



Sigurnost računala

Dan sigurnog Interneta – sigurnije
na Internetu

Pripremio: Petar Pervan

Uvod

- Brigu o sigurnosti ne možete ukloniti, no možete ju učiniti manje neugodnom i nepoznatom.
- Dok su ranije najveće opasnosti bile koncentrirane u tehničkim propustima softvera koji koristimo, danas su najveća opasnost korisnici kao meta napada.
- Svjedoci smo različitih pokušaja online prijave u različitim oblicima.
- **Vaše znanje i kritičko promišljanje osnova je obrane sigurnosti!**

Zašto postoji opasnost?

- Naše računalo, kada je spojeno na Internet, dostupno je svim drugim računalima spojenima na Internet, unatoč tome komunicirali mi s njima ili ne!
- Zaraženo računalo vrlo vjerojatno sudjeluje u koordiniranoj mreži zaraženih računala!

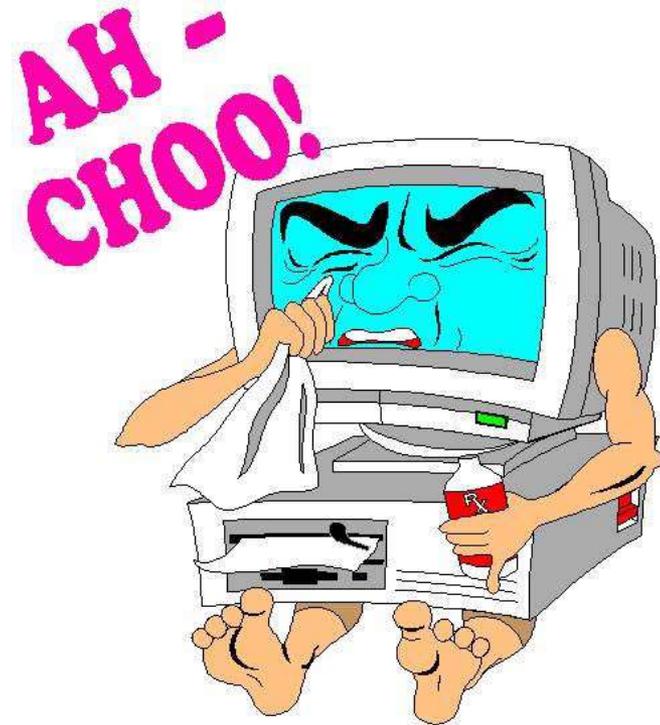


Zlonamjerni softver

- Programi s ugrađenim zlonamjernim kodom mogu dolaziti u različitim oblicima i obavljati različite manje ili više štetne radnje:
 - Virusi
 - Crvi
 - Trojanski konji
- Ostale opasnosti:
 - Lažne poruke (eng. Hoax)
 - Neželjene poruke (eng. Spam)
 - Lažno predstavljanje

Zlonamjerni softver

- Zlonamjerni softver se može sam ugraditi u naše računalo.
- To se obično događa kroz sigurnosne rupe u operacijskom sustavu ili programima koje koristimo.
- Izmanipulirani korisnik nesvjesno može i sam instalirati i aktivirati zlonamjerne programe.

