BIC LJUBLJANA

GIMNAZIJA IN VETERINASKA ŠOLA

CESTA V MESTNI LOG 47

LJUBLJANA

SEMINARSKA NALOGA

MAJ 2009

***PROGRAMSKI VSILJIVCI***

Programski vsiljivci povzročajo veliko preglavic. Nekateri niso zelo škodljivi,drugi pa imajo kar resne posledice,če se znajdejo na računalniku. Nekateri programski vsiljivci imajo to funkcijo,da lahko dokumente,ki niso bili namenjeni širši javnosti pošiljajo drugim uporabnikom. Na ta način lahko utrpite kar veliko škodo,sploh,če gre pri teh dokumentih za kaj pomembnega.

## VIRUSI

Čeprav je lahko namen virusov,da uničujejo podatke,so pogosto samo nadležni. Večina virusov je usmerjena v lastno nekontrolirano reprodukcijo,kar troši računalniška sredstva,kot so procesorska moč,pomnilnik ali količina prostega trdega diska. Zgodovinsko gledano so se prvi računalniški virusi pojavili za velike računalnike,nakar so se pisci virusov,skupaj z večanjem dostopnosti osebnih računalnikov,osredotočili na osebne računalnike. Virusi so samo eden od različnih tipov programov,ki so narejeni z zlobnimi nameni. Računalniške črve,trojanske konje in ostale vrste zlobnih programov pogosto imenujemo virusi,kar pa lahko zmede uporabnike,saj do dandanes virusi veliko manj pogosti kot so bili včasih. Dandanes prevladujejo predvsem trojanski konji in črvi. Zaradi tega se uporabniki pogosto varujejo samo pred določenim tipom zlobnih računalniških aplikacij in so s tem bolj ranljivi za ostale. Pred virusi se bojujemo s pomočjo protivirusnih programov,požarnih zidov in pravočasnih popravkov programja. Danes ti programi niso več namenjeni samo boju proti virusom,ampak služijo tudi preprečevanju prisotnosti vohunskega programja. Računalniški virusi niso omejeni samo na osebne računalnike z okoljem Microsoft Windows. Obstajajo tudi za razne UNIX/Linux sisteme, operacijske sisteme, ki poganjajo vgradne naprave, kot so mobilni telefoni ali dlančniki.

## Varnost in osnovni pojmi

Z razvojem računalništva in informatike in s povezovanjem v internet je problem varnosti postal še bolj pomemben kot včasih. Kaj se je spremenilo?

* 1. Napadalci so bolj usposobljeni in izobraženi ter imajo boljša orodja
  2. Bolj smo odvisni od informacijskih tehnologij in več izgubimo kot nekdaj
  3. Implementacija in upravljanje varnostne tehnologije je cenejše
  4. Svet postaja manj vreden zaupanja

Pred nadaljevanjem moramo spoznati osnovno terminologijo. Koristno je tudi, da poznamo angleške izraze:

- Gostiteljski računalniški sistem (host) je računalnik, ki ga moramo varovati. To je lahko strežni računalnik, ali pa odjemalec, ki komunicira s strežnikom.

- Storitev (Service) je  program v uporabniškem prostoru, kjer izvaja kakšno uporabno nalogo

- Ranljivost (vulnerability ) je pomanjkljivost, hiba v programu,  kritična z vidika varnosti. Napadalec išče take pomanjkljivosti v programih s ciljem, da si poviša pravice oziroma dostopnost v našem sistemu.

- Sistem za odkrivanje vdorov - IDS (intrusion detection system)  poskuša odkriti oziroma preprečiti napade

- Napad (attack) je metoda izkoriščanja ranljivosti.

