**MREŽNO POVEZIVANJE UREĐAJA**

**1. RAČUNALNA MREŽA (computer network)** je **skup** povezanih **uređaja** kojima je omogućena **razmjena podataka** **neovisno** **o** njihovoj **udaljenosti**.

**PREDNOSTI I NEDOSTACI UMREŽAVANJA:**

**Brza razmjena i prijenos podataka -pristup neprimjerenim sadržajima** (koji potiču mržnju, nasilje,

**Dijeljenje resursa** (pisač, skener, DVD uređaj…)nesnošljivost, diskriminaciju, dezinformacije, pornografiju …)

**Pretraživanje svjetskih baza podataka - nedovoljna sigurnost**

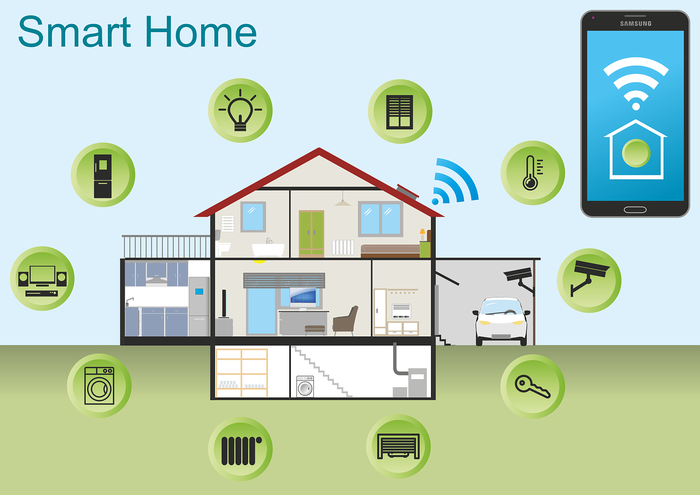
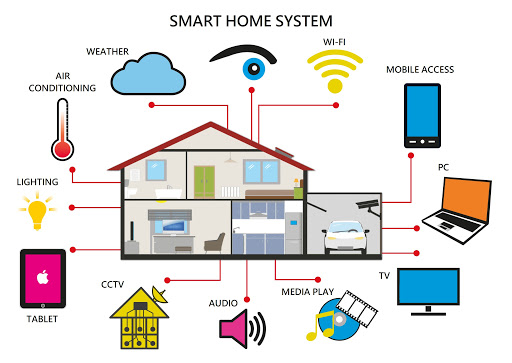
**Pristup edukacijskim sadržajima - zlonamjerni programi**

**Spremanje podataka na 1 računalo ili oblak - složenije održavanje sustava**

**Online igranje računalnih igrica - cyberbullying**

**Cyberbullying = cyber nasilje = zlostavljanje putem** (nasilje korištenjem) **digitalnih tehnologija.** 10 stvari koje tinejdžeri žele znati o cyber nasilju – pročitajte[**ovdje**](https://www.unicef.org/bih/pri%C4%8De/cyber-nasilje-cyberbullying-%C5%A1ta-je-i-kako-ga-zaustaviti)**.**

Mreža je stvorena od **čvorova** i **medija** („niti“) koji prenose te podatke.   
 Dakle, mediji su prenosioci podataka.

Primjeri pametne kuće

**IoT** = **Internet of Things** = **povezivanje** **uređaja** iz okoline **u globalnu mrežu**.

PONOVI:

1. Što je **mreža računala**?

2. Koje su **prednosti** povezivanja računala u mrežu?

3. Koji su **nedostaci** umrežavanja?  
4. Što je **cyberbuillying**?

5. Što je **IoT**?

**2. NAČINI MREŽNOG POVEZIVANJA**

U mreži su povezani (**umreženi**) **digitalni uređaji** **pomoću** **medija** koji **prenose podatke**.