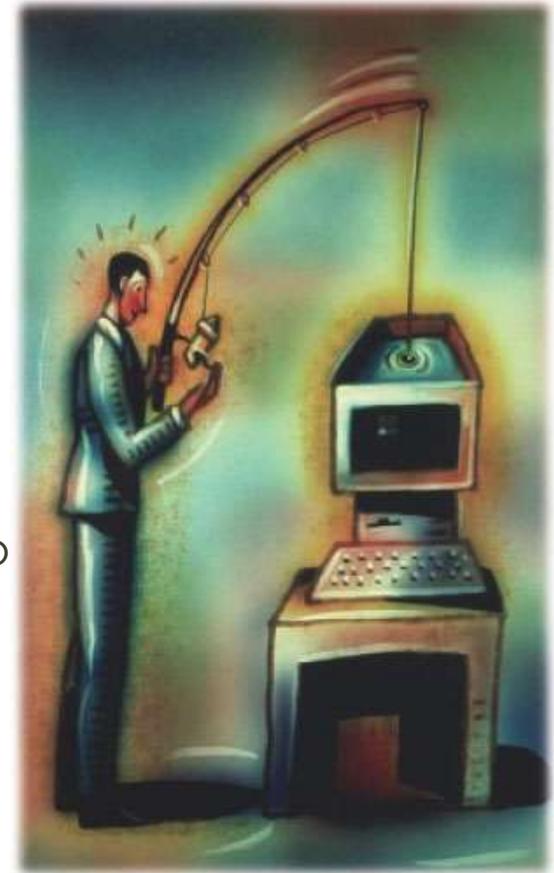


Socijalni inženjering

- Manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator sam ne može doći.
- Manipulator korisnika prijevarom navuče na otkrivanje povjerljivih informacija ili da za njega obavi neku radnju (najčešće nedopuštenu).

Phishing

- Pojam phishing (od eng. fishing – pećanje) je način na koji se od nas prikupljaju podatci o našem identitetu – služi u svrhu krađe online identiteta.
- Veliki broj osoba se zasipa porukama u kojima ih se nastoji nagovoriti da osobne podatke upisuju u različite formulare na nekoj web stranici, nadajući da će se netko „upecati“.
- Obično se oni koji od nas traže podatke lažno predstavljaju, npr. kao naša banka, a često puta stranice na koje nas navode u porukama izgledaju slično stranicama onih u čije se ime predstavljaju, kako bi se što lakše privuklo naivne korisnike.

