Ponovimo – Povezivanje računala

- Što je mreža računala?

  Mreža računala je skup povezanih računala koja mogu međusobno komunicirati u cilju razmjene podataka preko nekog medija za prijenos podataka.

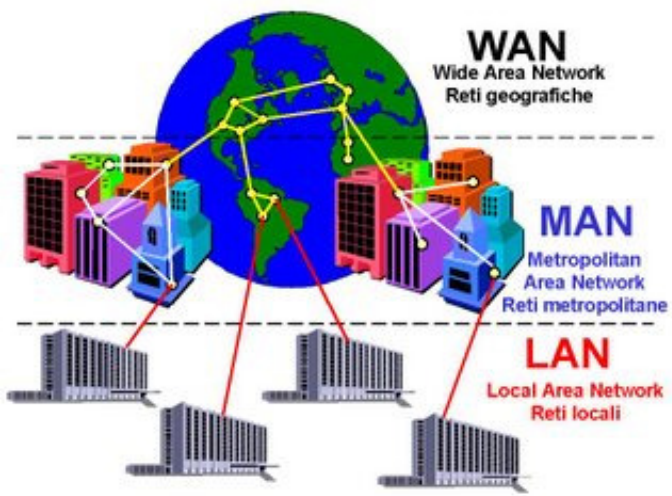
- Koliko najmanje moramo imati povezanih računala?

  2

- Računalnu mrežu čini koja strojna i programska oprema?
  - računalo kao primatelj/pošiljatelj
  - medij za prijenos podataka (obično žični, a može biti i bežični)
  - norme za prijenos (protokoli)
  - uređaji za povezivanje i upravljanje komunikacijom

Ponovimo – Povezivanje računala

- Vrste računalnih mreža?
  - **Po načinu razmjene podataka u mreži?**
    - **žične (*ethernet*)**
    - **bežične (*wireless*)**
    - **optičke mreže**
  - **Po broju i lokaciji umreženih računala?**
    - **LAN (*Local Area Network*)**
    - **MAN (*Metropolitan Area Network*)**
    - **WAN (*Wide Area Network*)**



Ponovimo – Povezivanje računala

- **Paketni prijenos podataka,** zašto ga tako nazivamo?

- **Svaki paket sastoji se iz tri dijela:**
  - zaglavlja (Header) – sadrži podatke o primatelju i pošiljatelju
  - tijelo sa podacima
  - začelje (Flag) – dio paketa namjenjen provjeri ispravnosti isporuke

