Smernice o orodjih za zaščito zasebnosti na internetu

Kaj lahko sami storimo za zasebnost na internetu?

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice dajejo uporabnikom konkretne napotke za zagotavljanje višje stopnje varnosti in zasebnosti na spletu. Obsegajo kratko predstavitev nekaterih najbolj dostopnih informacijskih orodij in aplikacij, ki uporabnikom omogočajo bolj anonimno raziskovanje spleta.
Ciljne javnosti:	Uporabniki spleta
Status:	Javno
Verzija:	1.0
Datum verzije:	15.12.2011
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, splet, zasebnost, nadzor, informacijska varnost, anonimnost, kriptiranje, brskalniki, dodatki za brskalnike, virtualna zasebna omrežja, protivirusna zaščita.

VSEBINA

O smernicah Informacijskega pooblaščenca

Namen smernic IP je podati skupne praktične napotke za posameznike, katerih osebni podatki (OP) se obdelujejo ter za upravljavce in obdelovalce osebnih podatkov. Smernice naj bi na jasen, razumljiv in uporaben način odgovorile na najpogosteje zastavljena vprašanja na posameznem tematskem področju varstva osebnih podatkov. S pomočjo smernic želi Pooblaščenec doseči boljše poznavanje in spoštovanje informacijske zasebnosti ter določb Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- *Mnenja Pooblaščenca*:
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/

- *Brošure Pooblaščenca*:
  http://www.ip-rs.si/publikacije/prirocniki/

- *Smernice Pooblaščenca so objavljene na spletni strani:*
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

1. Namesto uvoda: Zakaj varovati svojo informacijsko zasebnost?

Posameznik je čedalje bolj vpet v obsežno digitalno omrežje, ki ga ne sestavljajo več le v internet povezani računalniki, pač pa tudi prenosni telefoni in druge digitalne naprave. V trendu vsesplošne digitalizacije in vse cenejše RFID (radijsko frekvenčne) tehnologije se v nekakšen „internet stvari“ povezujejo tudi čisto vsakdanji predmeti. Tako se pred našimi očmi riše podoba novega sveta, kjer nič več ne bo zunaj digitalnega omrežja.

Čeprav takšno vsesplošno **povezovanje prinaša številne koristi**, ni odveč poudariti, da **se hkrati pojavljajo tudi številne nevarnosti, ki ogrožajo posameznikovo zasebnost. Vse tiste zasebne informacije, ki jih s pomočjo elektronskih naprav in povezav** (računalnika, elektronske pošte, prenosnih telefonov) **delimo s svojimi bližnjimi, v resnici niso tako zelo zaupne in zavarovane pred nepoklicanimi očmi, kot to pogosto** (in žal tudi naivno) **upamo.**

Ne gre le za to, da je informacije, ki se pretakajo prek digitalnih omrežij, mogoče zakonito ali nezakonito prestrezati. Ne, **najbolj nevarno je** pravzaprav recimo temu **„normalno delovanje“ spleta in drugih digitalnih omrežij**, in sicer zato, **ker nas po eni strani zapelje v lažen občutek varnosti in anonimnosti, po drugi strani pa zato, ker je funkcija samodejnega nadzora že vgrajena v zakonite storitve** (spletne strani, trgovine, iskalnike), **ki jih internet nudi.**

Ob tem pomisleku marsikdo preprosto (še vedno) **skomigne z rameni, češ, ničesar nimam skrivati. Pa je res tako? Kaj pa naša zasebna elektronska pošta? Si želimo, da bi se z vsebino intimnih pisem seznanile tudi tretje osebe? Kaj pa telefonski pogovori z zaupniki? In naše na videz varno spravljene informacije na trdih diskih računalnikov? Nam je res vseeno, kdo vse ve, katere spletne strani, kdaj in kje si jih ogledujemo?**

Če se nam ob vseh teh pomislekih še vedno zdi, da nimamo ničesar skrivati, je tu še vedno zelo realna nevarnost, da nas spletni nepridipravi oberejo za težko prigaran denar. **Vsakdo, ki kupuje prek spleta ali uporablja storitve spletnega bančništva, tvega, da ga bodo zaradi brezbrižnosti, nepazljivosti ali lahkovernosti goljufi nekoč opetnajstili.** Že zgolj ta finančni razlog zadostuje (ali bi vsaj moral zadostovati), da tehtno **razmislimo o varovanju svoje informacijske zasebnosti** – še posebej, ker je takšna varnost pogosto lahko kar brezplačna. Naj poudarimo, da naš namen ni odvračanje od interneta in internetnih trgovin, naš namen je, da vas opozarjamo, kako tehnologije, ki so nam na razpolago, varno uporabljati.

Če ne želimo biti izključeni iz informacijske družbe, smo žal pogosto primorani uporabljati različne storitve in naprave, ko moramo skorajda slepo zaupati v pošteno in zakonito ravnanje cele verige podjetij, od proizvajalcev naprav, prek ponudnikov komunikacijskih poti, do ponudnikov storitev. Ne glede na navedeno, pa lahko **za svojo zasebnost marsikaj postorimo tudi sami. Namen pričujočih smernic je ravno ta – prikazati nekaj uporabnih orodij, s katerimi lahko skrb za svojo zasebnost vzamemo v svoje roke. Osveščeni in tehnično podkovani uporabniki sodobnih tehnologij jih že poznajo, zakaj jih ne bi tudi vi? Večina teh orodij je namreč povsem preprostih za uporabo.**

2. Na kratko o nevarnostih, ki prežijo na našo informacijsko zasebnost

Z množico podatkov, ki so bolj ali manj varno shranjeni (tako vsaj upamo!) na trdih diskih, pametnih karticah, DVD-jih, USB ključkih in drugih podatkovnih medijih, pa se s podatki, ki se pretakajo med pošiljanjem elektronske pošte, brskanjem po spletu in kramljanjem po telefonu, v resnici lahko zgodi marsikaj neprijetnega. Zaradi napak v strojni in komunikacijski opremi se podatki lahko popačijo ali celo izbrišejo. Podobno se lahko zgodi v primeru, če je posredi zlonameren posameznik, le da takrat obstaja precejšnja možnost, da se podatki ne le uničijo ali poškodujejo, ampak da se z njimi seznani nekdo drug. Posledice so večinoma odvisne od vrednosti takšnih informacij. Če gre za zlorabo digitalnih potrdil in gesel za uporabo e-bančništva, pa je škoda lahko tudi zelo oprijemljiva.

