

# Računalniška varnost, zasebnost in etika

Informacijske tehnologije

Doc. dr. Aleš Hladnik

## Računalniška varnost

- n Eno od področij informacijske varnosti (INFORmation SECurity, INFOSEC)
- n **Računalniško varnostno tveganje** – dejanje, ki ogrozi delovanje ali poškoduje računalniški sistem
- n Zlonamerni programi – programski vsiljivci
  - u Virusi
  - u Črvi
  - u Trojanski konji
- n Računalniški vdori (Hacking)
- n Kraja strojne/programske opreme
- n Odpoved sistema

## Računalniški virusi, črvi in trojanski konji

---

- n **Virus** je potencialno škodljiv računalniški program
  - u Veže se na gostitelja – program ali datoteko – lahko se samodejno razmnožuje (replicira) in poškoduje datoteke
- n **Črv** se širi s samorazmnoževanjem po računalniških omrežjih, izkoriščajoč njihove ranljivostne točke in lahko povzroči onesposobitev računalnika ali omrežja
- n **Trojanski konj** izgleda kot legitimen program (ali je vanj vgrajen) in postane škodljiv, ko ga uporabnik zažene
  - u Za njihovo razmnoževanje in širjenje je potrebno sodelovanje uporabnika

## Vrste virusov

---

- n Zagonski (Boot sector) virusi
  - u Nahajajo se v zagonskem sektorju trdega diska in ga spreminjajo
- n Virusi, ki se širijo z e-pošto
- n Logične in časovne bombe
  - u Aktivirajo se ob določenem dogodku (npr. tiskanje) ali datumu
- n Makro virusi
- n “Cross-site scripting” virusi
  - u Izkoriščajo ranljivosti spletnih brskalnikov in spletnih aplikacij

## Širjenje virusa s pomočjo e-pošte

**1. korak** Zlonamerni programerji napišejo virusni program. Virus skrijejo v Wordov dokument, ki ga pripnejo e-sporočilu



**2. korak** Po internetu pošljejo e-sporočilo na tisoče naslovov uporabnikov po vsem svetu

**Korak 3a**  
Nekateri uporabniki odprejo priponko, s čimer postane njihov računalnik okužen z virusom

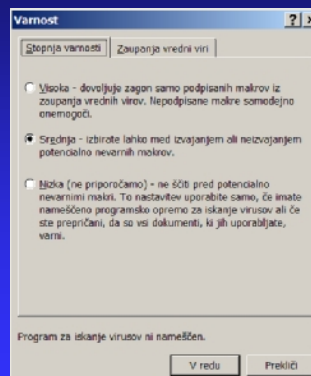


**Korak 3b** Ker ne pozna pošiljatelja, večina uporabnikov ne odpre sporočila in ga izbriše. Njihovi računalniki niso okuženi.



## Makro virusi

- n **Makro** – program, ki se uporablja za razširjanje funkcionalnosti programov kot sta urejevalnik besedil ali program za delo s preglednicami
- n **Makro virus** – računalniški virus, ki se prenaša z makro programi
- n Zaščita pred makro virusi
  - u Nastavi nivo makro varnosti v programih, ki omogočajo pisanje makrov
  - u Pri srednjem nivoju varnosti se pojavi opozorilo, da dokument vsebuje makro



## Protivirusni program

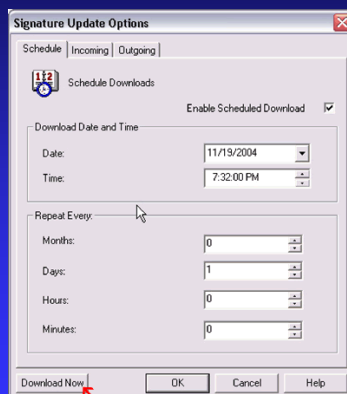
- n Program za odkrivanje in odstranjevanje računalniških virusov
- n Običajno ščiti tudi pred črvi in trojanskimi konji

### POPULAR ANTIVIRUS PROGRAMS

- AVG Anti-Virus
- eTrust EZ Antivirus
- F-Secure Anti-Virus
- Kaspersky Anti-Virus Personal
- McAfee VirusScan
- Norton AntiVirus
- Trend Micro PC-cillin
- Vexira Antivirus