- Grožnja (threat): pomeni napadanje s strani motiviranega in sposobenga nasprotnika

Za varnost moramo poskrbeti na naslednjih komponentah računalniškega sistema:

* Odjemalec: Preprečiti moramo neavtoriziran dostop. Uvesti moramo zaščito privatnosti pred zlonamerno kodo, ki povzroča spreminjanje ali uničevanje naših programov in podatkov.  Zavarovati se moramo tudi pred nenamernim, slučajnim vnašanjem nekonsistentnosti
* Omrežje: Preprečiti moramo prestrezanje zaupnih informacij. Pomagamo si lahko z enkripcijo
* Strežnik: Ne smemo dovoliti neavtoriziranega dostopa. Strežniku se lahko »zgodi« tudi napad, ki povzroči  takoimenovano »odklonitev storitve« (denial of service)

Varnost mora upoštevati zunanje okolje sistema in sistem zaščititi pred:

* Neavtoriziranim dostopom.
* Zlonamernim spreminjanjem ali uničevanjem

## - Varnostni system mora upoštevati zunanje okolje sistema. Govorimo o takoimenovani »sistemski varnosti«, ki pokriva: 🡪 Varnost računalnika + varnost omrežja + varnost interneta - Lažje se zaščitimo pred slučajno, nenamerno napačno uporabo kot pred zlorabo

### Vrste napadalcev

Varnostni sistem mora upoštevati dve vrsti napadalcev: zunanje in notranje. Notranji napadalci so lahko tudi naši zaposleni:

- Med aktivnostmi zunanjih napadalcev sodijo:

🡪 Napadi virusov, črvov in drugih vsiljivcev, spam in kraja računalnikov (tudi to)

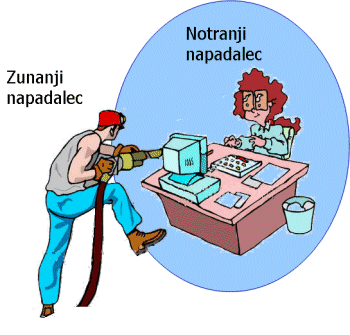
- Notranji napadalci pa nas lahko ogrožajo na naslednje načine:

🡪 Finančne goljufije, sabotaže, posredovanje privilegiranih podatkov izven organizacije

🡪 Zavračanje in pomanjkanje odgovornosti

🡪Pretirano zaupanje v IT

🡪 Telefon in faks sta bolj zanesljiva



Slika :Zunanji in notranji napadalec

**Zunanji napadalec**

🡪Potrebuje dostop do sistema

🡪 Deluje hitro, da ga ne bi odkrili

🡪 Vgradi “zadnja vrata” (trapdoors) za nadaljni dostop

🡪 Deluje v okolju, ki ga ne pozna

**Notranji napadalec**

🡪 Ima dostop do sistema

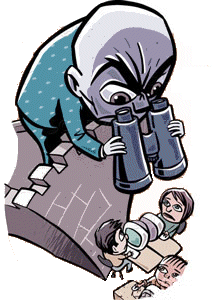
🡪 Deluje lagodno

🡪 Ima zagotovljen dostop v prihodnosti

🡪 Dela v znanem okolju

🡪 Ve, kaj je pomembno

NA KAJ MORAMO BITI POZORNI

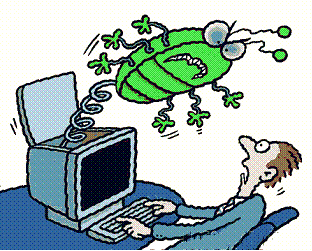


Slika : Nepridiprav

* Pozor na  sumljive vzorce aktivnosti – na primer večkratno vnašanje napačnih gesel kaže na ugibanje gesel.
* Zapisovanje dogodkov (Audit log) – zapisovanje časa, uporabnika, tipa vseh dostopov do objekta, kar olajša obnavljanje in razvoj boljših varnostnih mer.
* Periodično skeniranje sistema za odkrivanje varnostnih lukenj. To delamo tipično, ko je računalnik manj obremenjen.
* Iščemo:
* Kratka gesla, ki jih je lahko uganiti
* Neavtorizirane programe
* Nepričakovane stalno tekoče programe
* Napačne zaščite direktorijev
* Napačne zaščite sistemskih podatkovnih datotek

POJMI

-Računalniški virus je računalniški program, ki se je sposoben sam razširjati preko drugih računalniških programov ali dokumentov. Zaradi tega se računalniški virus obnaša zelo podobno biološkemu virusu, ki se širi tako, da okuži celice. Do okužbe pride s kopiranjem takih programov preko interneta ali z disketami .