Na naše bolj ali manj dragocene podatke torej prežijo številne nevarnosti. Med širšo javnostjo so zaradi medijske odmevnosti najbolj znane tiste, ki so povezane z **vdori v informacijske sisteme in s spletnimi goljufijami**. Pri tem gre za kazniva dejanja, ki jih **zlonamerni posamezniki** (hekerji oziroma bolj točno, krekerji, pa tudi goljufi) izvajajo z namenom uresničevanja različnih ciljev: zaradi finančne koristi, potrjevanja pred vrstniki, maščevanja, preizkušanja svojih sposobnosti, idr.

Zlonamerni posamezniki svoje napade izvajajo tako, da iščejo ranljivosti v našem informacijskem sistemu ali celo v nas samih. V tem drugem primeru gre za izkoriščanje zaupanja in naivnosti, takšen napad pa je bolj znan kot socialni inženiring1. Proti tej nevarnosti se je mogoče boriti tako, da sistematično vzdržujemo neko „zdravo“ mero nezaupanja in občutljivih informacij (zlasti gesel) ne posredujemo neznancem. **Proti napadom na informacijski sistem, ki potekajo z izkoriščanjem ranljivosti v aplikacijah in operacijskem sistemu, pa se borimo predvsem tako, da operacijski sistem redno posodabljamo z varnostnimi popravki, da uporabljamo požarni zid in dobro protivirusno zaščito, ki jo moramo prav tako redno posodobljati. Poleg tega je zelo koristna metoda varovanja podatkov šifriranje (enkripcija)** podatkovnih medijev, posebej trdih diskov in USB ključkov, ki pride najbolj do izraza takrat, ko računalnik ali USB ključek izgubimo ali nam ga ukradejo. Če je podatkovni medij kriptiran z močnim algoritmom in zavarovan s kompleksnim geslom, smo lahko dokaj brez skrbi, saj je možnost, da se nepridipravi dokopljejo do naših podatkov, majhna. V nasprotnem primeru, torej če podatkov ne kriptiramo, pa se hitro lahko zgodi, da se bo srečni najditelj z njimi seznanil in jih v najslabšem primeru izkoristil nam v škodo.

Poleg teh najbolj očitnih nevarnosti na uporabnike spleta in drugih omrežij prežijo številne druge manj opazne nevarnosti. **Ko obiščemo spletno stran, ta stran oziroma tisti, ki z njo upravlja, pridobi od našega računalnika ali prenosnega telefona podatke o tem, katero spletno stran smo obiskali prej, kakšen jezik uporabljamo, IP naslov in s tem tudi približno geografsko lokacijo, kjer se trenutno nahajamo, pa operacijski sistem, resolucijo zaslonske slike** in še kaj. **Poleg tega številne spletne strani uporabljajo t.i. piškotke, to je programske paketke, ki se med brskanjem po spletu namestijo na naš računalnik in sledijo naši dejavnosti na internetu – katere spletne strani smo obiskali, kaj smo iskali, kaj kupili, kaj nas zanima ali ne zanima, s kom se družimo na facebooku in drugih spletnih socialnih omrežjih**, idr. Takšni piškotki torej sledijo našemu spletnemu življenju na takšni ravni, da si jo pravzaprav kar težko predstavljamo! Na srečo pa se je takšnemu samodejnemu in v splet vgrajenemu nadzoru mogoče v veliki meri izogniti z nekaterimi prijemi, kot na primer z uporabo ustreznih nastavitev v spletnem brskalniku, s povezovanjem v virtualna zasebna omrežja in seveda z razvijanjem pametnih navad.

3. Prvi varnostni obroč: Posodabljanje operacijskega sistema, požarni zidovi in protivirusna zaščita

3.1 Posodabljanje operacijskega sistema

Zlonamerni programi (virusi, črvi, druga škodljiva programska koda) iščejo varnostne luknje v operacijskih sistemih, saj jim te, če jih odkrijejo, pogosto omogočajo, da prevzamejo nadzor nad našim računalnikom ali mobilnim telefonom. Zato je **zelo pomembno, da je naš operacijski sistem vedno posodobljen z najnovejšimi varnostnimi popravki, ki odpravljajo kritične ranljivosti oziroma „krpajo varnostne luknje“.** Takšen varnostni ukrep sicer ni popolni, je pa vsekakor prvi in najmanj zapleten korak pri zagotavljanju višje stopnje varnosti in s tem tudi informacijske zasebnosti.

Kratka navodila za nastavitev samodejne posodobitve operacijskega sistema Windows XP, Windows Vista in Windows 7 (navodila so povzeta iz spletne strani http://support.microsoft.com):

Windows XP:
1. Kliknite Start, Zaženi, vnesite sysdm.cpl in nato pritisnite ENTER.
2. Kliknite zavihek Automatic Updates in izberite eno od teh možnosti. Priporočamo vam, da izberete možnost Automatic (recommended) Automatically download recommended updates for my computer and install them (Samodejno (priporočeno) Samodejno prenesi in namesti priporočene posodobitve za moj računalnik)
3. Kliknite V redu.

Windows Vista in Windows 7
1. Kliknite Start, v iskalno polje vnesite Windows Update, nato pa na seznamu Programi kliknite Windows Update.
2. V levem podoknu kliknite Spremeni nastavitve.
3. Izberite želeno možnost.
V razdelku Priporočene posodobitve potrdite polje Želim priporočene posodobitve, tako kot prejemam pomembne posodobitve ali Pri prenašanju ali nameščanju posodobitev ali obveščanju o njih vključi priporočene posodobitve in kliknite V redu.

Operacijski sistemi, ki temeljijo na jedru Linux, uporabljajo različne načine za (samodejno) posodobitev. Na tem mestu so povzeta zgolj kratka navodila za posodobitev priljubljene ***Linux distribucije Ubuntu*** *(različica 11.10 z grafičnim vmesnikom Unity).*
1. Kliknite Dom pregledne plošče.
2. V iskalnik vtipkajte Upravljalnik posodobitev in kliknite na ikono, ki se prikaže.
3. V oknu, ki se odpre, najprej kliknite preveri, nato pa namesti posodobitve.
4. Če vas sistem vpraša za vnos administratorskega gesla, ga vnesete, in posodobitev se izvrši.