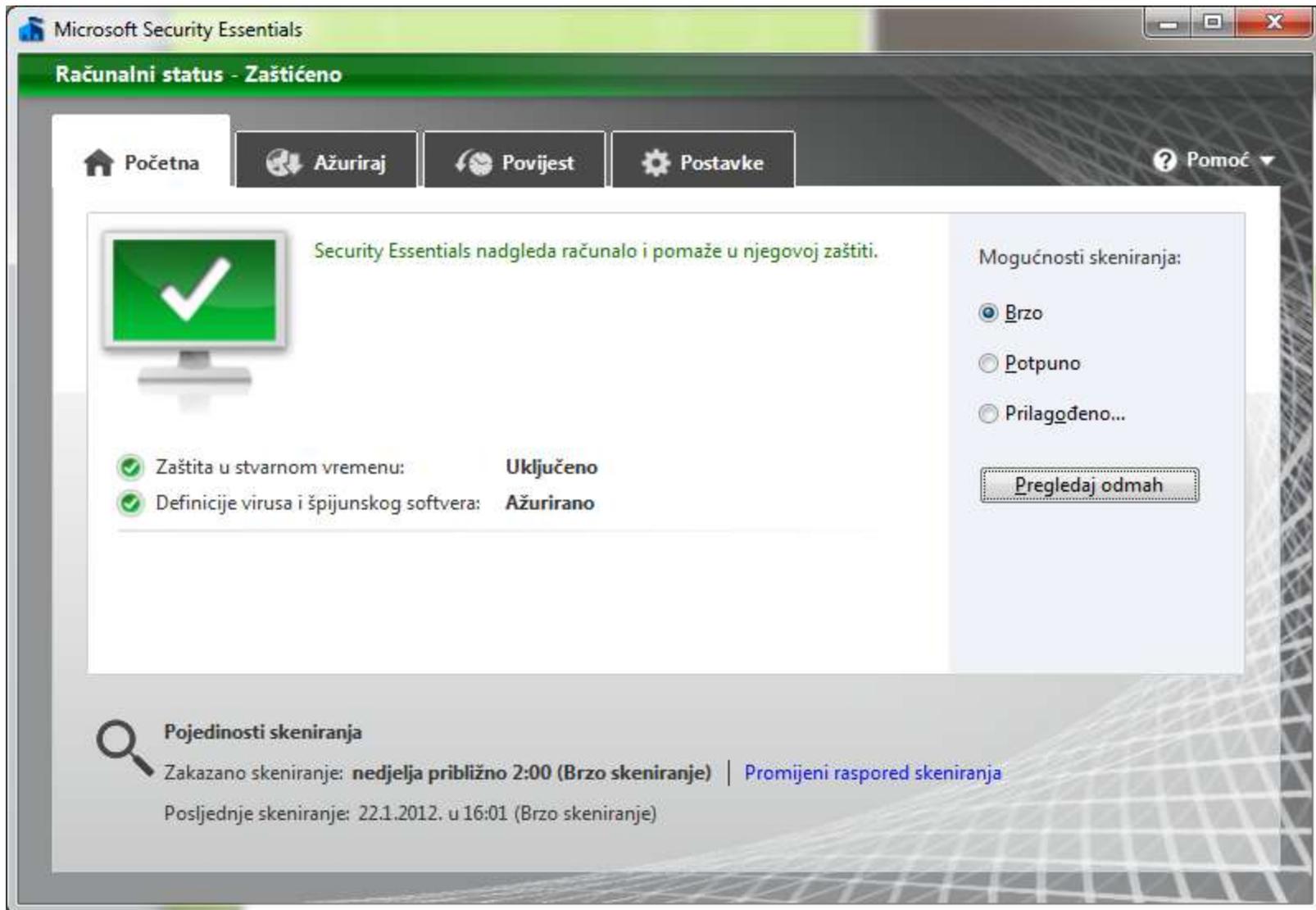


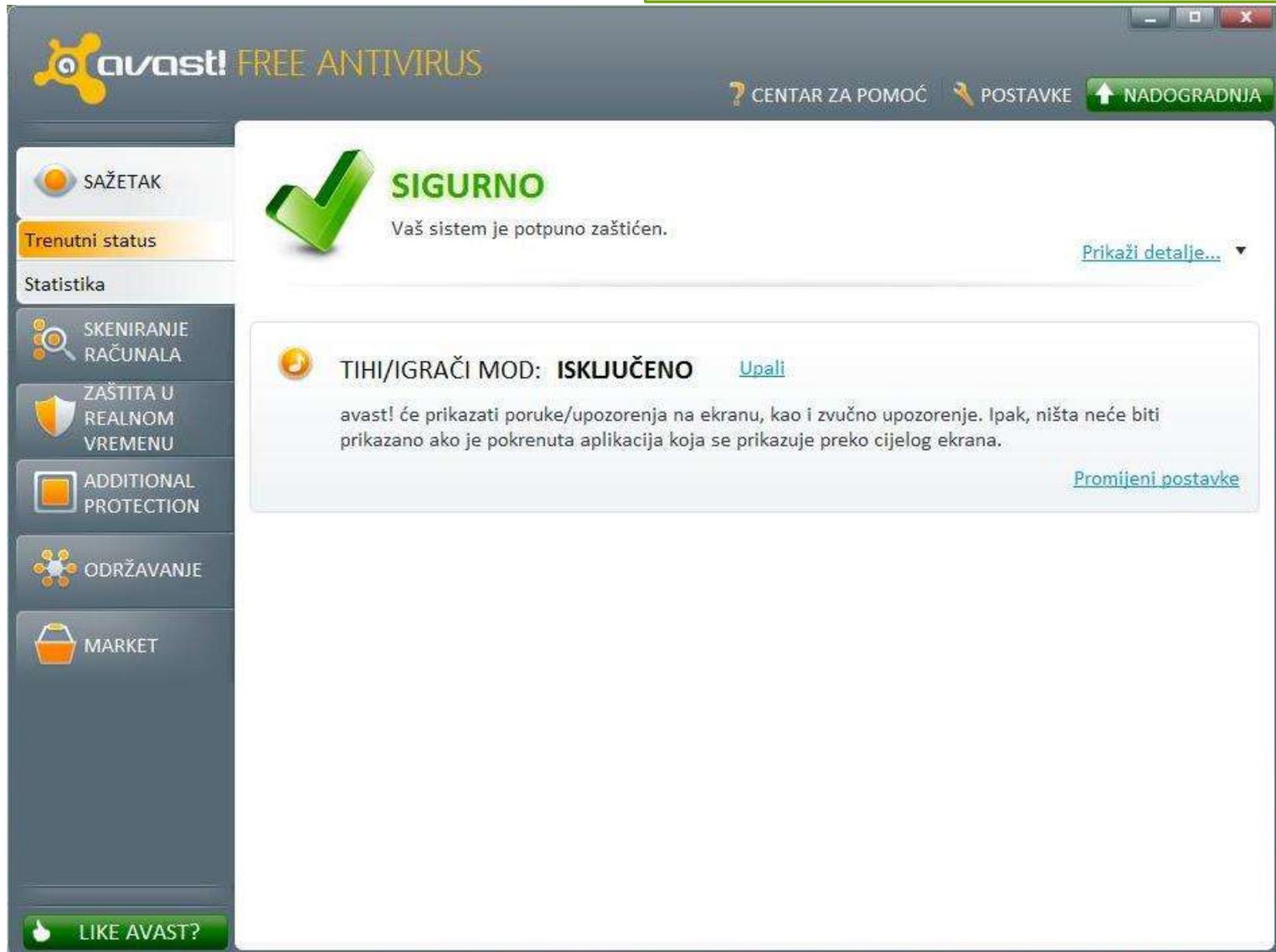
Kako se zaštititi?