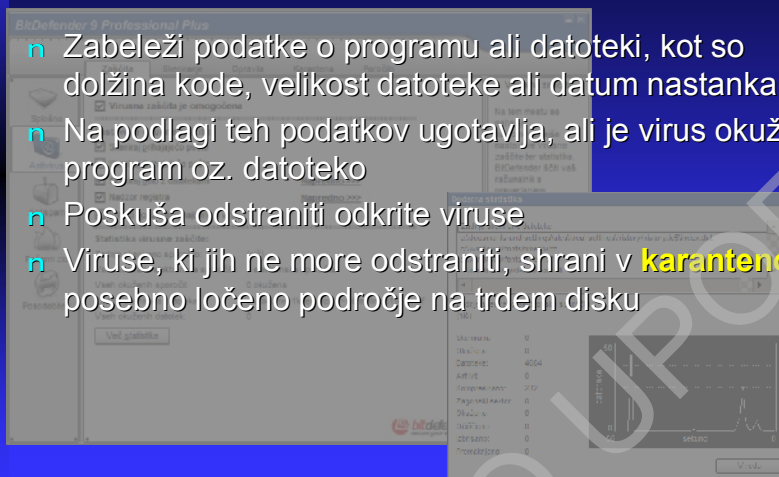
## Virusni podpis

- n Specifični vzorec virusne kode
- n Protivirusni programi iščejo virusne podpise (definicije)
- n Pomembno redno posodabljanje



## Kako deluje protivirusni program

- n Zabeleži podatke o programu ali datoteki, kot so dolžina kode, velikost datoteke ali datum nastanka
- n Na podlagi teh podatkov ugotavlja, ali je virus okužil program oz. datoteko
- n Poskuša odstraniti odkrite viruse
- n Viruse, ki jih ne more odstraniti, shrani v **karanteno** – posebno ločeno področje na trdem disku



## Kako preprečiti okužbe

- n Nastavi makro varnost v programih, tako da boš lahko omogočil ali onemogočil makre
- n Namesti protivirusni program na vseh svojih računalnikih
- n Nikoli ne odpiraj e-poštnih priponk, če jih ne pričakuješ ali če niso od znane osebe
- n Če te protivirusni program opozori, da je priponka okužena, jo takoj izbrši
- n Vse z interneta prenešene programe in datoteke skeniraj glede morebitne prisotnosti programskih vsiljivcev
- n Namesti oz. omogoči osebni požarni zid

## Onesposobitev storitev in stranska vrata

---

- n **Onesposobitev storitev** (Denial of Service, DoS) – napad, ki onemogoči oz. prepreči računalniku dostop do internetnih storitev, npr. spleta ali e-pošte
- n **Stranska vrata** (Back door) – program ali skupek navodil v programu, s katerim lahko zlonamerni uporabnik obide varnostne mehanizme pri dostopanju do računalniških virov

## Lažno predstavljanje (IP spoofing)

---

- n Ogrožanje omrežja z nepooblaščenim dostopom
- n Lažno predstavljanje pošiljatelja npr. pri prenosu podatkov po internetu
  - u Uporabnik – žrtev – je prepričan, da gre za pošiljatelja z zaupanja vrednega računalnika oz. IP naslova

## Požarni zid

- n Varnostni sistem namenjen preprečevanju nepooblaščenih dostopov oz. vdorov
  - u Sestoji iz strojne in/ali programske opreme

- u **Osebni požarni zid**

### PERSONAL FIREWALL SOFTWARE

BlackICE PC Protection
McAfee Personal Firewall Plus
Norton Personal Firewall
Sygate Personal Firewall Pro
Tiny Personal Firewall
ZoneAlarm Pro

- t Program za zaščito osebnega računalnika in podatkov pred nepooblaščenimi dostopi
- t Spremlja promet v in iz računalnika
- t Obvešča o poskusih vdora

## Varnostno središče Windows XP

Varnostno središče programa Windows

Varnostno središče  
Zaščitite svoj računalnik

**Viri informacij**

- Najnovejša Microsoftove informacije o varnosti in virusih
- Poiščite zadnje posodobitve na spletnem mestu Windows Update
- Podpora v primeru varnostnih težav
- Poiščite pomoč o varnostnem središču
- Spremeni obliko opozoril varnostnega središča