Alternativna možnost nameščanja sistemskih posodobitev je vnos ukaza v terminal:
1. sudo apt-get update
2. sudo apt-get upgrade
Kratka navodila za posodobitev operacijskega sistema Mac OS X (povzeto po: http://support.apple.com)
1. Kliknite na ikono jabolka in izberite posodobitve programske opreme.
2. Kliknite namesti, nato vnesite administratorsko uporabniško ime in geslo.

3.2 Požarni zidovi

Komunikacija z računalniki ali mobilnimi telefoni, ko so enkrat povezani na internet, je praviloma dvosmerna. Komunikacija po eni strani omogoča uporabniku, da prek svoje elektronske naprave dostopa do podatkov, ki so shranjeni na oddaljenih strežnikih, kamor sodi tudi branje elektronske pošte in brskanje po spletnih straneh. Vendar **to** po drugi strani **pomeni, da lahko v določenih okoliščinah tudi drugi (zlonamerni) posamezniki dostopajo do podatkov, ki so shranjeni na našem računalniku ali prenosnem telefonu.** Ker si praviloma (izjema je oddaljena tehnična podpora) takšnega nepooblaščenega stikanja po naših dragocenih podatkih, s tem pa tudi poseganja v informacijsko zasebnost ne želimo, je **pomembno, da imamo operacijski sistem na računalniku ali prenosnem telefonu zaščiten s t.i. požarnim zidom**. Če si naš računalnik predstavljamo kot srednjeveško mesto, potem je požarni zid obzidje z mestnimi vrati in stražo, ki odloča, kdo (kateri paket podatkov) lahko gre v mesto ali iz njega, kdo pa ne. V osnovi gre za nekakšno filtriranje povezav po vnaprej postavljenih pravilih, kar bistveno otežuje nepooblaščen dostop do našega računalnika, večinoma pa otežuje tudi morebitnim zlonamernim programom, ki so že nameščeni na našem sistemu, da bi se povezali na neke oddaljene lokacije.

Operacijski sistemi Windows XP, Windows Vista in Windows 7 imajo nameščene svoje požarne zidove, zato pogosto ni potrebe po iskanju alternativ ali nadgradnji. Pomembno je le, da se prepričamo ali so ti požarni zidovi tudi vklopljeni, in jih, če niso, vklopimo.

Kratka navodila za vklop požarnega zidu v operacijskem sistemu Windows XP, Windows Vista in Windows 7 *(navodila so povzeta iz spletne strani http://support.microsoft.com):*
1. Kliknite Start (v levem spodnjem kotu zaslona), nato kliknite Nadzorna plošča, zatem Varnost in končno še Požarni zid programa Windows.
2. Kliknite Vklop ali Izklop požarnega zidu programa Windows. Če računalnik od vas zahteva skrbniško geslo ali potrditev, vnesite geslo ali izvedite potrditev.
Kliknite Vklopi (priporočeno) in nato kliknite V redu.

Kratka navodila za vklop požarnega zidu v operacijskem sistemu Ubuntu Linux*:*
1. S pomočjo programa Upravljalnik paketov (Synaptic packet manager) ali z ukazom v terminalu namestite grafični vmesnik Gufw za že nameščen požarni zid Ufw.
2. Kliknite na ikono Nastavitev požarnega zidu (najdete jo s pomočjo iskalnika)
3. Nato kliknite na ikono ključavnice, vnesite administratorsko geslo in končno kliknite še na zavihek vključeno.

Kratka navodila za vklop požarnega zidu v operacijskem sistemu Mac X OS*:*
1. Kliknite na ikono jabolka, nato kliknite na sistemske nastavitve.
2. Izberete pogled, nato kliknete na varnost&zasebnost.
3. Kliknite na zavihek požarni zid, in nato na vklopi.

Lahko namestite tudi kakšen drug požarni zid. Nekateri alternativni požarni zidovi omogočajo bolj učinkovit, pa tudi naprednejši sistem nadzora nad povezavami med našim računalnikom in omrežjem, spet tretji omogočajo celo nadzor nad sumljivimi notranjimi procesi, ki tečejo na računalniku. Vendar pa za običajnega uporabnika osnovni požarni zidovi (npr. tisti, ki je že vgrajen v novejše različice operacijskega sistema Windows) zadostujejo.
Ob tem si velja zapomniti, da praviloma namestimo in uporabljamo le en požarni zid. Hkratna uporaba dveh ali več požarnih zidov pogosto privede do kopice težav, najpogostejša je upočasnjeno delovanje celotnega sistema, v zameno pa ne ponudijo bistveno višje stopnje varnosti.

Spodaj je navedenih nekaj bolj znanih in učinkovitih požarnih zidov, ki so popolnoma brezplačni. Namestitev je praviloma zelo enostavna, iz spletne strani prenesete datoteko (večinoma s končnico .exe), nanjo dvakrat kliknete in sledite navodilom.

ZoneAlarm Free Firewall
http://www.zonealarm.com
Sunbelt Personal Firewall
http://www.sunbeltsoftware.com
Comodo Firewall
http://www.comodo.com
Online Armor Free
http://www.online-armor.com

3.3 Protivirusna zaščita

Škodljiva programska koda - sem sodijo virusi, trojanski konji, vohunski programi, črvi, idr., predstavlja eno najbolj pogostih nevarnosti, ki prežijo na običajnega uporabnika. Škodljiva programska koda lahko povzroči škodo na naši programski (v nekaterih primeri celo strojni!) opremi ali/in na shranjenih podatkih. V nekaterih primerih pa napadalcu celo omogoči, da prevzame nadzor nad našim računalnikom, prenosnim telefonom ali drugo v omrežje povezano elektronsko napravo. Še posebej so nevarni t.i. trojanski konji, ki se (kakor pove že ime) pod krinko običajnega programa ali datoteke namestijo na računalnik in napadalcu omogočijo, da prevzame nadzor. S tem nič hudega sluteči uporabnik v enem zamahu izgubi nadzor nad svojo elektronsko napravo in nad podatki, ki so shranjeni v njej.