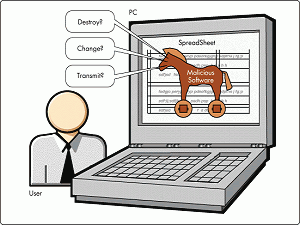
Slika : Računalniški virus

-Računalniški črv je prav tako kot virus, ki se širi iz računalnika v računalnik, vendar tako, da sam izvaja funkcije računalnika za prenos datotek ali podatkov. Ko se črv naseli v sistem, lahko potuje sam. Velika nevarnost črvov je njihova sposobnost izjemno hitrega širjenja. Hekerji so postali mojstri skrivanja računalniških črvov kot prilog elektronske pošte. Ko nič hudega sluteči uporabnik odpre prilogo, je črv aktiviran in se, odvisno od namena hekerja, razpošlje kot priloga e-pošte na vse naslove v e-poštnem imeniku uporabnika.



Slika : Računalniški črv

-Trojanski konj je egment kode, ki zlorabi svoje okolje.  Izkorišča mehanizme, ki omogočajo programom, pisanih  s strani enih uporabnikov, da jih izvajajo drugi.  Trojanski konj oponaša funkcionalnost legitimnega istoimenskega programa.  Vendar ima skrito “poslovanje.” Ima torej v resnici (še) drugo funkcijo, ki je uporabniku neznana.



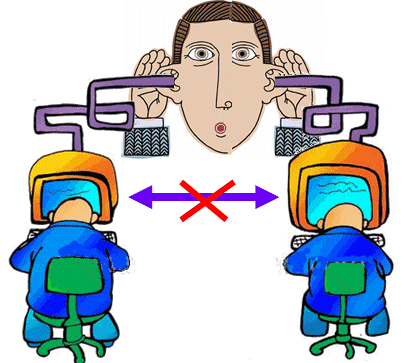
Slika 5:Trojanski konj

-Zadnja vrata so poseben identifikator uporabnika ali geslo, ki omogoča, da obidemo normalne varnostne postopke.

Zadnja vrata so poseben identifikator uporabnika ali geslo, ki omogoča, da obidemo normalne varnostne postopke.

* Lahko so vključena tudi v prevajalnik.
* Po angleško jim pravimo  trap doors ali backdoors.
* Omogočajo dostop do sistema s preskokom običajnih vstopnih (login) postopkov
* Omogočajo nepooblaščen dostop v sistem.

### Napad moža v sredini



Slika : Napad moža v sredini

Smisel napada, ki mu pravimo “man-in-the-middle” je v preusmeritvi prometa med dvema računalnika proti tretjemu (napadalcu), ki se dela, da je legitimna komunikacijska točka.

* Komunikacija na temelju javnega ključa, recimo med Jankom in Metko, je ranljiva.
* Predpostavimo, da vdiralec Pepe lahko prisluškuje tako Jankotu kot Metki, lahko pa tudi spreminja, briše in nadomešča sporočila ter ustvarja nova. Pepe lahko tako pooseblja Metko, ko se ta pogovarja z Jankom, ter Janka, ko se ta pogovarja z Metko. Napad bi lahko potekal tako.
* Janko pošlje Metki svoj javni ključ, Pepe ga prestreže in pošlje Metki svoj javni ključ.
* Metka tvori svoj naključni ključ seanse (session key), kodira z njim Jankov javni ključ (ki je v resnici Pepetov) in ga pošlje Janku.
* Pepe prestreže njeno obvestilo, dekodira ključ seanse s svojim privatnim ključem, zakodira ga z javnim ključem Janka in mu ga pošlje.
* Janko sprejme sporočilo, za katerega misli,  da je od Metke. Dekodira ga s svojim privatnim klučem in dobi tako ključ seanse (session key).