**Osnovni varnostni ukrepi**  
V varnostnem središču lahko upravljate varnostne nastavitve programa Windows. Če želite zaščititi računalnik, morajo biti trije ključni varnostni ukrepi vklopljeni. Če nastavitve kažejo, da niso vklopljeni, upoštevajte priporočila. Če se želite pozneje vrniti v varnostno središče, odprite spodnjo ploščo. [Kaj novega ponuja program Windows za zaščito računalnika?](#)

**Požarni zid** DELUJE

**Samodejno posodabljanje** DELUJE

**Protivirusna zaščita** DELUJE

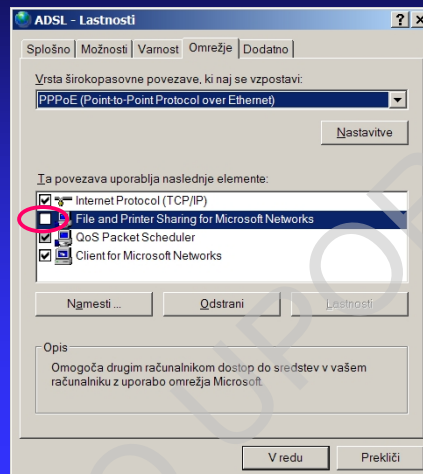
**Upravljanje varnostnih nastavitev za:**

- Internetne možnosti
- Automatic Updates
- Požarni zid programa Windows

Pri Microsoftu skrbimo za vašo zasebnost. Prosim, preberite našo izjavo o zasebnosti.

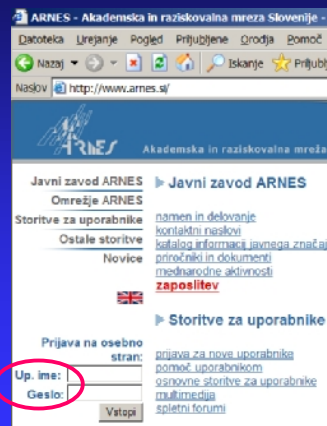
## Skupna raba datotek in tiskalnikov

- n Z **onemogočenjem** skupne rabe in dostopanja do sredstev (datoteke, tiskalniki) v našem računalniku zmanjšamo verjetnost vdorov oz. zlorab



## Uporabniško ime in geslo

- n **Uporabniško ime** – edinstvena kombinacija znakov namenjena identifikaciji posameznika
- n **Geslo** – zasebna kombinacija znakov, ki v povezavi z uporabniškim imenom omogoča dostop do računalniških in omrežnih virov



## Varnost gesla

n Daljša gesla zagotavljajo višjo stopnjo varnosti

PASSWORD PROTECTION		AVERAGE TIME TO DISCOVER	
Number of Characters	Possible Combinations	Human	Computer
1	36	3 minutes	.00018 second
2	1,300	2 hours	.00065 second
3	47,000	3 days	.02 second
4	1,700,000	3 months	1 second
5	60,000,000	10 years	30 seconds
10	3,700,000,000,000,000	580 million years	59 years

- Possible characters include the letters A–Z and numbers 0–9
- Human discovery assumes 1 try every 10 seconds
- Computer discovery assumes 1 million tries per second
- Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations

## Biometrična naprava

n Potrditev identitete uporabnika na podlagi njegovih fizičnih ali vedenjskih značilnosti

- u Prstni odtis
- u Oblika roke
- u Podpis
- u Vzorec šarenice
- u Glas



## Kraja strojne opreme

---

- n Zaščita pred krajo ali njenimi neprijetnimi posledicami – izgubo podatkov ali pomembnih osebnih informacij
  - u Zaklepanje računalnikov (ključavnice, kabli)
  - u Alarmi, gesla, pametne kartice, biometrika
  - u Remote Laptop Security (RLS): lastnik prenosnika lahko onemogoči dostop do podatkov na ukradenem računalniku s poljubnega računalnika z internetnim dostopom

## Kraja programske opreme

---

- n Kraja ali nelegalno kopiranje programske opreme ali namerno brisanje programov
- n **Piratstvo** – nelegalno kopiranje avtorsko zaščitene programske opreme
  - u Ponarejanje
  - u Nalaganje na disk
  - u Mehko piratstvo
  - u Dajanje v najem
  - u Internetno piratstvo

## Licenčna pogodba

---

- n Pogodba, v kateri so opredeljene pravice do uporabe oz. izkoriščanja programske opreme
  - u **Licenčna pogodba za končnega uporabnika** – dovoljuje uporabniku namestitev programa na enem računalniku, ustvarjanje varnostne kopije in prodajo programa po odstranitvi z računalnika