Te vrste nevarnosti je možno zelo zmanjšati z uporabo protivirusne zaščite. Na trgu je veliko protivirusnih programov, nekateri so plačljivi, drugi brezplačni. **Ko uspešno namestimo protivirusni program, je zelo pomembno, da ga redno posodabljamo**. Škodljiva programska koda se hitro razvija, zato zastarela protivirusna zaščita ni več dovolj učinkovita – z rednim posodabljanjem pa zagotovimo, da smo v koraku s časom in se tako izognemo nevarnostim, ki prežijo na nas. Prav tako je zelo **pomembno, da celoten sistem** (računalnik, tablico, prenosni telefon) r**edno pregledujemo s protivirusnim programom.** To je dobro storiti enkrat tedensko, vsekakor pa vsaj enkrat mesečno.

Tako kot za požarne zidove tudi v tem primeru velja, da je en kakovosten in redno posodobljen program boljša izbira kot sočasna uporaba različnih protivirusnih programov. Takšna hkratna uporaba zelo pogosto privede do opazne upočasnitve celotnega sistema. Izjemo predstavljajo specializirani protivirusni programi, ki jih je prav tako priporočljivo namestiti kot dopolnilo klasični protivirusni zaščiti.

Nekateri kakovostni brezplačni protivirusni programi:
Avira AntiVir Personal Edition *(http://www.freeav.com/en/products/1/avira_antivir_personal__free_antivirus.html)*
Microsoft Security Essentials
(http://www.microsoft.com/Security_Essentials/)
Avast! Free Antivirus
(http://www.avast.com/en-au/free-antivirus-download)

Dodatna brezplačna programa za odstranjevanje vohunske kode, ki predstavljata koristno dopolnilo osnovni protivirusni zaščiti.
SuperAntiSpyware
(http://www.superantispyware.com/)
Malwarebytes Anti-Malware Free
(http://www.malwarebytes.org/)

Pri operacijskih sistemih, ki temeljijo na jedru ***Linux,*** *je izbira protivirusne zaščite bistveno manjša, saj je tudi nevarnost okužbe z virusi bistveno manjša. Najbolj znan brezplačen protivirusni program je* ***ClamAV*** *http://www.clamav.net).*

Različico istega protivirusnega programa, ki se imenuje ***ClamXav****, brezplačno namestite na operacijske sisteme* ***Mac X OS*** *(http://www.clamxav.com/).*

Opozorilo!: Škodljiva programska koda se včasih zamaskira v protivirusne programe. Zato je potrebno biti pri nameščanju teh previden, kar v praksi pomeni, da se je dobro izogibati neznanim znamkam, prav tako pa je protivirusne (in druge) programe dobro nalagati le iz zaupanja vrednih spletnih strani (to so pogosto kar uradne spletne strani proizvajalcev posameznih programov).

4. Drugi varnostni obroč: Kriptiranje podatkov in anonimno sprehajanje po spletu

Podatki, ki jih imamo shranjene na trdih diskih v računalnikih, na spominskih karticah v prenosnih telefonih, na USB ključkih, DVD-jih in drugih medijih, so največkrat v nešifrirani obliki. To pomeni, da se lahko zlonamerni ali zgolj radovedni posameznik brez težav seznani z njihovo vsebino, ko jih enkrat dobi v roke. Zelo priporočljiv varnostni ukrep, ki v veliki meri ščiti tudi našo informacijsko zasebnost, je šifriranje (kriptiranje) podatkov. S širiranjem zagotovimo, da nepooblaščene osebe ne bodo znale prebrati naših zaupnih sporočil ali podatkov. Kriptiramo lahko že shranjene podatke, torej vse tisto, kar je shranjeno na našem računalniku, pametnem telefonu ali USB ključku. Prav tako pa lahko kriptiramo tudi podatke, ki se prek komunikacijskega kanala prenašajo iz ene lokacije na drugo, tako kot npr. elektronska pošta.

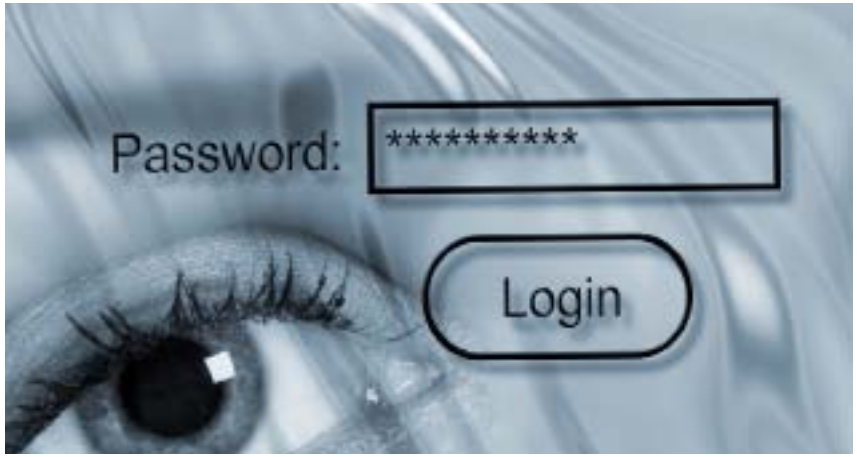
Čeprav je kriptiranje v svojem bistvu precej zapleten matematičen proces, je uporaba aplikacij za enkripcijo podatkov zelo enostavna. Preprosto poiščemo ustrezen program za kriptiranje, ga namestimo na naš računalnik ali pameten telefon, sledimo navodilom, izberemo nekaj pomembnih parametrov (šifrirni algoritem, podatke, ki jih želimo kriptirati), geslo (naj bo čim bolje izbrano: glej priporočila za izbiro gesel!), in počakamo, da program kriptira podatke.

Pogosto se dogaja, da posameznik izgubi prenosnik, mobilni telefon, USB ključek ali pa mu ga ukradejo. Če podatki niso kriptirani, se lahko kdorkoli brez večjih težav seznani z njihovo vsebino. In če gre pri tem za občutljive osebne podatke ali celo tajne podatke, lahko zelo hitro nastane medijski škandal, če ne celo kaj hujšega. S kriptiranjem po drugi strani to nevarnost odpravimo oziroma bistveno zmanjšamo. Kriptirani podatki so namreč brez poznavanja ustreznega gesla nekoristni, saj ne predstavljajo za človeka berljivih informacij (tako kot nekriptirani podatki), pač pa le naključno zaporedje alfanumeričnih znakov. **Če izgubite ali vam ukradejo računalnik, kjer so podatki kriptirani, je skrb odveč – izgubili ste nekaj sto evrov vredno opremo, toda po drugi strani se vsaj s podatki najverjetneje nihče ne bo mogel seznaniti.**

Kriptiramo lahko celoten disk ali drug podatkovni medij, lahko pa to storimo le s posamezno datoteko. Kriptiranje celotnega diska je bolj zanesljivo, saj so na ta način zavarovani vsi podatki, ki so shranjeni na disku. V tem primeru je vsekakor potrebno redno delanje varnostne kopije pomembnih podatkov. S tem se zavarujemo v primeru, če pozabimo kriptirno geslo ali če pride do okvare diska. Lahko pa kriptiramo zgolj posamezno datoteko, ki nam služi kot majhen trezor, kamor shranjujemo najbolj občutljive informacije.