- Iako se do računala ponekad može doći i bez odobrenja, većinom su naše odluke prva i posljednja crta obrane. Svijest o informacijskoj sigurnosti najbolji je sigurnosni alat.
- Potrebno je računalo zaštititi odgovarajućim sigurnosnim softverom te ispravnim postavkama operacijskog sustava i programa.
- Postoji mnoštvo besplatnih rješenja.

Antivirus/antispyware/antimalware

- Rješenja za prepoznavanje i zaustavljanje zlonamjernih programa. Obvezno je imati antivirus na računalu.
- Većina antivirusa štiti i od ostalih štetnih programa (crvi, trojanci,...)
- Preporuke besplatnih programa:
 - Microsoft Security Essentials*
 - * besplatan uz aktivirane (legalne) Windows operacijske sustave
 - Avast Antivirus





avast! FREE ANTIVIRUS

CENTAR ZA POMOĆ POSTAVKE NADOGRADNJA

SAŽETAK

Trenutni status

Statistika

SKENIRANJE RAČUNALA

ZAŠTITA U REALNOM VREMENU

ADDITIONAL PROTECTION

ODRŽAVANJE

MARKET

LIKE AVAST?

SIGURNO
Vaš sistem je potpuno zaštićen. [Prikaži detalje...](#)

TIHI/IGRAČI MOD: ISKLJUČENO [Upali](#)

avast! će prikazati poruke/upozorenja na ekranu, kao i zvučno upozorenje. Ipak, ništa neće biti prikazano ako je pokrenuta aplikacija koja se prikazuje preko cijelog ekrana. [Promijeni postavke](#)

Pozor – lažni antivirus!

- Postoji još jedan način obmane, a to su lažni antivirusni programi.
- Slično kao što se putem e-maila može dobiti lažna poruka, tako nam se na računalo može instalirati i lažni program koji se:
 - pretvara da je antivirusni program
 - pokazuje nam da naše računalo ima virusa (lažno)
 - navodi nas na upute za čišćenje virusa
- Upute za čišćenje virusa često budu poveznice za aktivaciju stvarnog virusa ili se traži uplata određenog iznosa novca kako bi se dobila puna verzija programa koja može očistiti virus.

Antivirus 2010 software

Antivirus 2010 Security Centre

PC is threatened! [Trial Licence, You need check your PC!] [Fix now!](#)

Please, click to scan your computer



My Protection

Protection of your computer



Scan my Computer

Files and computer scan



Update Center

Downloading updates (65%).