## Drugi ukrepi proti kraji programske opreme

---

- n Aktivacija programske opreme
  - u Vnos identifikacijske številke izdelka preko interneta ali po telefonu
  - u Uporabnik prejme edinstveno namestitveno identifikacijsko številko
- n **Business Software Alliance** (BSA) skrbi za boljše razumevanje in večjo osveščenost glede problemov programskega piratstva

## Enkripcija (šifriranje)

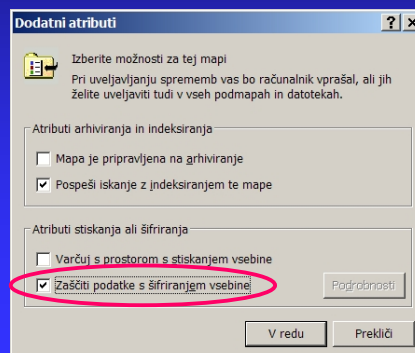
- n Oblika zaščite pred krajo informacij
- n Postopek pretvorbe navadnega besedila (Plaintext) v šifrirano (Ciphertext)
- n Enkripcijski ključ navadno vključuje več metod šifriranja
- n Da bi lahko prebral sporočilo, mora prejemnik dekriptirati (dešifrirati) podatke

SAMPLE ENCRYPTION METHODS

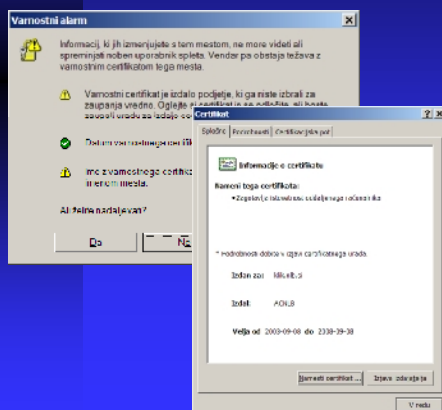
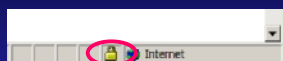
Name	Method	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYERY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)

## Enkripcija v Windows XP

- n Enkripcija vsebine datotek in map
  - u Raziskovalec → zelena datoteka ali mapa → desni miškin gumb → Lastnosti/Splošno/Dodatno



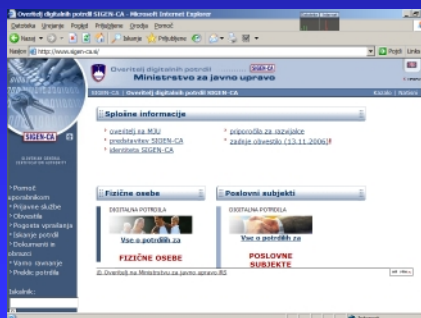
## Internetna varnost



- n Večina spletnih brskalnikov uporablja enkripcijo
- n **Varna stran (povezava)** – stran, ki uporablja enkripcijo za zavarovanje podatkov
- n **Digitalno potrdilo (certifikat)** – obvestilo, ki jamči legitimnost spletne strani

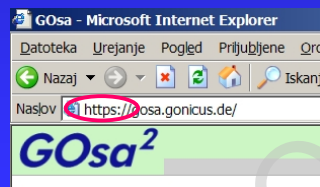
## Internetna varnost

- n **Overovitelj** (Certificate Authority, CA) – pooblaščen oseba ali podjetje, ki izdaja in potrjuje digitalna potrdila
- n Uporabniki zaprosijo za digitalno potrdilo pri overovitelju
  - n VeriSign
  - n SIGEN-CA