Nekatere različice operacijskih sistemov imajo že vgrajen program za kriptiranje (v MS Windows se imenuje BitLocker, v Mac OS X pa FileVault). Sicer pa je zelo razširjena brezplačna alternativa TrueCrypt. Namestimo ga lahko na različne operacijske sisteme, omogoča kriptiranje celotnega diska in posameznih datotek.
Najdemo ga na spletni strani http://www.truecrypt.org/downloads. Ko enkrat pridobimo datoteko truecrypt.exe, dvakrat kliknemo nanjo, sledimo navodilom in dokončamo namestitev.

Priporočljivo je, da začetnik najprej ustvari le kriptirno datoteko, kamor bo shranjeval svoje pomembne podatke. Enkripcija celotnega diska je sicer preprosta, vendar je potrebno nekaj več previdnosti (zlasti velja prej narediti varnostno kopijo vseh pomembnih podatkov), saj si lahko v najslabšem primeru onemogočimo dostop do podatkov na disku. Še kratka navodila: http://www.truecrypt.org/docs/



10 priporočil za varna gesla

*1. **Gesla naj bodo dolga vsaj 6-7 znakov.***
*2. **Vsebujejo naj alfanumerične znake** (velike in male črke, simbole in številke).*
*3. **Gesel ne zapisujemo na listke!** Če se temu ne moremo izogniti, listkov nikakor ne hranimo v bližini računalnika (na monitorju, pod tipkovnico, pod telefonom, v lahko dosegljivih predalih ipd.)*
*4. **Gesla redno menjujemo.** Priporočljivo jih je menjati vsak mesec ali pa vsaj na vsake tri mesece.*
5. Ne uporabljamo starih gesel in ne kombiniramo preteklih gesel z dodatnim številkami (npr. janez1, janez2 itd.)
6. Ne uporabljamo zaporednih črk ali številk (npr. "abcdefg" ali "234567") in ne uporabljamo sosednjih tipk na tipkovnici (npr. "qwertz").
*7. **Ne uporabljamo besed, ki se nahajajo v slovarjih in ne uporabljamo gesel, ki jih je lahko uganiti ali njihovih običajnih kombinacij** (imen hišnih ljubljenčkov, partnerjev, otrok, avtov, registrskih številk, letnic in datumov rojstev ipd.).*
*8. **Dobro in varno geslo je takšno, ki ga vemo samo mi, obenem pa si ga je lahko zapomniti in ga ni potrebno nikjer zapisovati.***
9. Kako torej sestaviti varno geslo, ki pa si ga je tudi lahko zapomniti in mi ga ni potrebno zapisovati? Dobro in varno geslo lahko enostavno sestavimo tako, da si npr. izberemo priljubljeno pesem in uporabimo recimo prve črke posamezne besede. Če dodamo še nekaj številk, recimo našo težo, višino ali kaj podobnega, kar vemo bolj ali manj samo mi, dobimo geslo, ki si ga hitro zapomnimo, obenem pa je precej varno. Pri zamenjavi gesla enostavno uporabimo drugo pesem in drugo številko.
10. Še tako dobro sestavljeno geslo nam nič ne pomaga, če nasedemo na socialni inženiring. Gre za metodo, pri kateri se napadalec lažno izkazuje za npr. sodelavca iz IT oddelka ali nekega zunanjega vzdrževalnega servisa in od vas zahteva dostopna gesla zaradi nekih vzdrževalnih aktivnosti, ki jih mora opraviti. Vedno se najprej vprašajte, ali to res potrebuje in dvakrat preverite, ali je upravičen do teh podatkov. Raziskave potrjujejo, da več kot polovica običajnih uporabnikov računalnikov nasede na različne pristope socialnega inženiringa.

4.1 Anonimno brskanje po spletu

Čeprav internet prinaša številne prednosti, skriva v sebi tudi mnogo pasti. Nekatere pasti se dotikajo prav zasebnosti, ki je med sprehajanjem po spletu bistveno zmanjšana. **Običajni uporabniki spleta si pogosto ne predstavljajo, kako veliko podatkov puščajo za seboj. Temu pravimo t.i. elektronske sledi, ki nastanejo, ko obiščemo neko spletno stran, uporabimo določeno storitev, ali se zgolj povežemo v omrežje.** Med podatki, ki jih puščamo za seboj, je IP naslov računalnika, telefona ali druge omrežne naprave, pa tip operacijskega sistema, spletni brskalnik, resolucija zaslona, jezik operacijskega sistema in še kaj.

Med sprehajanjem po spletu upravljavci različnih spletnih strani na naš računalnik nameščajo majhne programske datoteke, ki se imenujejo piškotki in lastnikom spletnih strani omogočajo, da nam sledijo. Pri tem ne pridobivajo zgolj informacij o naši geografski lokaciji, pač pa tudi podatke o tem, kje se sprehajamo, kaj gledamo, kaj iščemo, kakšne navade imamo, kaj nas zanima, skratka, skušajo ugotoviti kdo in kaj smo.

Pozabiti pa ne smemo niti na nepridiprave, ki prežijo na nas in na naše podatke zato, da bi nam škodovali. Vse pogostejša je t.i. kraja identitete, ko neka tretja oseba pridobi o nas dovolj pomembnih podatkov, da se lahko tudi izdaja za nas. In če naredi kakšno neumnost ali celo kaznivo dejanje, bomo čisto lahko mi tisti, ki bomo padli v roke organom pregona. Tudi če bomo dokazali, da gre za drugo osebo, ki se izdaja za nas, nam bo to povzročilo kar nekaj preglavic in neprespanih noči.