My Settings

Protection preferences

My protection status

Antivirus program protects your computer against malicious programs and unauthorized access and provides security access to the network



 Protected private data
Documents, presentations, logins and passwords, any personal info, and more

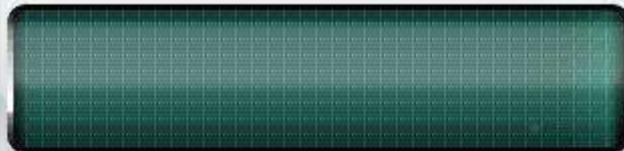


 Protected programs and applications
Protects system files and applications installed on your PC



 Protected online activity
Protects web sites, banking and online shopping, email and instant messaging

Total objects scanned: 368



Threats detected	0
Viruses:	0
Trojans:	0
Malware:	0
Adware/Spyware:	0
Other threats:	0

| License key: No license key

The screenshot displays the Security Tool application interface. The main window has a sidebar with navigation options: System Scan, Protection, Privacy, Update, and Settings. The 'System Scan' window is active, showing a table of detected threats. A red alert dialog box is overlaid on the scan results, indicating a critical infection.

System Scan Results:

Type	File Name	Name	Details
Backdoor	netevent.dll	Backdoor.win32,S...	This Trojan makes it possible for a r...
Backdoor	oleaccrc.dll	Backdoor.Win32,S...	This Trojan program makes it possibl...
Malware	panmap.dll	Virus.DOS.Vole.487	These are very dangerous nonmem...
Worm	rundll32.exe	Worm.Win32.Doo...	This worm spreads via the Internet,...

Security Alert Dialog:

Security Tool

mspaint.exe is infected with Virus.DOS.Glew.4245. This worm is trying to send your credit card details using mspaint.exe to connect to remote host.

Ok

Path: Scanning is finished. Cleanup required.

Infections: **36**

Save Report Remove

Get Full protection with Security Tool

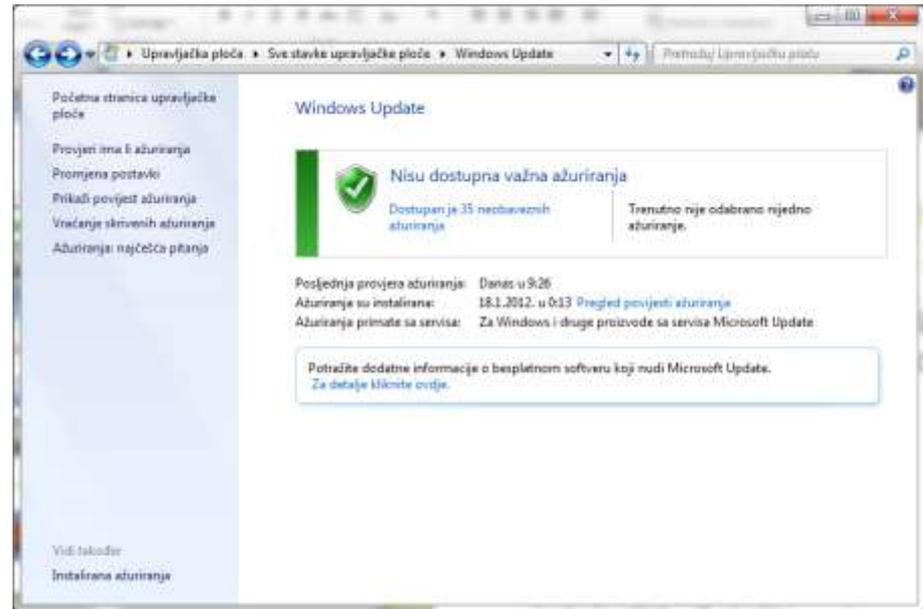
Vatrozid (eng. Firewall)

- Ograničava mrežnu komunikaciju između računala i Interneta.
- Selektivno propušta promet i na taj način se izbjegava neovlaštena komunikacija.
- Dio operacijskog sustava Windows (od XP s uključenim Service Pack 2) i dio mrežne infrastrukture (implementiran u usmjernicima)
- Alternativni vatrozidi:
 - ZoneAlarm
 - Comodo



Automatsko ažuriranje operacijskog sustava

- Sigurnosni propusti u softveru se stalno otkrivaju.
- Poželjno je uključiti automatsko ažuriranje u operacijskom sustavu kako bi se redovito instalirale „zavrpe“ za poznate propuste.