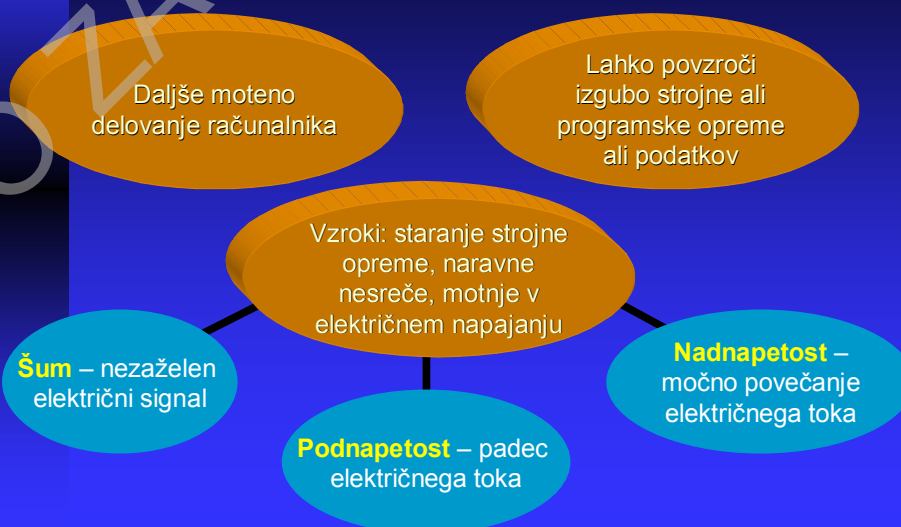


## Internetna varnost

- n **Sloj varnih vtičnic** (Secure Sockets Layer, SSL) – protokol, ki omogoča šifrirano povezavo in s tem šifriran prenos vseh podatkov med strežnikom in odjemalcem
  - u Uporaba pri plačilu blaga ali storitev po internetu (e-trgovina), spletnem brskanju, e-pošti, internetnem faksiranju, itd.



## Odpuved sistema



## Odpoved sistema

- n **Brezprekinitveno napajanje** (Uninterruptible Power Supply, UPS) – naprava, ki zagotavlja napajanje računalnika ob izpadu ali motnjah električne energije
  - u Vsebuje zmogljiv akumulator



## Varnostno kopiranje (arhiviranje)

Izdelava varnostne kopije datoteke, programa ali diska

**Celotno kopiranje**  
vseh datotek v računalniku

**Selektivno kopiranje**  
izbranih datotek

**Trigeneracijsko kopiranje**  
treh kopij pomembnih datotek

V primeru odpovedi sistema ali poškodovanih datotek lahko datoteke **obnovimo** tako, da jih skopiramo na prvotno mesto

## Brezžična varnost

- n Zagotovitev varnosti brezžične dostopovne točke (Wireless Access Point, WAP)
  - u WAP ne sme oddajati omrežnega imena uporabnika
  - u Omogočenje Wired Equivalent Privacy (WEP) ali Wi-Fi Protected Access (WPA)

## Etika in družba

- n Moralne smernice glede uporabe računalnikov in informacijskih sistemov

Nepooblaščen uporaba računalnikov in omrežij

Kraja programske opreme

Pravilnost podatkov in informacij

Avtorsko pravo in intelektualna lastnina

Pravila obnašanja

Informacijska zasebnost

## Informacijska zasebnost

- n Pravica posameznikov in podjetij do onemogočenja ali omejevanja zbiranja in uporabe informacij o njih
- n Dandanes v praksi težko izvedljiva zaradi velike količine on-line podatkov oz. informacij
- n **Nadzor zaposlenih** – legalna uporaba računalnikov z namenom ugotavljanja, v kakšne namene zaposleni uporabljajo računalnik na delovnem mestu

## Zaščita osebnih podatkov

V obrazce, garancijske liste in ostale on-line formularje vpiši le zahtevane podatke

Izogibaj se nakupovalnih klubov in uporabe kreditnih kartic

Po končanem spletnem brskanju počisti zgodovino obiskanih strani

Namesti program za nadzor oz. filtriranje piškotkov

Ustvari si brezplačni e-račun in ga uporabljaš za vnos v komercialne obrazce

Opozori trgovce, da ne smejo širiti tvojih osebnih podatkov

Namesti osebni požarni zid

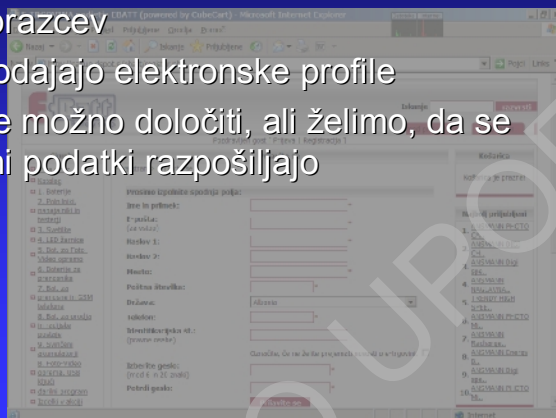
Uporabi možnost filtriranja e-sporočil, ki jo nudi tvoj ISP ali namesti program za boj z nezaželeno pošto