Ob vseh teh nevarnosti se zdi razumno, da tudi sami poskrbimo za določeno mero digitalne zasebnosti. To lahko storimo vsaj na tri načine:

1) S prilagoditvijo brskalnika – ta je pogosto nastavljen tako, da omogoča sprejemanje piškotkov in različnih programskih skript, kar je z vidika uporabniške izkušnje lepo in prav, z vidika zagotavljanja zasebnosti pa škodljivo.

2) Z uporabo ustreznih programov – ti omogočajo preusmeritev internetnega prometa prek posredniških strežnikov (proxy serverjev) in na ta način zabrišejo izvor povezave, npr. naš IP naslov. Enako pomembno je kriptiranje vsebine povezave, kar v primeru morebitnega prestrezanja podatkov radovednežu onemogoči (ali vsaj bistveno oteži) seznanitev s samo vsebino komunikacije.

3) Z razvijanjem dobrih navad – vsa tehnologija nam ne bo pomagala veliko, če se bomo preveč lahkomiselno sprehajali po spletu. S preudarnim izbiranjem spletnih strani, filtriranjem piškotkov in selektivnim nameščanjem raznih dodatkov, še bolj pa s zadostno mero previdnosti pri razdajanju osebnih podatkov, lahko bistveno utrdimo svojo sfero zasebnosti, s tem pa tudi varnosti.

4.1.1 Prilagoditev spletnega brskalnika

Programi, ki jih uporabljamo za brskanje po spletu, se imenujejo spletni brskalniki (ang. web browsers). Med bolj znanimi so **Internet Explorer, Mozilla Firefox in Google Chrome**. Žal so brskalniki ob namestitvi na računalnik pogosto nastavljeni tako, da ne omogočajo najboljšega varovanja zasebnosti. Zato je priporočljivo pregledati nastavitve, saj lahko zgolj z nekaj preprostimi „kliki z miško“ sebi ali svojim bližnjim zagotovimo bistveno višjo stopnjo zasebnosti in varnosti med brskanjem po spletu.

Ker brskalniki (lahko) shranjujejo zgodovino našega brskanja, besede, ki smo jih vpisali v iskalnike (npr. v Google), pa tudi t.i. piškotke, je priporočljivo, da izberemo takšne nastavitve, ki bodo to onemogočile. Slaba stran je, da bodo zaradi tega lahko naše spletne izkušnje nekoliko bolj osiromašene.

Ob rob brskalnikom: Zakaj piškotki niso vedno okusni?

Seveda ne gre za čokoladne piškotke, pač pa za majhne datoteke, ki se imenujejo „piškotki“ (ang. cookies). Te med obiskom spletne strani strežnik pošlje našemu brskalniku, ta pa jih nato shrani na podatkovni medij (ponavadi kar na trdi disk) naše elektronske naprave (računalnika, pametnega telefona).

V piškotku je lahko zapisana identifikacijska številka uporabnika, geslo za dostop do internetne strani in drugi osebni podatki, ki jih puščamo na spletnih straneh. Kljub temu, da piškotki predstavljajo zelo koristno orodje na področju interaktivnih poslovnih spletnih aplikacij, pa njihova uporaba posega v našo varnost in zasebnost – skozi proces nadziranja, iskanja varnostnih pomanjkljivosti, razkritja in zbiranja podatkov.

Eno izmed orodij za nadzor nad piškotki je upravitelj piškotkov (ima ga vsak spletni brskalnik). Upravitelji piškotkov uporabniku omogočajo, da s pomočjo nastavitev določijo ravnanje s piškotki in tudi preprečijo njihovo. **S tem se zavarujemo pred potencialnimi grožnjami piškotkov,** a hkrati tudi omejimo funkcionalnost določenih spletnih strani. **Koristi tudi redno brisanje že nameščenih piškotkov**. Z upraviteljem piškotkov imamo torej večji nadzor nad piškotki in njihovo vsebino.

Upravitelj piškotkov omogoča:
- *pregled spletnih strani s piškotki,*
- *pregled časa trajanja posameznih piškotkov,*
- *pregled datotek elektronski piškotkov,*
- *onemogočanje elektronskih piškotkov,*
- *selektivno sprejemanje piškotkov,*
- *rutinsko brisanje piškotkov trdega diska.*

Za brisanje piškotkov v Internet Explorer upoštevajte naslednje korake:
1. Odprite brskalnik Internet Explorer
2. Izberite »Orodja« >, »Internetne možnosti« > in jeziček »Splošno«.
3. Pod »Začasne internetne datoteke kliknite »Brisanje piškotkov ...«
4. Ob sporočilu»Ali želite izbrisati vse piškotke v mapi za začasne internetne datoteke?« kliknite »V redu«.
5. Kliknite »V redu« za izhod.

Za brisanje piškotkov v brskalniku Mozilla Firefox upoštevajte naslednje korake:
6. Odprite brskalnik Mozilla Firefox.
7. Kliknite »Orodja« > »Možnosti« > »Zasebnost«.
8. Kliknite »Piškoti« > Odstrani vse piškote«.
9. Izberite »V redu« za izhod.

Za brisanje piškotkov v brskalniku Google Chrome upoštevajte naslednje korake:
1. Odprite brskalnik Google Chrome
2. V orodni vrstici brskalnika kliknite ikono ključa
3. Kliknite zavihek Napredne možnosti.
4. V razdelku »Zasebnost« kliknite Nastavitve vsebine.
5. V pogovornem oknu »Nastavitve vsebine« kliknite zavihek Piškotki
6. Kliknite Vsi piškotki in podatki mest, da odprete pogovorno okno »Piškotki in drugi podatki«.
7. Če želite izbrisati vse piškotke, kliknite Odstrani vse na dnu pogovornega okna.
8. Če želite izbrisati določen piškotek, izberite spletno mesto, ki ga je shranilo, nato piškotek in kliknite Odstrani.

Opozoriti je potrebno še na **t.i. super-piškotke** (Local Shared Objects oz. **Flash piškotki**). Nekatere spletne strani namesto običajnih spletnih piškotkov, katerih sprejemanje uporabnik lahko onemogoči v spletnem brskalniku, uporabljajo Flash piškotke, ki so po funkcionalnosti sicer precej podobni običajnim piškotkom (možnost shranjevanja različnih uporabniških nastavitev). A če uporabnik v brskalniku izbriše običajne piškotke, s tem ne izbriše tudi Flash piškotkov. Z njihovo pomočjo spletni strežnik identificira uporabnika in celo ugotovi, ali je ta uporabnik izbrisal običajne piškotke, nato pa lahko izbrisane piškotke "oživijo" oziroma ponovno pošljejo uporabniku.