**VEZA** među mrežnim uređajima može biti (**ovisno o MEDIJU** koji prenosi podatke):

1. **ŽIČANA** – **mrežni kabeli** (**bakreni**, **optička** vlakna) + **mrežna kartica** (u uređaju)  
    - (**vidi slike na sljedećoj stranici**)
2. **BEŽIČNA** (**wireless**), ostvaruje se na nekoliko načina:
3. **Radiovalovima (Wi-Fi)**   
   – bežično povezivanje uređaja gdje se podaci između 2 ili više umreženih uređaja prenose pomoću radijskih frekvencija (tj. radio valova) i odgovarajućih antena)

- najčešće u kućama, školama, tvrtkama - (**bežična** mrežna **kartica** te **pristupna točka**)

**Slika na kojoj se prikazuje tekst, računalo

Opis je automatski generiranA**. J**AVNA Wi-Fi mreža**

* Slobodan pristup mreži, tj. internetu
* Slika na kojoj se prikazuje tekst, isječak crteža

  Opis je automatski generiran Ne upisuje se lozinka
* Dostupna svima (JAVNA)

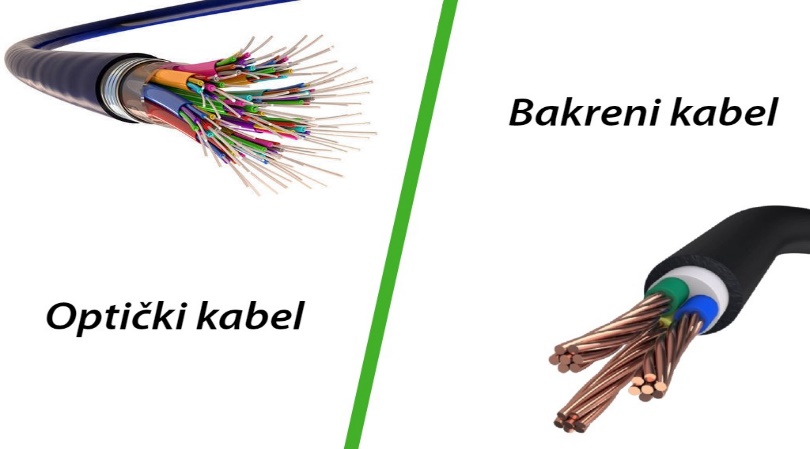
**B.PRIVATNA Wi-Fi mreža**

* Ne mogu se svi spojiti
* Zahtjeva unos lozinke
* Nije dostupna svima (privatna)
* Sigurnija od javne

1. **Mikrovalovima (Bluetooth)** (slika desno→)– radiovalovima **kratkog dometa** (do 10 m)   
   - **uređaji samo razmjenjuju podatke** npr. bežične slušalice, zvučnici, tipkovnice, miš, pametni telefon (Npr. razmjenjuju podatke. 2 pametna telefona, pametni telefon i zvučnik, pametni telefon i prijenosno računalo…)
2. **Infracrvenim valovima (IrDA)** (**I**nfra**r**ed **D**ata **A**ssociation)   
   - nedostaci: potrebna **direktna optička vidljivost** između 2 uređaja   
    te je **manja brzina** prijenosa podataka

**PROVJERI ZANJE:** [**KVIZ-1**](https://e.udzbenik.hr/U2020/infO6pov/62kviz1.htm)**,** [**KVIZ-2**](https://e.udzbenik.hr/U2020/infO6pov/62kviz2.htm)

**NEKI MEDIJI KOJI PRENOSE PODATKE**

**A. Od centrale do zgrade (kuće), B. Od utičnice** (za Internet)  **i od centrale prema do digitalnog uređaja koristi se   
određenom čvorištu: mrežni kabel**   
(prepoznat ćete ga po kvačici):

**Slika na kojoj se prikazuje kabel, priključak, prilagodnik

Opis je automatski generiran**

Slika na kojoj se prikazuje svijetlo

Opis je automatski generiran



**SAMO ZA ONE KOJI ŽELE ZNATI VIŠE - Dvije vrste mrežnog kabela**:

**UTP STP**

Slika na kojoj se prikazuje tekst

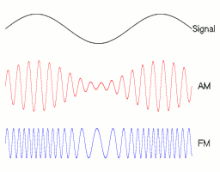
Opis je automatski generiranSlika na kojoj se prikazuje tekst