Windows Update u upravljačkoj ploči (eng. Control Panel)

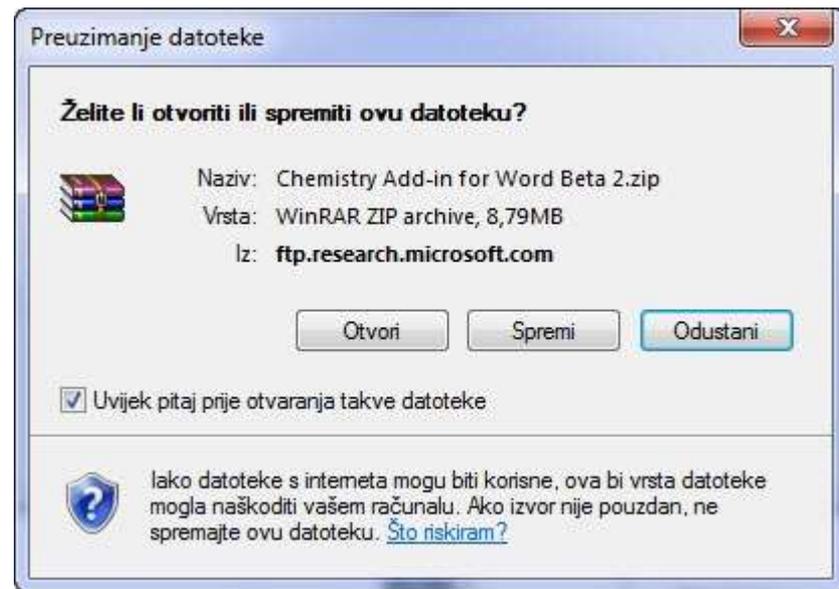
Automatsko ažuriranje programa

- Programi koji često dolaze u doticaj s dokumentima preuzetih s Interneta (primjerice pdf čitači ili MS Office programi) trebaju biti ažurni kako bi se spriječilo širenje štetnih programa preko njih.



Pazite na sadržaje koje preuzimate

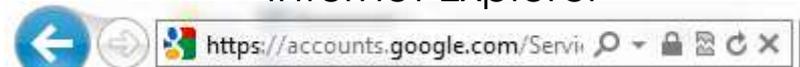
- Internet preglednik će nas uvijek upozoriti ukoliko odlučimo nešto preuzimati ili izvršiti.
- Na taj način imamo nadzor nad preuzimanjem sadržaja i aktiviranjem dodataka u pregledniku.



Koristite sigurni protokol

- Prijenos preko web stranica odvija se putem http i https protokola.
- Https protokol je zaštićeni protokol, i ukoliko na neku stranicu unosimo osobne podatke, protokol mora biti https.
- Koristi li stranica https protokol možemo vidjeti u adresnoj traci preglednika, po slici lokota i po promijenjenoj boji

Internet Explorer



Google Chrome



Mozilla Firefox



Radite pričuivne kopije

- Ukoliko računalo koristite za bilo što ozbiljnije od igranja i pregledavanja sadržaja na Internetu, važno je podatke koji su nam na računalu povremeno spremiti i na druga mjesta.
- Možemo raditi kopije podataka, ili slike cijelog sustava skupa s podacima.
- Važno je da medij na koji pohranjujemo pričuivne kopije (eng. Backup) nije dio našeg računala, već neka vanjska memorija koja je odvojena od samog računala.