Uporabniki Windows operacijskega sistema se lahko znebijo Flash piškotkov s pomočjo brezplačnega programa CCleaner (http://www.piriform.com/ccleaner), **uporabniki Firefoxa pa tudi z uporabo Firefox dodatka Better Privacy.**

Ob tem **velja omeniti, da se v Evropi pravkar spreminja pravni okvir za delovanje piškotkov**. Do sedaj so spletne strani in ponudniki storitev, ki uporabljajo piškotke, morali ponuditi uporabnikom interneta možnost, da se odjavijo od prejemanja piškotkov (opt-out). **Po novem** pa **bodo morali, predvsem za piškotke, ki sledijo uporabnikom preko različnih spletnih strani** (oglaševalski, analitični, ipd.), **pridobiti vnaprejšnjo privolitev uporabnikov – preden bo torej piškotek shranjen na vaš računalnik, boste morali v to privoliti.** Ponudniki bodo morali v svojih izjavah tudi natančno pojasniti, katere piškotke uporabljajo in za kakšen namen, tako da bodo uporabniki veliko bolje seznanjeni. V Sloveniji bo tak sistem implementiran v bližnji prihodnosti.

Do tedaj pa je koristno omeniti, da **že sedaj obstajajo določene platforme, na katerih uporabniki lahko označijo, s katerimi oglaševalskimi piškotki, ki jih nevede prejemajo na vsakem koraku, se ne strinjajo**. Te platforme so se razvile kot odziv na nevarnosti vedenjskega oglaševanja, ki temelji na sledenju uporabnika s piškotki. Odjava uporabnika od prejemanja takih piškotkov naj bi zmanjšala stopnjo nadzora, ki ga omogoča vedenjsko oglaševanje. **Odjavo od določenih oglaševalskih piškotkov je mogoče opraviti na naslednjih spletnih straneh http://selectout.org/, http://www.youronlinechoices.com/, http://www.networkadvertising.org/.** Pooblaščenec tu opozarja, da navedene spletne strani ne vsebujejo vseh upravljavcev piškotkov, temveč zgolj tiste, ki so člani platform – obstajajo torej še mnogi, od katerih se uporabnik s tem ne odjavi.

Okrepljena zasebnost: Nekaj koristnih dodatkov za brskalnike

Z namestitvijo nekaterih dodatkov (ang. plug-in) lahko bistveno povečamostopnjo zasebnosti, ki jo uživamo med sprehajanjem po spletu. Cena, ki jo v nekaterih primerih za to plačamo, je predvsem nekoliko osiromašena uporabniška izkušnja.

Upravljanje s piškotki

Better Privacy: Povrne kontrolo tudi nad superpiškotki (https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/)
CSLite: Nadzira katere strani vam piškotke smejo pošiljati in kaj se z njimi zgodi (http://download.cnet.com/CS-Lite/3000-2378_4-10719475.html)
No More Cookies: Omogoča nadziranje piškotkov (http://download.cnet.com/No-More-Cookies/3000-2144_4-10449885.html)

Blokiranje aktivnih skriptov

NoScript: Priljubljen dodatek, ki onemogoča samodejno zaganjanje JavaScript, Jave in Adobe Flasha (https://addons.mozilla.org/en-US/firefox/addon/noscript/)
AdBlock Plus: Blokiranje neželenih spletnih oglasov (https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/)
Ghostery: Odkriva in zapre t. i. nevidne elemente programske kode spletne strani, ki vohunijo za uporabniki (http://download.cnet.com/Ghostery/3000-11745_4-10974194.html)
FlashBlock: Blokira prikaz vsebin v Flashu (https://addons.mozilla.org/en-US/firefox/addon/flashblock/)

Ocenjevanje (ne)varnosti spletnih strani

WOT: Spletne strani so z uporabo tega dodatka rangirane glede na stopnjo varnosti. Seveda pa je klasifikacijo spletnih strani potrebno razumeti s pridržkom (https://addons.mozilla.org/en-US/firefox/addon/wot-safe-browsing-tool)
McAfee SiteAdvisor: Dodatek, ki pregleduje spletne strani, jih testira in analizira ter uporabniku sporoči, ali je spletna stran varna, delno varna ter predvsem ali nevarna (http://www.siteadvisor.com/download/windows.html)
LinkExtend: Prikazuje široko paleto informacij o spletnih mestih, ki jih obiščete. Ščiti vaš računalnik pred zlonamernimi programi in neprimernimi vsebinami (http://download.cnet.com/LinkExtend/3000-11745_4-10909733.html)

Uporaba varnih povezav

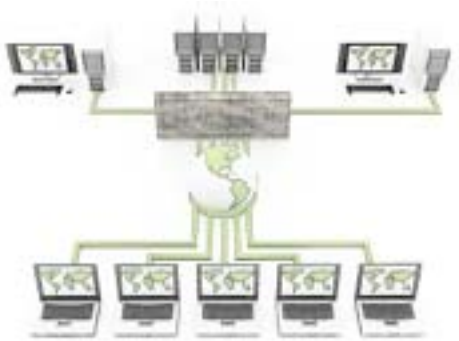
HTTPS Everywhere: Samodejna preusmeritev na uporabo varnega HTTPS protokola (šifrirana povezava) na spletnih straneh, ki to omogočajo. Sem sodijo Facebook, Google, Live (Hotmail), Microsoft, Mozilla, PayPal, Twitter, Wikipedia, idr. (http://download.cnet.com/HTTPS-Everywhere/3000-11745_4-75211397.html)
KB SSL Enforcer: Avtomatsko zaznava in preusmerja na uporabo protokola SSL, ki omogoča varno komunikacijo (http://code.google.com/p/kbsslenforcer/)
KeyScrambler Personal: Kriptira vse vnesene podatke preko tipkovnice (http://download.cnet.com/KeyScrambler-Personal/3000-2144_4-10571274.html)