Opis je automatski generiran

**Nezaštićene upredene parice Zaštićene (aluminijskom folijom) upredene parice**

**UTP** (**U**nshielded **T**wisted **P**air) - kabel sličan STP kabelu ali **bez vodljivog omotača**, što ga čini **neotpornim na šum i vanjske elektromagnetske utjecaje**. No moderna tehnologija uspješno prevladava navedenu slabost. Svaka parica samostalno je upredena (uvijena) i potom su sve međusobno uvijene kako bi se otpornost na vanjske utjecaje povećala. Naravno, oko svih parica zajedno je zaštitni plastični omotač

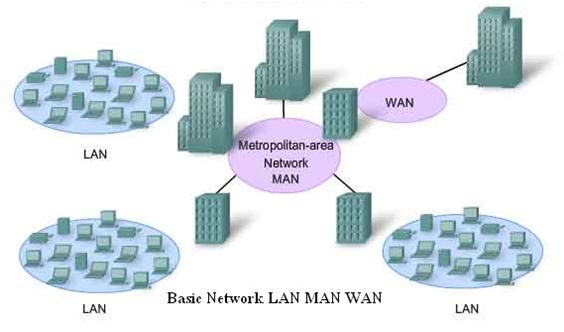
**STP** (**S**hielded **T**wisted **P**air) - **kabel s upredenim (uvijenim) bakrenim paricama oklopljen vodljivim pletivom ili omotačem,** u izvedbi s pojedinačno oklopljenim paricama (STP) ili samo s vanjskim vodljivim oklopom oko svih parica (ScTP - Screened Twisted Pair). Za potanju navedenu vrstu ponekad se koristi naziv FTP (Foil screened Twisted Pair), kada je u pitanju vodljiva folija kao oklop. Oko oklopa je plastični zaštitni omotač.

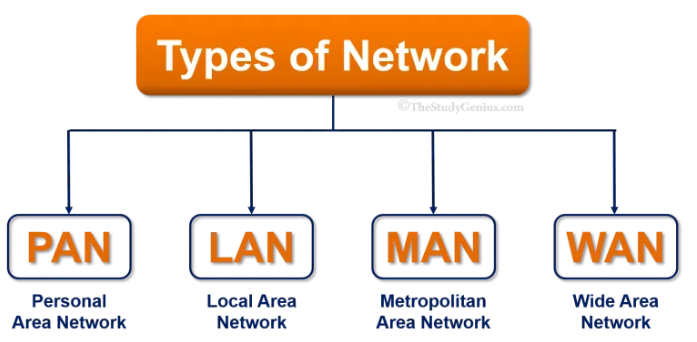


**Radiovalovi**

(animacijski prikaz)

**VRSTE MREŽA PREMA RASPROSTRANJENOSTI** – video možete pogledati [**ovdje**](https://www.youtube.com/watch?v=AHJSOnXAZb0&t=34s&ab_channel=TheStudyGenius)





**2. LAN**  (**L**ocal **A**rea **N**etwork) – **lokalna mreža**

**LOKALNA MREŽA** je mreža u kojoj se ovezuju računala i drugi mrežni uređaji na manjoj udaljenosti, odnosno na manjem (lokalnom) području, npr. školi, uredu…

- Najjednostavniji oblik LAN mreže, **najmanja** je (zato ide na 1. mjesto (po veličini)):

**1.PAN** (**P**ersonal **A**rea **N**etwork) – osobna / **kućna mreža**- spojeno barem 2 uređaja, a može ih biti i jako puno (vidi sliku u RB, pametna kuća)