Zaštita na društvenim mrežama - Facebook

- Korisnici društvenih mreža često nisu svjesni koje i kakve informacije objavljuju i tko ih sve može vidjeti, a samim time i zlouporabiti.
- Jako je bitno voditi računa o tome koje informacije zaista želimo podijeliti, i s kime.



Moguće zlouporabe

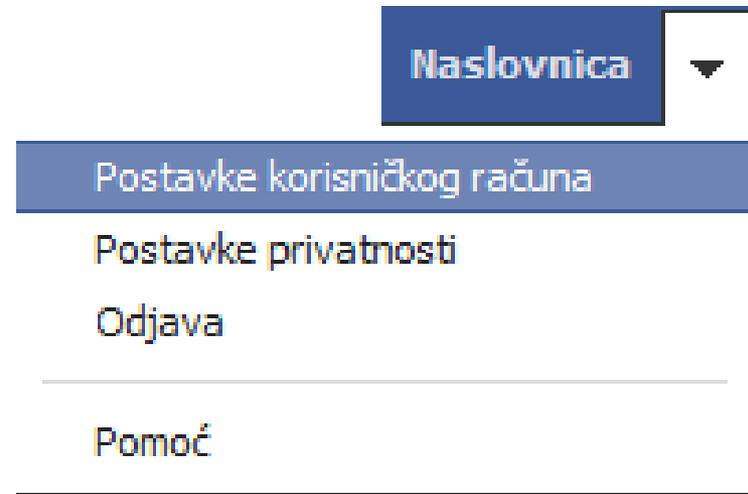
- Uzrokovanje štete ugledu osobe
- Zastrašivanje (tzv. cyber-bullying)
- Ucjenjivanje
- Prepoznavanje pomoću lica
- Krađa potpomognuta informacijama prikupljenim s mreže
- Krađa identiteta
- Lažno predstavljanje
- Uhođenje

Obratite pozornost:

- Kontaktne informacije i informacije o našoj trenutnoj lokaciji mogu se zlouporabiti.
- Pazite koga dodajete za prijatelja.
- Kad nešto postavljate na nečiji „zid” ili „timeline”, to odgovara njegovim/njezinim postavkama privatnosti, a ne našim!
- Aplikacije (igre, kvizovi i slično) na facebooku koriste naše informacije i često ih prosljeđuju drugima.

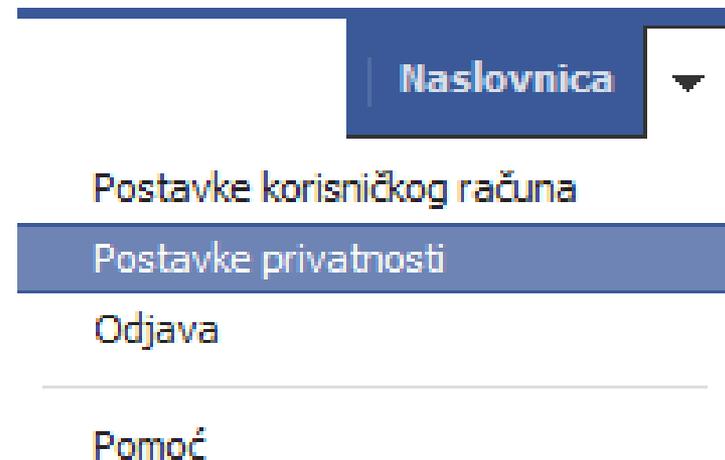
Postavke korisničkog računa

- Poželjno uključiti sigurno pretraživanje – https.
- Poželjno isključiti dijeljenje sadržaja za potrebe oglašavanja.



Postavke privatnosti

- Preporučuje se da glavna postavka vidljivosti bude „Prijatelji” (Friends).
- Ograničiti vidljivost lokacije.
- Ograničiti mogućnosti objave sadržaja na „zidu” ili „vremenskoj crti”.



Izvori i preporuke za daljnje čitanje i edukaciju

- <http://www.carnet.hr/abuse/sigurnost>
- <http://www.cert.hr/>
- <http://sigurnost.tvz.hr/>