proverite telefonski račun (ako koristite telefonsku vezu za pristup Internetu). Ukoliko je veoma i neuobičajeno visok, zatražite od telefonske kompanije spisak pozivanih brojeva; obratite pažnju na brojeva koji ukazuju na takozvane „vruće“ linije.
- Recite deci da vam obavezno kažu ukoliko im neko pošalje poruku punu mržnje i/ili nasilja, poruku seksualne ili sugestivne prirode ili nešto što im jednostavno ne odgovara.
- Ograničite deci vreme koje mogu da provode na mreži, i ukupno vreme korišćenja računara.

Kada dođe vreme da sa svojom decom porazgovarate o pitanjima koja se tiču Interneta, učinite to na prijateljski način, ne upuštajući se u sukobe i – ako je to moguće – pre nego što se desi incident koji će učiniti razgovor neophodnim. Pokušajte da prvo saznate šta vaša deca misle i ustanovite koliko su svesni potencijalnih opasnosti, pa tek onda kažite svoje mišljenje.

Ograničite deci računarske igre – kako vrste igara, tako i vreme provedeno u igranju. Potrudite se da učestvujete u izboru igara koje će biti instalirane na računaru ili do kojih će deca doći preko Interneta.