Anonimen spletni iskalnik

Spletni iskalniki, kot so Google, Yahoo in drugi, pridno hranijo in analizirajo naše vnose. Ko smo neko besedo vnesli v iskalnik, ostane tam dolgo, in če nas lahko iskalnik identificira s pomočjo piškotkov, začne na podlagi naših vnosov izdelovati celoten profil uporabnika. Spletni iskalniki tako zgolj na podlagi našega brskanja po spletu kmalu ugotovijo kakšne so naše navade, naši vzorci, vedenje, želje, družbeni status, idr. **Temu se je do neke mere mogoče izogniti z uporabo t.i. anonimnih spletnih iskalnikov.**
Eden od najbolj zasebnosti prijaznih je Ixquick. Vsi dnevniški zapisi (o tem kaj smo iskali) se samodejno uničijo po 48 urah, razen tega pa ta iskalnik sploh nima piškotov, ki bi nas zasledovali med našim sprehodom prek speta.
Ixquick: https://www.ixquick.com/

Začasna elektronska pošta

Nekaj anonimnosti si lahko (poleg kriptiranja običajne elektronske pošte) **zagotovimo z uporabo začasnih poštnih predalov. Te odpremo brez vnosa osebnih podatkov, aktivirani pa so kratek čas, npr. 10 ur ali nekaj dni, potem se** (ponavadi) **samodejno uničijo**. Koristni so predvsem za prijavljanje na različne spletne strani ali storitve, ki zahtevajo vnos elektronskega poštnega naslova – svojega pravega pa iz takšnih ali drugačnih razlogov ne želimo posredovati.
Nekaj storitev „anonimne elektronske pošte“:
Anonymous E-mail: https://www.awxcnx.de/mm-anon-email.htm
Safe-mail: https://www.safe-mail.net/cgi-bin/Safe-mail.net/gate/
HushMail: https://www.hushmail.com/
10 Minute Mail: http://10minutemail.com/10MinuteMail/index.html



4.1.2 Virtualna zasebna omrežja (VPN) in uporaba posredniških strežnikov (Proxy)

VPN je angleška kratica, ki označuje t.i. »virtualno zasebno omrežje« (ang. Virtual private network). Gre za računalniško omrežje, ki logično (ne fizično) povezuje dva ali več računalnikov oziroma drugih omrežnih naprav. Uporablja se zlasti v poslovnem okolju, predvsem pri povezavi v splet. **VPN omogoča varno izmenjavo podatkov med omrežji, strežniki in uporabniki s pomočjo varnih omrežnih protokolov** (IPsec, TLS/SSL, SSH).

Posamezniki, ki ne uporabljajo VPN tehnologije, svoje podatke pošiljajo v nezaščiteni obliki in so zato bolj izpostavljeni različnih nevarnostnim, npr. prestrezanju podatkov. Pri uporabi VPN omrežji pa uporabniki najprej potrdijo svojo identiteto, šele nato se izvrši prenos podatkov, ki se prenesejo v kriptirani

obliki. Na ta način je zagotovljena višja stopnja varnosti in zasebnosti pri prenosu podatkov

Seznam brezplačnih VPN:

LogMeIn Hamachi
(https://secure.logmein.com/products/hamachi/)

2. **Wippien**
(http://www.wippien.com/)

3. **CyberGhost VPN**
(http://cyberghostvpn.com/en)

Posredniki (angl. proxy) so strežniki, ki nenehno preusmerjajo zahteve po posredovanju ali prejemanju podatkov tako, da zaobidejo oziroma kar zapletejo neposredno pot med prejemnikom in pošiljateljem podatkov. Zato podatki ne potujejo več od točke A (npr. od nekega strežnika) do točke B (našega računalnika) neposredno, pač pa prek cele mreže vmesnih točk C, D, E in tako naprej.

Najbolj razširjeno anonimno omrežje strežnikov, preko katerih lahko uporabniki koristijo internet, je omrežje Tor. Uporaba Tor omrežja poteka tako, da si uporabnik v računalnik namesti Tor klienta. Ko uporabnik želi npr. prebrati elektronsko pošto ali obiskati spletno stran, Tor klient najprej poizve, kateri Tor strežniki so na voljo v omrežju, nato pa naključno izbere enega od njih in se s šifrirano povezavo poveže nanj. Ta se poveže na naslednjega, in tako naprej, dokler se zadnji strežnik v omrežju končno ne poveže na spletno stran ali na poštni strežnik, do katerega je zahteval dostop uporabnik. **Podatki** pa **so šifrirani na tak način, da vsak strežnik v omrežju ve le, od katerega strežnika je podatke dobil in komu jih je posredoval, ne pozna pa izvora in cilja komunikacije.**

Zelo preprosta aplikacija, ki omogoča uporabo Tor posrednikov, je Vidalia:
https://www.torproject.org/projects/vidalia.

Iz spletne strani jo je mogoče prenesti kot samostojen paket, ki vsebuje tudi brskalnik Mozilla Firefox in navodila, v tej obliki pa jo je mogoče zagnati kar neposredno iz USB ključa, kar je koristno zlasti, če brskamo po spletu iz javnega računalnika (v knjižnicah, v cybercaffejih).

5. Za konec: Zdrava pamet in dobršna mera previdnosti

Internet prinaša številke koristi in priložnosti, hkrati s tem pa tudi varnostna tveganja. Številna od teh tveganj se dotikajo naše zasebnosti, ki na spletu postaja vse bolj ranljiva. Če se želimo v čim večji meri izogniti pastem interneta, hkrati pa še vedno uživati koristi, ki jih ta nudi, je nujno, da se seznanimo z nekaterimi orodji in ukrepi za zagotavljanje zasebnosti na spletu.

Čeprav se na prvi pogled zdi, da splet posamezniku, ki sedi na drugi strani računalniškega ekrana, nudi varno in zasebno izkušnjo, to žal ni tako. Na vsakem koraku nehote puščamo t.i. elektronske sledi, ki izdajajo našo prisotnost, še več, ki izdajajo tudi to, kaj nas zanima, kakšne so naše navade, želje, pričakovanja, kdo so naši prijatelji, itd. Tako pridobljene informacije različni subjekti uporabljajo za različne namene. Žal vse prepogosto naivno računamo na to, da bodo drugi varovali našo zasebnost, A največ zagotovo lahko storimo le sami. Prav to je tudi namen teh smernic – posameznike bolje seznaniti z nekaterimi orodji, s katerimi lahko tudi sami aktivno varujejo svojo zasebnost. Ne pozabite pa na najpomembnejše – zdravo kmečko pamet, predvsem pri objavah osebnih podatkov na spletu. Brez tega orodja vam tudi druga ne bodo pomagala:-).