V nobenem primeru ne odgovarjaj na nezaželeno pošto

Onemogoči skupno rabo datotek in tiskalnikov preko internetne povezave

## Elektronski profil

- n Podatki, ki se zbirajo na podlagi izpolnjenih spletnih obrazcev
- n Trgovci prodajajo elektronske profile
- n Običajno je možno določiti, ali želimo, da se naši osebni podatki razpošiljajo



## Piškotki (Cookies)

Uporabniške nastavitve

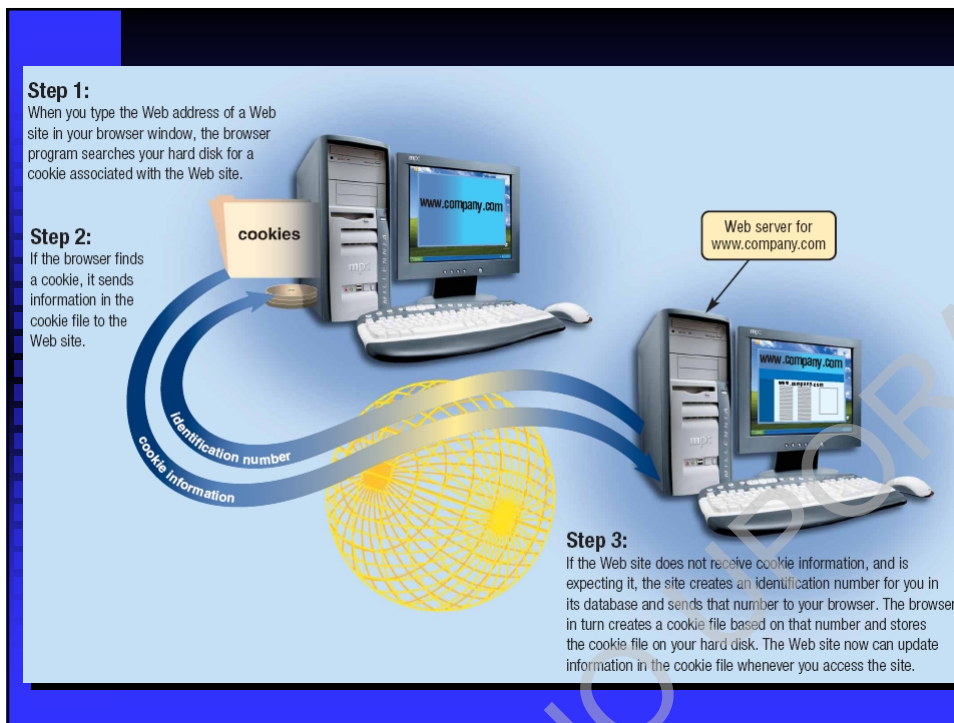
Datoteka v našem računalniku, kjer so shranjeni podatki o nas

Nekatere spletne strani prodajajo ali trgujejo z informacijami, shranjenimi v piškotkih

Kako pogosto obiskujemo spletne strani

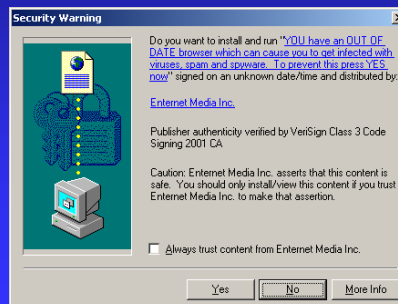
Interesi in brskalne navade

Nastavi brskalnik, da sprejema piškotke, te vpraša pred sprejemanjem ali pa jih onemogoči



## Vohunski in oglaševalni programi

- n **Vohunski program** (Spyware) – omogoča skrivno in nepooblaščno spremljanje stanja ali aktivnosti uporabnika računalnika in zbiranje osebnih informacij
- n **Oglaševalni program** (Adware) – pri uporabi interneta se samodejno namesti v računalnik uporabnika in omogoča sprejemanje in prikazovanje reklamnih sporočil