Janko in Metka si začneta izmenjevati sporočila z uporabo ključa seanse. Pepe, ki sedaj prav tako ima ta ključ, lahko nemoteno dešifrira kompleten pogovor.

🡪 Danes prevladujejo predvsem trojanski konji in črvi. Zaradi tega se uporabniki pogosto varujejo samo pred določenim tipom zlobnih računalniških aplikacij in so bolj ranljivi za ostale.

## Varnost na omrežju

* Manj varno: brezžično omrežje
* Drugo najmanj varno: stalno ožičene povezave
* Tretje najmanj varno: Občasne povezave (na primer dial-up)
* Najbolj varno: Nikoli povezan računalnik

## PROTIVIRUSNI PROGRAMI

-Za zaščito pred virusi najpogosteje uporabljamo **protivirusni** program, ki je lahko prosto dostopen (npr. AVG,…) ali plačljiv (npr. McAfee, F-Secure, Norton…). Vsak protivirusni program vsebuje knjižnico virusov. Najpomembnejše je, da program posodablja to knjižnico virusov (najpogosteje prek spletne strani proizvajalca programa) vsakodnevno ali celo večkrat na dan, če je računalnik stalno povezan v internet. Ena od pomembnejših nastavitev je tudi pregledovanje datotek (angl. "scan") na zunanjih pomnilnikih (tudi dohodne in odhodne pošte), ki naj bo prav tako vsakodnevno. Ko protivirusni program najde virus, ga lahko (več v nastavitvah programa):

* + uniči (pozdravi),
  + preimenuje oz. premakne v karanteno (onemogoči njegovo delovanje)
  + ali izbriše (če je vgrajen v sistemske datoteke, ne brišimo).

ŠKODLJIVI PROGRAMI

🡪 Parazitski programi, parasiteware, je programje, ki prepiše oglaševalske in oglasne povezave in jih nadomesti s svojimi. Tako preusmerja promet na druge spletne strani in krade zaslužek poštenim oglaševalcem in trgovcem. Za varnost sicer ne predstavlja posebne grožnje. Precej drugačen je v tem pogledu malware ali zlonamerno programje. *Malware* je splošna oznaka za zlo kodo, katere namen je predvsem čimbolj učinkovito poseči v delovanje računalniškega sistema. Sem spadajo predvsem virusi in trojanski konji (s katerimi se vzpostavljajo nezakonita prikrita omrežja), bi pa lahko v to kategorijo uvrstili tudi nekatere oglaševalske programe, ki storijo vse, da bi se obdržali na sistemu. Mednje pogosto spadajo tudi ugrabitelji brskalnikov (ang. Browser Hijackers) - gre za programe, ki “ugrabijo” spletni brskalnik (ponavadi IE) ter spremenijo začetno stran na kakšen "megasearch", ki je natrpan še s kakšnimi dodatnimi "prijetnimi" programskimi paketi. Ugrabitelji brskalnikov ponavadi niso škodljivi so pa izjemno nadležni in v večini primerov precej težavni za odstranjevanje s sistema. Za namestitev se navadno uporablja prikrita namestitev ali pa poskus z ukano prepričati uporabnika, da ga namesti na računalnik. Dialerji pa so navadno “brezplačno darilo” iz pornografskih strani. Njihov primarni namen je z ali brez vednosti uporabnika prekiniti obstoječo klicno povezavo v internet in vzpostaviti novo povezavo, seveda na komercialno telefonsko številko. Ti programi zato lahko povzročijo veliko finančno škode uporabniku, saj pogosto kličejo na plačljive številke v oddaljene kraje sveta. Seveda so tej nevarnosti izpostavljeni predvsem lastniki klicnega dostopa do interneta.