ZAGLAVLJE	Tijelo s podacima	ZAČELJE

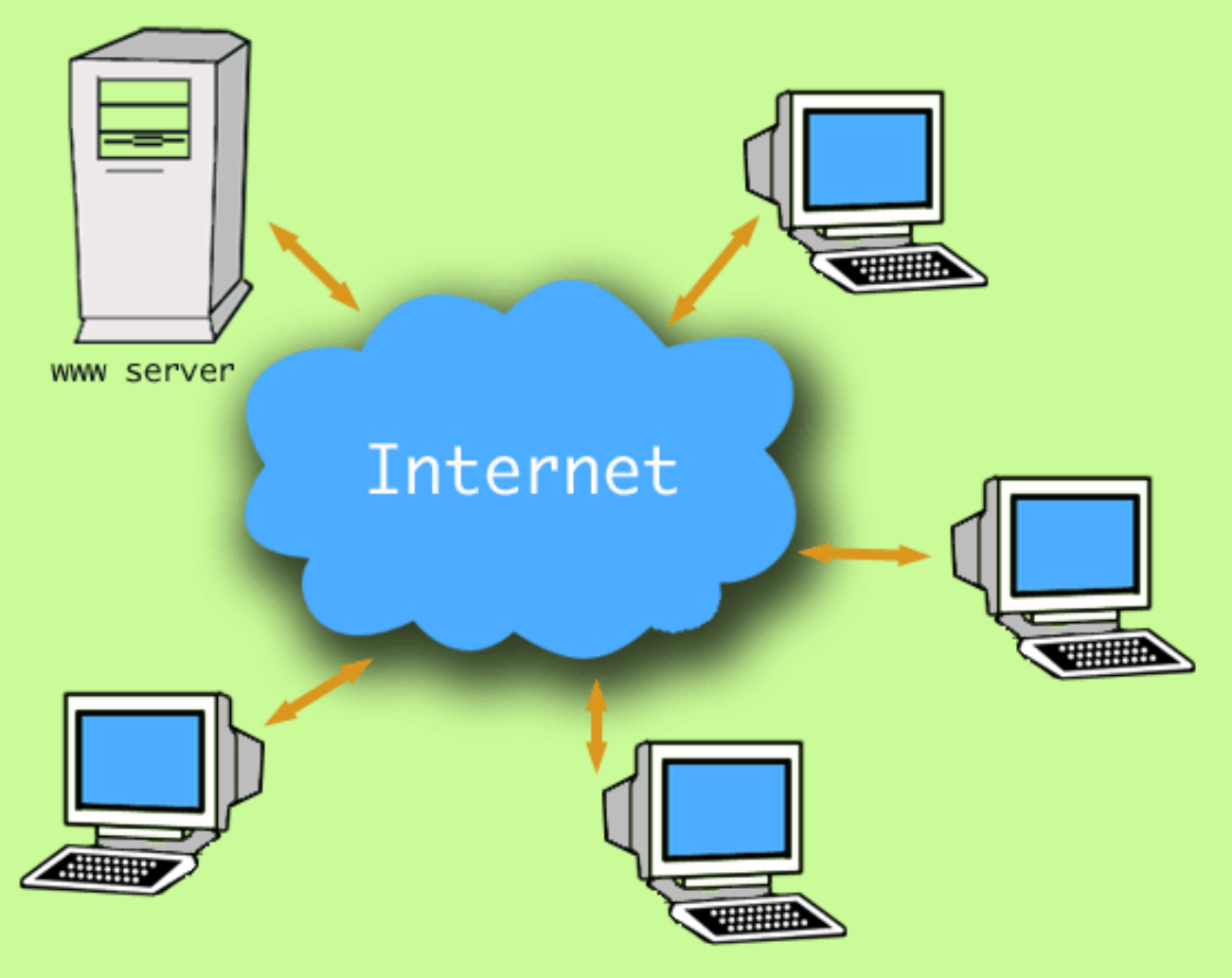
Ponovimo – Povezivanje računala

- **Norme za prijenos – protokoli**
  - Kako bi prijenos podataka bio uspješan, i računala i mrežni uređaji se moraju držati dogovorenih pravila.
  - Skup tih pravila nazivaju se **norma za prijenos (protokol).**
  - **Norme za prijenos** se brinu za dijeljenje podataka u pakete kod računala-pošiljatelja, pronalaze siguran put do računala-primatelja i osiguravaju ispravno spajanje paketa kako bi na odredište stigli identični podaci.
  - Najpoznatija norma za prijenos je **TCP/IP** na kojoj se temelji Internet.

- **Adresa računala**
  - **IP adresa**
    - **JEDINSTVENA!!**

5. Internet

5.1. Sustavno prikupljanje sadržaja s Weba (1)


www server
Internet

Kakav je internet medij

- Možemo reći da je Internet kao medij po mnogim osobinama poseban, jer povezuje različite oblike usluga koje omogućuju spremanje i razmjenu podataka kao i komunikaciju među korisnicima.

TRI GRUPE PROBLEMA korištenja Interneta:

1. Maliciozni (zlonamjerni) programi usmjereni prema računalu
2. Neželjeni sadržaji usmjereni prema korisniku
3. Neprovjereni ili neistiniti sadržaji

1. Malicionizmi (zlonamijerni) programi

- Zloćudni program je napravljen kako bi bez svjesnog pristanka korisnika ušao u korisnikovo računalo i načinio neku štetu.

- **TU SPADAJU:**
  1. **Računalni virusi**
  2. **Crv (worm)**
  3. **Trojanski konj**
  4. **Spyware (špijunski alat)**
  5. **Adware (oglasni alat)**

1. Malicionizmi (zlonamijerni) programi

1. Računalni virusi

- Obično se prikače za neku izvršnu datoteku
- **Šire se** prenošenjem te datoteke na drugo računalo putem nekog medija za distribuciju (spremnički štapić, CD/DVD) ili elektroničkom poštom (e-mail).
- **Posljedice** djelovanja virusa variraju od bezopasnog (koji uglavnom dosađuju korisniku) pa sve do teških posljedica kada dolazi do oštećenja datoteke, programa ili cijelog sustava.

1. Malicionizmi (zlonamijerni) programi

2. Crv (worm)

- Program (ili skupina programa) koji je sposoban samostalno se kopirati i raširiti funkcionalne kopije na druga računala preko mreže.