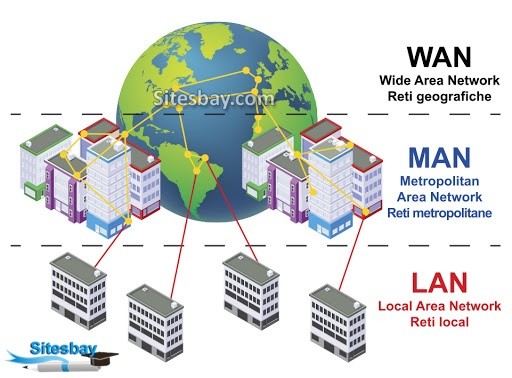
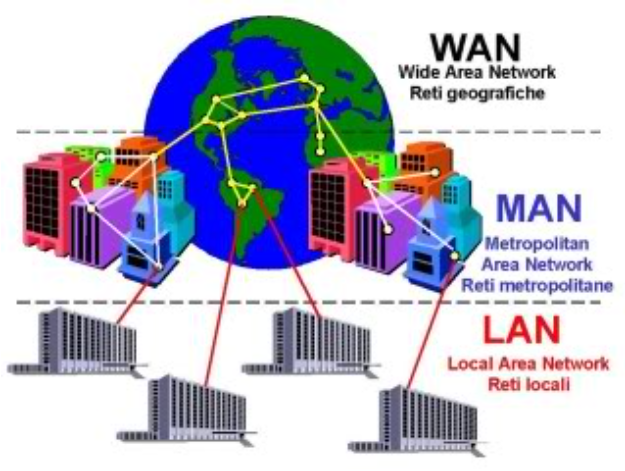
**3. MAN**  (**M**etropoliten **A**rea **N**etwork) – **gradska mreža** i šire

**GRADSKA MREŽA** - nastaje spajanjem lokalnih mreža lokalnih mreža koje su povezana na većim udaljenostima poput kvartova, gradova, manjih regija, županija …

**4. WAN** (**W**ide **A**rea **N**etwork) – **široko rasprostranjena mreža**

**RASPROSTRANJENA MREŽA** – nastaje spajanjem lokalnih mreža koje su povezane na većim udaljenostima poput država, regija (više gradova, više država), kontinenata.

**Internet – najpoznatija WAN mreža – „mreža svih mreža“**

**Provjeri svoje znanje:** [[**KVIZ**](https://e.udzbenik.hr/U2020/infO6pov/62kviz3.htm)](https://e.udzbenik.hr/U2020/infO6pov/62kviz3.htm)**-3**

[**KVIZ**](https://e.udzbenik.hr/U2020/infO6pov/62kviz4.htm)**-4**

Više o **vrstama mreža** možete pročitati [**ovdje**](https://hr.education-wiki.com/9440827-types-of-network).

**MREŽA NA MOBILNIM UREĐAJIMA**

Internet koristimo ovisno o tarifi i ovisno o postavkama mobilne mrežne veze.

**Mobilna mrežna veza omogućuje:**

* + 1. **Upućujete i primate pozive**
    2. Pod uvjetom da je uključena **PODATKOVNA VEZA:**
       - Korištenje usluge prijenosa podataka
       - Pregledavanje interneta
       - Primanje i slanje e-pošte
       - Dobivanje ažuriranih informacija za aplikacije

Što sve može MOBILNI UREĐAJ?

1. **Spojiti se na Wi-Fi** mrežu
2. Biti **Wi-Fi** **hotspot** (**pristupna točka**) – može dijeliti mobilnu vezu drugim uređajima (drugom mobitelu dajete pristup internetu jer. Npr. imate u tarifi beskonačan Internet, a vaš prijatelj je svoju količinu interneta potrošio).

**Kod Android** uređaja na **Wi-Fi hotspot** se može spojiti **do 5 uređaja** bežičnim putem.

**Kako uključiti i postaviti mobilnu pristupnu točku (hotspot)   
 pogledajte** [**ovdje**](https://e.udzbenik.hr/U2020/infO6pov/62hotspot.mp4)**.**

**4. VRSTE ŠTETNIH DJELOVANJA PREKO MREŽE**

**ZLONAMJERNI PROGRMI** (**malware, maliciozni**) – programi koji se pokreću na računalu bez  
 stvarnog pristanka korisnika čineći **štetu na računalnom i mrežnom sustavu.**

**VRSTE** ZLONAMJERNIH PROGRAMA:

**a) RAČUNALNI VIRUS** – računalni program koji se bez znanja korisnika kopira u datoteke ili memoriju računalnog sustava. Pri pokretanju zaraženog programa pokreće izvršavanje virusnog koda.