🡪 Adware ali programi namenjeni prikazovanju oglasov so, kot pove že ime, namenjeni prikazovanju oglasov. Da bi bil učinek oglaševanja večji, tovrstni programi skušajo o uporabniku oziroma njegovih brskalnih in nakupnih navadah zbrati čimveč podatkov (pogosto tudi z uporabo piškotkov), na podlagi teh podatkov pa potem prikazujejo personalizirane oglase. V to kategorijo uvrščamo tudi programe, ki podatkov o uporabniku ne pošiljajo v internet, pač pa samo prikazujejo oglase iz obsežne zbirke vnaprej pripravljenih oglasov. Za razliko od njih, pa je *spyware* nekoliko bolj aktiven, saj aktivno spremlja uporabnikove internetne aktivnosti (vključno z analizo pikotkov in priljubljenih povezav) in te podatke sporoča upravitelju vohunskega omrežja. Izraz vohunski je pravzaprav malce zavajajoč, saj ne gre za obveščevalno vohunjenje, pač pa za zbiranje podatkov za potrebe marketinga in profiliranje uporabnikov. Zbrani podatki so nato uporabljeni za direktno oglaševanje. Prikrita omrežja so poseben problem, zato jih tukaj omenjamo le na kratko. Gre za omrežja med seboj povezanih računalnikov, ki jih je mogoče uporabiti za shranjevanje podatkov ali skupno uporabo procesorskega časa, delijo pa se na zakonita in nezakonita. Slednja se pogosto uporabljajo za napade in zanje se uporablja tudi izraz *botneti*.

🡪 Izraz '*spyware*' ali vohunski program se je prvič pojavil na USENET-u 16. oktobra 1995, kjer se je nekdo [norčeval](http://groups-beta.google.com/group/rec.humor/browse_thread/thread/b4ce62633b90473b/6aef24c0e13cd161?q=spyware&rnum=2&hl=en#6aef24c0e13cd161) iz Microsoftove programske opreme, ki naj bi po internetu na prikrit način zbirala informacije o uporabnikih Microsoftove programske opreme. Izraz se je dokončno uveljavil leta 1999, ko ga je uporabilo programersko podjetje Zone Labs, ter v začetku leta 2000, ko se je pojavil prvi program za odstranjevanje tovrstnih vohunskih programov OptOut.

-Simptomi okužbe:

Simptomi okužbe z raznimi *spyware* programi se kažejo na več načinov, eni so manj, drugi so bolj neprijetni. Spet eni izmed teh znakov so bolj ali manj očitni. Najbolj očiten znak, da se nekaj dogaja z računalnikom je vsekakor veliko število raznih pop-up oglasov, ki se včasih množijo hitreje, kot jih uporabnik zapira. Posebej očitni postanejo s svojim pojavljanje takrat, ko brskalnik sploh ni v uporabi.

Drug precej očiten znak, da se nekaj dogaja je nepojasnjena počasnost računalnika. Programi so namreč v večini primerov zelo slabo spisani in jim uspe drastično zmanjšati zmogljivost računalnika, včasih do te mere, da je že komaj uporaben za čisto pisarniška opravila ali pa celo popolnoma odpove. Nekateri spyware programi ob odstranitvi celo poškodujejo sistemske datoteke.

Še eden zelo očitnih znakov je "ugrabitev brskalnika". V tem primeru spyware privzeto domačo stran zamenja z neko drugo, namestitev stare privzete spletne pa ni mogoča. Te ugrabitve so zelo neprijetne, v večini primerov se jih je precej težko znebiti. Ponavadi najbolj zaleže ročno odstranjevanje s primernimi programskimi orodji.

-Kako se znebiti podatkov?