## Nezaželena pošta

- n **Nezaželena oz. nadležna pošta** (Spam) – nadležno elektronsko sporočilo s komercialno vsebino, poslano na več naslovov
  - n Edini strošek oglaševalca je vzdrževanje mailing liste potencialnih kupcev
  - n Težko je dokazati krivdo oglaševalcem zaradi njihovega reklamiranja

## Boj z nezaželeno pošto



## Lažno predstavlanje (Phishing)

- n Nezakonit način zavajanja uporabnika z namenom pridobivanja njegovih osebnih podatkov (št. bančnega računa, uporabniška imena, gesla, ipd.)
- n Širjenje v obliki e-sporočil, trenutnega sporočanja ali pojavnih oken



## Nadzor vsebin

- n Omejevanje dostopa do določenih spletnih vsebin oz. strani
  - n Pornografija
  - n Nasilje
  - n Programsko piratstvo
  - n Nestrpnost (rasna, verska, politična, itd.)
- n Internet Content Rating Association (ICRA) je razvila sistem za kategorizacijo spletnih vsebin v razrede
- n **Programi za omejevanje dostopa** (Censorware, Web filtering)

## Računalniška forenzika

---

- n Računalniška (digitalna, omrežna ali kiberforenzika)
- n Odkrivanje, zbiranje in analiziranje dokazov, ki jih najdejo na računalnikih in omrežjih
- n Strokovnjaki računalniške forenzike morajo imeti široko izobrazbo (pravo, računalniška in druga tehnična znanja, komunikacijske sposobnosti) in pripravljenost na učenje

## Računalniki in zdravje

---

- n **Sindrom računalniškega vida (CSV)**
- n **Obolenje zaradi ponavljajoče se obremenitve (RSI)**
  - n Sindrom karpalnega kanala – vnetje živca, ki povezuje zapestje s podlaktjo
  - n Tendonitis – vnetje kit zaradi ponavljajočih se gibov
- n **Računalniška odvisnost** – oblika zasvojenosti z računalniki ali internetnimi storitvami, ko računalnik “požre” celotno družabno življenje

## Računalniki in zdravje

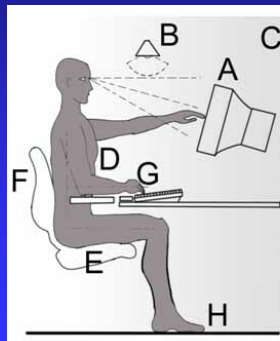
### TECHNIQUES TO EASE EYESTRAIN



- Every 10 to 15 minutes, take an eye break.
  - Look into the distance and focus on an object for 20 to 30 seconds.
  - Roll your eyes in a complete circle.
  - Close your eyes and rest them for at least one minute.
- Blink your eyes every five seconds.
- Place your display device about an arm's length away from your eyes with the top of the screen at eye level or below.
- Use large fonts.
- If you wear glasses, ask your doctor about computer glasses.
- Adjust the lighting.

## Računalniki in zdravje

**Ergonomika** – znanost, ki raziskuje udobje, učinkovitost in varnost na delovnem mestu



- A- Position monitor 18" to 24" away (approximately arm's length) and about 15° to 30° below your line of sight.
- B- Don't let light shine in your eyes or on your screen.
- C- Square screen to your line of vision.
- D- Forearms 90° from your spine.
- E- Thighs 90° from your spine.
- F- Use a well-made, adjustable office chair, preferably with padded, adjustable arms.
- G- Use a wrist pad to support your hands when not typing.
- H- Feet flat on the floor.

<http://www.rsiwarrior.com/ergonomics.html>

## Računalniki in zdravje

- n **Zeleno računalništvo** (Green computing) – zmanjšanje električne porabe in negativnih vplivov na okolje pri uporabi računalnikov

### GREEN COMPUTING SUGGESTIONS

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use paperless methods to communicate.
5. Recycle paper.
6. Buy recycled paper.
7. Recycle toner cartridges.
8. Recycle old computers and printers.
9. Telecommute (saves gas).



## Spletni naslovi

- n <http://www.itsecurityportal.com/> (novice v zvezi z IT varnostjo)
- n <http://www.securitywombat.com/security/home.php> (varnost domačih računalnikov)
- n <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp> (razlike med virusi, črvi in trojanskimi konji)
- n <http://www.sigen-ca.si/> (Slovenski overitelj digitalnih potrdil)
- n <http://computer-forensics.safemode.org/> (Računalniška forenzika)