1. Malicionizmi (zlonamijerni) programi

3. Trojanski konj

- Imaju svojstvo da na prvi pogled izgledaju poput nekog običnog, korisnog programa, ali ipak nanosi štetu računalu na koje se instalira.

1. Malicionizmi (zlonamijerni) programi

4. Spyware (špijunski alat)

- Program koji se preko Interneta instalira na računalo i nepoznatoj osobi šalje podatke o korisnikovoj aktivnosti sa ciljem da ukrade broj kreditne kartice ili druge podatke koje može zloupotrijebiti.

1. Malicionizmi (zlonamijerni) programi

5. Adware (oglasni alat)

- Bez znanja korisnika se instalira na računalo i uznemiruje ga nepoželjnim oglasima.

2. Neželjeni sadržaji usmjereni prema korisniku

- **TU SPADAJU:**
  1. Spam
  2. Lažna obavijest *(hoax)*
  3. Phishing
  4. Dialer

2. Neželjeni sadržaji usmjereni prema korisniku

1. Spam

- Neželjena poruka koja stiže isključivo elektroničkom poštom i u većem opsegu može zatrpati poštanski sandučić (*Inbox*) elektroničke pošte.
- Obično su to reklame raznih proizvoda i bezvrijedna pošta sa linkovima na nesigurne stranice.

2. Neželjeni sadržaji usmjereni prema korisniku

2. Lažna obavijest *(hoax)*

- Nastoji nagovoriti korisnika na neku radnju koja može biti ilegalna ili može uzrokovati oštećenje računala ako korisnik naivno povjeruje.

2. Neželjeni sadržaji usmjereni prema korisniku

3. Phishing

- Postupak krađe tajnih podataka (zlouporaba identiteta) na način da se korisnika navede na otkrivanje povjerljivih podataka vjerujući da se radi o legalnoj instituciji.

2. Neželjeni sadržaji usmjereni prema korisniku

4. Dialer

- Program koji prekida telefonsku vezu sa davateljem internetske usluge i poziv preusmjerava a neku udaljenu zemlju, a posljedica je enormno velik telefonski račun.

3. Neprovjereni ili neistiniti sadržaj

- Internet sadrži veliku količinu informacija, ali nisu sve informacije jednako vrijedne jer svatko može napraviti web stranicu.

- Kako između svih tih stranica prepoznati one koje sadrže relevantne informacije, da im možemo vjerovati?
  - Prisiljeni smo neprestano provjeravati istinitost informacija na Internetu

Kako se zaštititi?

Sigurnosni alati i praktični savjeti:

- **Koristiti vatrozid (*firewall*).**

Program koji nadzire (filtrira) prijenos podataka između računala i mreže.
Uloga: ograničiti tu komunikaciju tako da zloćudni programi ne mogu bez vašeg znanja pristupiti računalu.

- **Koristiti antivirusni program.**

Uloga: da na računalu spriječi aktiviranje poznatih zlonamjernih aplikacija, poznatijih pod nazivima virusi, crvi i trojanski konji.
Antivirusni program prepoznaje zlonamjerne aplikacije koje su mu poznate uspoređivanjem njihovog koda s bazom takozvanih antivirusnih definicija. Zbog toga je vrlo važno redovito ažurirati (osvježavati) definicije vašeg antivirusnog softvera korištenjem automatskog ažuriranja dostupnog u većini antivirusnih alata (*Automatic Update*).

- **Koristiti redovite softverske nadogradnje.**
  - Ni jedan program, kao ni operacijski sustav nije savršen program i upravo ti propusti su najveći sigurnosni problemi.

Kako se zaštititi?

Praktični savjeti:

- Ne otvarati privitak elektroničke pošte ako ne poznajemo osobu koja ga je poslala.
- Lozinke koje se koriste za različite pristupe ne smiju biti predvidljive jer se lako probiju.
- Kada ostavljate osobne podatke na web-obrascima provjerite da li se radi o sigurnim web stranicama (imaju slovo "s" iza protokola - https://). Sjetite se da na internetu, surfajući ili dopisujući se nikad niste sami. Stoga prije nego ostavite osobne podatke dvaput razmislite jer mogu biti upotrijebljeni u zlonamjerne svrhe.
- Izbjegavati sumnjive lokacije na Internetu gdje bi mogli biti izloženi zlonamjernim programima.
- Ne otvarajte *PopUp* prozore jer često predstavljaju zamku.
- Nikad ne instalirajte nepoznat program.
- Informirajte se o računalnoj sigurnosti.