**b) RAČUNALNI CRV** – računalni program koji iskorištavajući sigurnosne propuste softvera ulazi u sustav te sam sebe umnožava kako bi se proširio na 2. računala

**c) TROJANSKI KONJ** – je program koji najčešće ima skrivenu štetnu funkcionalnost i obično se lažno predstavlja kao igra ili sadržaj koji se šalje u e-poruci.

**d) ŠPIJUNSKI PROGRAM** (**Spyware**) skuplja informacije i preuzima kontrolu nad zaraženim računalom.

**e) OGLASNI PROGRAM** (**Adware**) -korisniku prikazuje oglase i vrlo su opasni jer mogu  
 prikupljati korisnikove informacije kao što su podaci za prijavu (login),   
 adresa e-pošte, IP adresa računala, lokacija i slično.

**f) RANSOMWARE** – je program koji šifrira korisničke datoteke   
 (obično dokumente i slike) te tako onemogućuje njihovo daljnje korištenje.   
 Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje   
 nesmetano korištenje računala i datoteka.

**NEŽELJENI SADRŽAJI**

**a) Spam** – elektronička poruka u kojoj se nude razne usluge(internetska kupovina i sl.) bez odobrenja korisnika za njihovo primanje.

**b) Phishing** – poruke koje navode korisnika da klikne određeni link koji ga vodi na mrežne stranice zloćudnog mrežnog poslužitelja. (npr. predstave se lažno kao mrežne strnaice banaka te navode korisnika da upiše svoje povjerljive podatke).

**c) Hoax** - poruke elektroničke pošte neistinitog sadržaja poslane s ciljem zastrašivanja ili dezinformiranja primatelja.

**ZA ONE KOJI ŽELE ZNATI VIŠE - Ostale najčešće vrste štetnih djelovanja**

**Crimeware** je zlonamjerni program koji služi **za obavljanje kriminalnih radnji** kojima je krajnji cilj ostvarivanje nekog oblika imovinske koristi pomoću primjerice **krađe identiteta i osobnih podataka**.

**Keylogger** je program koji je namijenjen **tajnom praćenju i snimanju svih pritisnutih tipki na računalu**. Uglavnom se koristi **za krađu povjerljivih podataka** (brojeva kreditnih kartica, lozinke za pristup različitim servisima za plaćanje, PIN-ova…).

**Scareware** predstavlja zlonamjerni program **koji se širi prijevarom (plašenjem) korisnika**. Cilj je kod korisnika **izazvati zabrinutost ili strah** od određene prijetnje te ga **navesti na instalaciju zlonamjernog** softvera. U većini slučajeva **scareware** se pojavljuje u obliku **pop-up prozora**, oglasa (**banner**) i **lažnih** mrežnih **stranica** na koje je korisnik preusmjeren.

**Lažni** **anti**-**spyware** **alati** distribuiraju se **u obliku web reklama** koje **upozoravaju** korisnike **na zaraženost** računala zlonamjernim softverom te ih **navode da kupe lažni alat** koji ustvari ne uklanja **spyware**, već ga **instalira na korisničko računalo**. Stoga se **ne preporučuje instalacija lažnih besplatnih antivirusnih programa** ili anti-spyware zaštite, osim ako su službeno navedeni kao legitimni proizvodi.

**Rootkit** je vrsta zlonamjernog programa koja napadaču omogućuje **udaljenu administrativnu kontrolu nad računalom**. **Nevidljivi** su na računalu kojeg zaraze pa mogu proći mjeseci pa čak i godine prije nego bude primijećen. Za uklanjanje ovog softvera potrebno je **potpuno brisanje diska i reinstalacija operacijskog sustava.**

**Logic bomb** je računalni kod koji je **namjerno umetnut u softverski sustav** koji pokreće zlonamjernu funkciju kada se ispune određeni uvjeti. **Na primjer**, programer može sakriti dio koda koji **započinje brisanje datoteka** (poput okidača brisanja baze **podataka o plaćama** u nekoj firmi).