Antivirusni programi so namenjeni odstranjevanju virusov in ne odstranjujejo *spywara*. Razlog je v tem, da je med proizvajalci AV programov in proizvajalci *spywara* prišlo do pravnih sporov, v katerih so popustili proizvajalci AV programske opreme. Torej – protivirusni programi ne zadostujejo. Kljub vsemu pa je pred odstranjevanjem *spywara* priporočljivo pregledati disk in odstraniti morebitne trojanske konje in viruse.

Preden se lotite dela z namenskim programjem za odstranjevanje, je priporočljivo poskusiti ročno odstraniti *spyware*, ki to dovoli. Nekatere programe se da odstraniti iz Windows vmesnika za odstranjevanje/popravljanje programske opreme, nameščene na računalniku. V večini primerov pa je potrebno uporabiti prepričljivejše prijeme. Seveda je pred čiščenjem sistema potrebno odstraniti tudi programe, s katerimi se namesti *spyware*, ker v nekaterih primerih po čiščenju ne bodo delovali ali pa bodo poskrbeli za družbo ob prvi priložnosti – beri povezavi z internetom.

Zelo učinkovit program za popravljanje ugrabitev brskalnika je *Hijack This!*, ki pa zahteva nekoliko več znanja – poišče namreč vse z brskalnikom povezane vnose v registru, dobre ali slabe, ki jih nato uporabnik identificira in sam odstrani. Pri tem lahko pride do napake, tako da je potrebno biti pazljiv, da poleg *spywara* ne odpove še kak legitimen program.

Za odstranjevanje je na voljo več različnih programov, od katerih sta izpostavljena *Adaware* in *SpyBot*, ki se razlikujeta v tem, da je *Adaware* lažji za uporabo, je pa *SpyBot* agresivnejši in posledično učinkovitejši. Poleg teh dveh programov je dobro uporabiti tudi *Microsoftov Windows AntiSpyware* program, ki je še sicer v beta razvojni različici, vendar deluje zelo dobro. Nekateri uporabljajo tudi Anti-Spy.info. Seveda je potrebno pred uporabo programje oziroma bazo iskanik zajedalskih programov posodobiti. Priporočljivo je tudi uporabiti kombinacijo več programov, ker se lahko zgodi, da posamezen program kaj spregleda.

🡪 Še ena, predvsem z *CoolWebSearch* trojancem povezana težava so poškodovane sistemske datoteke. V tem primeru je potrebno ponovno namestiti te datoteke z Windows namestitvenega CD-ja. To so navadno

* control.exe
* rundll32.exe
* wmplayer.exe
* msconfig.exe
* notepad.exe
* shell.dll
* SDHelper.dll

Te datoteke namreč trojanec namesti z lastnimi kopijami in se tako ponovno namesti na sistem vsakič, ko Windows pokliče katero od teh datotek.

-Obramba

V lastno obrambo lahko naredimo več stvari. Prva in verjetno najpomembnejša je pazljivost pri prenašanju programov. Pred namestitvijo kakšnega specifičnega programa se je najbolje najprej pozanimati kakšne so izkušnje drugih uporabnikov. Iskanje po raznih straneh, kot je download.com se lahko zaključi s programom, ki sicer opravi delo, obenem pa nas preseneti s kakim po možnosti dobro skritim dodatkom. Prav tako je potrebna previdnost pri klikanju med brskanjem po spletu in pri odpiranju priponk elektronske pošte

V primeru uporabe brskalnika Microsoft Internet Explorer je potrebno izklopiti uporabo *ActiveX* kontrolnikov in zategniti varnost za območje interneta. Potrebno se je tudi zavedati, da razni dodatki za MSIE, npr. brskalnika Maxthon ali Avant, nudijo dodatno funkcionalnost, obenem pa trpijo za istimi varnostnimi luknjami kot MSIE na katerem temeljijo. Še najlažja in obenem najbolj učinkovita rešitev je zamenjava MSIE z Mozillo, Firefoxom, Opero ali kakšnim alternativnim brskalnikom. Seveda je nujno potrebno tudi pravočasno in temeljito nameščanje varnostnih popravkov za operacijski sistem MS Windows. Uporabniki širokopasovnih povezav naj uporabljajo samodejno posodabljanje sistema, uporabniki analognih ali ISDN linij pa naj nameščajo vsaj popravke za varnostne luknje, označene kot kritične.