**PROVJERITE SVOJE ZANANJE:** [**KVIZ-5**](https://e.udzbenik.hr/U2020/infO6pov/62kviz5.htm)**,** [**KVIZ-6**](https://e.udzbenik.hr/U2020/infO6pov/62kviz6.htm)

**5. ZAŠTITA RAČUNALA, PROGRAMA I PODATAKA NA MREŽI**

**RAČUNALNA SIGURNOST** obuhvaća **skup mjera za osiguranje podataka na računalu**.

**Što možemo napraviti?**

- napraviti **sigurnosnu kopiju** **podataka**   
 (na medijima odvojenim od računala, npr. na prijenosnom tvrdom disku)

- održavajte **sustav ažuriranim** (čim su dostupne instalirajte redovite   
 nadogradnje (**update**) OS i najkorištenijih aplikacija)

- samo **s pouzdanih izvora preuzimajte** dokumente i programe

- **oprezni** budite **pri otvaranju** **nepoznate elektroničke poruke**

- **uključite vatrozid** (**firewall**) jer on nadzire, propušta ili odbacuje mrežni promet   
 (tj. filtrira, analizira i provjerava podatke koji dolaze s interneta i odlaze na njega.

-**instalirajte antivirusni program** (oprez SAMO JEDAN)

**ANTIVIRUSNI PROGRAM** – je računalni program koji prepoznaje zlonamjerne programe na vašem računalu, obavještava korisnika o pronalasku i uklanja ih prema potrebi.

**SAVJETI:**

**Ako dobijemo neki prijenosni medij (CD, DVD, memorijski štapić, prijenosni tvrdi disk itd.) što moramo prvo učiniti s podacima koji se na njemu nalaze? – Testirati antivirusnim programom.**

**Najčešći oblik pirenja malicioznih programa je njihovo slanje putem elektroničke pošte.**

**Detaljno o postavljanju i održavanju antivirusne zaštite pročitajte** [**ovdje.**](https://e.udzbenik.hr/U2020/infO6pov/62AVzastita.pdf)

**O dozvolama pristupa aplikacijama pročitajte** [**ovdje**](https://e.udzbenik.hr/U2020/infO6pov/62dozvole.pdf)**.**

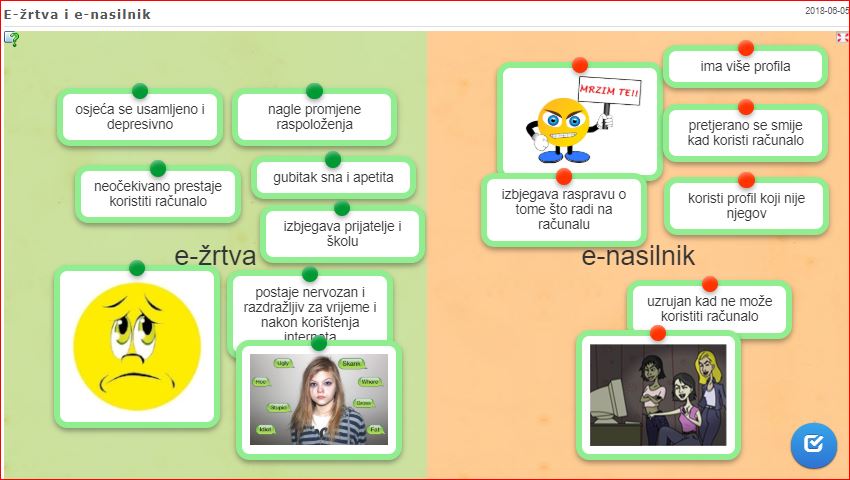
**PROVJERITE SVOJE ZNANJE:** [**KVIZ-7**](https://e.udzbenik.hr/U2020/infO6pov/62kviz7.htm)**,** [**KVIZ-8**](https://e.udzbenik.hr/U2020/infO6pov/62kviz8.htm)**.**

**6. PONAŠANJE NA MREŽI**

PONAŠANJE NA MREŽ**I**

* **Što je DIGITALNI TRAG?**  
  **Digitalni trag** su **sve informacije,** POZITIVNE i NEGATIVNE,koje su **ostavljene na internetu** NAMJERNO ili SLUČAJNO.
* **Razlika između DIGITALNOG ili OBIČNOG traga:  
  Digitalni trag ne nestaje s vremenom, već je ZAUVIJEK POHRANJEN,** a obični trag uglavnom s vremenom nestaje.
* **Navedi 3 aktivnosti koje pridonose stvaranju digitalnog traga:**                1. slanje elektroničke pošte  
                  2. komentare na društvenoj mreži  
                  3. bilo kakvo pretraživanje
* **Po čemu je objava informacija na internetu slična objavi informacija na oglasnoj ploči:**  
  INFORMACIJE su javno **dostupne**, svima vidljive, mogu se kopirati, dijeliti i **širiti bez kontrole vlasnika**.
* Informacije **NA INTERNETU I NA OGLASNOJ PLOČI**su svima dostupne, svima vidljive, mogu se kopirati, dijeliti i širiti bez kontrole vlasnika zato kažemo da je **objavljivanje informacija na internetu** **slično objavljivanju informacija na oglasnopj ploči.**
* **Što je NETIQUETTE?**  
  **NETIQUETTE je skup pravila dobrog ponašanja i komunikacije na internetu.  
                         Vidi:** [Netiquette](http://www.os-vnazor-cepin.skole.hr/upload/os-vnazor-cepin/images/static3/1051/File/netiquette.pdf)[**Kviz**](https://e.udzbenik.hr/U2019/infOS6/66link4.htm) **s ponuđenim odgovorima.**
* **Što je ELEKTRONIČKO NASILJE?**  
  **ELEKTRONIČKO NASILJE je bilo kakav oblik komunikacije preko interneta kod kojeg se određena osoba ZADIRKUJE, OMALOVAŽAVA, PONIŽAVA ili se na bilo koji način ŠIRI MRŽNJA prema pojedincu ili grupi.**
* **Nabroji 3 vrste elektroničkog nasilja:**  
   **- širenje govora mržnje  
   - širenje nasilnih ili uvredljivih komentara  
   - prosljeđivanje tuđih fotografija bez njihovog dopuštenja  
   - otkrivanje tuđih privatnih informacija**
* **Kako PRIJAVITI ELEKTRONIČKO NASILJE?  
   - POLICIJI pomoću stranice**[**http://redbutton.mup.hr**](http://redbutton.mup.hr/) **(zapamti adresu ove stranice)**                       
  **RODITELJU, UČITELJU/-ICI  ili nekoj 2. ODRASLOJ OSOBI.**
* **Besplatan i anoniman telefon u slučaju nasilja na internetu (za djecu i roditelje)**  
                         **0800  606  606 (zapamti ovaj broj telefona)**
* **Navedi 3 savjeta kako zaštititi svoj profil na mreži.  
   1. Podesiti postavke privatnosti  
   2. Ne prihvaćati zahtjeve za prijateljstvom od ljudi za koje nisi siguran da su ti prijatelji.  
   3. Ne objavljivati osobne podatke niti ih navoditi u opisu profila.**

[**Spajanje**](https://learningapps.org/5286632) **parova - E-žrtva i e-nasilnik - riješi zadatak  
 Rješenje zadatka (na sljedećoj stranici)**

[](http://os-22lipnja-sk.skole.hr/upload/os-22lipnja-sk/images/static3/1678/File/E-%C5%BErtva%20i%20e-nasilnik.JPG)

Najbolje mrežne stranice za mene

[](https://learningapps.org/display?v=puqofvbpn19)