Eden zanimivejših pristopov k blokiranju *spyware* programov je tudi blokada dostopa do *spyware* strežnikov s pomočjo ustreznega vnosa v Windows *hosts* datoteko. Seznam spyware strežnikov ponuja npr. spletna stran [www.accs-net.com/hosts](http://www.accs-net.com/hosts/), od koder je mogoče prenesti že pripravljeno *hosts* datoteko, ki jo prekopirate v ustrezen imenik (c:\Windows\system32\drivers\etc\) s čimer preprečite povezovanje na spyware strežnike. Uporaba teh prirejenih *hosts* datotek je primerna tudi za domače usmerjevalnike, saj tako z eno potezo zablokiramo dostop do spyware strežnikov za celotno domače omrežje.

Seveda je pa potrebno poleg vseh zgoraj naštetih postopkov redno pregledovati sistem s posodobljenimi verzijami programov za odkrivanje *spywara* in predvsem paziti, kaj prenašamo, kakšne pogoje uporabe sprejemamo in kje klikamo na OK gumbe. Predvsem se je pa potrebno ustrezno podučiti tudi o “stranskih učinkih” uporabe interneta.

## 10 zakonov varnosti

•         Če te zlobnež prepriča, da poženeš njegov program na svojem računalniku, to ni več tvoj računalnik.   
•         Če lahko zlobnež spremeni operacijski sistem na tvojem računalniku, to ni več tvoj računalnik   
•         Če ima zlobnež neomejen fizični dostop do tvojega računalnika, to ni več tvoj računalnik   
•         Če dovoliš zlobnežu, da nalaga programe (upload) na tvojo spletno stran, to ni več tvoja spletna stran   
•         Slaba gesla zahtevajo močno zaščito   
•         Računalnik je le toliko varen, kolikor je zanesljiv njegov administrator   
•         Enkriptiran podatek je le toliko varen, kolikor je varen ključ za dekripcijo   
•         Neaužuriran skener virusov je le nekaj več vreden od nobenega virusnega skenerja   
•         Absolutna anonimnost ni praktična ne v realnem življenju in ne na spletu   
•         Tehnologija ni zdravilo za vse

ZAŠČITA IN PREVENTIVA PRI DELU V INTERNETU

* Bodimo previdni pri **prenašanju** podatkov z disketo, zgoščenko …
* Zaščitimo **brskalnik** (internetne možnosti: neželena okna).
* Namestimo zanesljiv **požarni zid** (nastavitve).
* Namestimo **protivohunske** programe.
* Redno izdelujmo **rezervne kopije sistemskih datotek.**
* **Posodabljajmo licenčne programe** s popravki (angl. "update") proizvajalcev teh programov.
* Programi, ki jih dobimo brezplačno na internetu, niso vedno zanesljivi in brez virusov. Preden program namestimo, se pozanimajmo o zanesljivosti.
* Bodimo previdni, ko beremo **elektronsko pošto in priloge**: ko prejmemo elektronsko pošto, nikoli ne odpirajmo ali shranjujmo priloge (angl. "attachment"), za katero ne vemo, kaj vsebuje (npr. vbs, .srs in .pif ali dokument.doc.vbs ali pamela.exe, joke.exe, nude.exe)! Nikoli ne odpirajmo ali shranjujmo priloge, ki nam jo pošlje neznanec/neznanka! Shranjujmo samo datoteke takšnih tipov, ki jih poznamo: DOC (Word), XLS (Excel), JPG (slika), GIF (slika), BMP (slika) … predvsem pa od ljudi, ki jih poznamo. Pozanimajmo se na spletu, kakšno e-pošto smo prejeli, preden jo

Odpiramo.