

Centar za nestalu i zlostavljaju djeću



**Znaš li koji su
RIZICI DIGITALNOG DOBA?**

Projekt „Prepoznaj rizike digitalnog doba”



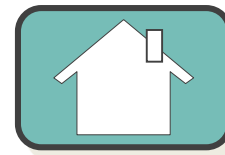
INTERNET



- **Internet** je svjetska računalna mreža, odnosno skup mreža, velikih i malih, koje se povezuju zajedno te čine jednu cjelinu kojoj je namjera razmjena podataka i korištenje raznih sadržaja, usluga i servisa.
- Računala koja su spojena na Internet mogu biti međusobno povezana **žičnim i bežičnim putem**.
- **WWW** (World Wide Web – u prijevodu „svjetska mreža“) se često pogrešno koristi kao sinonim za Internet, a zapravo predstavlja jednu uslugu kojom se ostvaruje razmjena podataka preko Interneta.
- Za dohvaćanje i prikaz sadržaja koriste se računalni programi koji se nazivaju **web-preglednici**.



INTERNET



- Na Internetu su vam dostupni svi **sadržaji** koje možete zamisliti:

glazba, slike, video
(jednom riječju -
"multimedija"),

rječnici,
enciklopedije,
obrazovanje,

turizam, zemljopisne
karte, raznolike upute i
savjeti,

elektroničko
bankarstvo, kupnja,
prodaja,

izravno
komuniciranje,
zabava

Dostupno je sve što bi netko želio učiniti dostupnim što većem broju korisnika, bilo to korisno, nekorisno ili čak i štetno...

DRUŠTVENE MREŽE



- **Društvena mreža** je vrsta internetskog servisa, koji služi za međusobno povezivanje korisnika.
- Danas postoje **stotine** ovakvih servisa.
- Društvene mreže se najčešće koriste za **komunikaciju** između dva ili više korisnika.
- Među **najpopularnijim** modernim sustavima za komunikaciju na internetu su: Facebook, Twitter, YouTube, Instagram, Skype i dr.
- **Korisnik** društvenih mreža može biti bilo tko.

Digitalni rizici

DRUŠTVENE MREŽE



Digitalni rizici

- **Anonimnost** predstavlja najveći rizik na društvenim mrežama.
- Nikad ne možemo biti potpuno sigurni da je osoba s kojom se dopisujemo baš ona za koju se predstavlja da je.
- Korisnici često na društvenim mrežama ostavljaju **osobne podatke**, stoga može doći do **zlouporabe** tih podataka.
- Društvene mreže su podložne **hakerskim upadima**.
- Najčešće **žrtve** takvih upada su maloljetnici.
- Zbog toga, mnoge društvene mreže imaju **zaštitu i kontrolu sadržaja**.



NASILJE PREKO INTERNETA

- **Nasilje preko Interneta** (cyberbullying) je jednako ozbiljno kao i nasilje u stvarnom svijetu. _____
- Ono podrazumijeva svaku komunikacijsku aktivnost cyber-tehnologijom koja se može smatrati **štetnom** za pojedinca. _____
- Djeca jedna drugu vrijeđaju koristeći različite **stranice** ili **aplikacije** na mobitelima, čime su te uvrede dostupne puno široj grupi ljudi nego kad se to događa „licem u lice“. _____
- Od takvog nasilja dijete ne može pobjeći u sigurnost svoga doma jer su **podsjetnici** na nasilje stalno dostupni putem računala i mobitela. _____



NASILJE PREKO INTERNETA

Postoje dvije vrste nasilja preko interneta: _____

1. Izravan napad događa se kada maloljetnik šalje uznemirujuće poruke mobitelom, elektroničkom poštom (e-mailom) ili na chatu; ukrade li ili promijeni lozinku za e-mail ili nadimak na chatu; objavljuje privatne podatke ili neistine na chatu, blogu ili internetskoj stranici; šalje uznemirujuće slike preko e-maila ili MMS-poruka na mobitelu; postavlja internetske ankete o žrtvi; šalje viruse na e-mail ili mobitel; šalje pornografiju i neželjenu poštu na e-mail ili mobitel te se lažno predstavlja kao drugo dijete. _____

2. Nasilje preko posrednika događa se kada počinitelj napada žrtvu preko treće osobe, koja toga najčešće nije ni svjesna. _____



Digitalni rizici

OPASNOSTI

- **Opasnosti** na Internetu su **mnogobrojne**, od izloženosti zlostavljanju osobito djece (putem uznemirujućih, agresivnih, prijetećih poruka, zastrašivanja, maltretiranja i sl.), preko direktne komunikacije s osobom koja traži neprimjerene odnose, do izlaganja neprimjerenim sadržajima (pornografski, slike nasilja, govor mržnje, poticanje nasilja, izazivaju strah, sram, razvijaju pogrešnu sliku o spolnosti...).
- Također postoji opasnost navođenja osobe na **odavanje osobnih podataka** (ugrožavanje privatnosti ili sigurnosti) radi **zloupotrebe** istih.
- Česta pojava u današnje vrijeme, kada zapravo ovisimo o tehnologiji, je **ovisnost o Internetu** koja nas ometa u socijalnom funkcioniranju te **narušava naše psihičko i/ili fizičko zdravlje** i javlja se uslijed **pretjeranog korištenja** Interneta.

OPASNOSTI



Digitalni rizici

- Osoba ovisna o internetu pokazuje određene **simptome**: pretjerano je zaokupljena internetom, provodi sve više vremena na internetu, ne može kontrolirati, smanjiti ili prekinuti upotrebu interneta, nemirna je, razdražljiva i neraspoložena, ostaje on-line duže negoli je namjeravala, ugrožava poznanstva, prijateljstva i veze, karijeru ili obrazovanje, laže članovima obitelji, prijateljima ili suradnicima kako bi prikrla koliko je uistinu zaokupljena internetom.
- **Posljedice** ovisnosti o Internetu: zanemarivanje obitelji ili prijatelja, smanjena učinkovitost na poslu/školi/fakultetu, socijalna izoliranost, kronična neispavanost, smanjena tjelesna aktivnost, sukobi s okolinom i sl.
- Na Internetu također postoji mogućnost **izlaganje neistinitim ili nepotpunim informacijama** koje mogu u krivom smjeru oblikovati naše stavove.
- Nije sve što pročitamo i saznamo putem Interneta istinito.



ZAŠTITA



- Kako se zaštititi na Internetu? Pokušajmo prvo usvojiti nekoliko osnovnih pojmova.
- **Antivirusni program** je računalni softver koji se koristi za identifikaciju, uklanjanje i zaštitu od računalnih virusa te drugih programa koji mogu uzrokovati probleme u korištenju računala, oštetiti softver i/ili podatke, a jednim imenom ih se naziva **malware** (još se naziva i zloćudni software ili maliciozni program).
- **Maliciozni programi** (malware) – računalni programi koji se pokreću na računalnom sustavu bez stvarnog korisnikovog pristanka i imaju neku vrstu nepoželjnog učinka (oštećenje programa i podataka, širenje na druga računala, krađa podataka, omogućavanje neovlaštenog udaljenog pristupa na računalo, prikazivanje reklamnih poruka, masovno slanje neželjene elektroničke pošte i dr.).
- To **mogu biti** crvi, računalni virusi, trojanski konji, spyware, adware, phishing napadi i slično.





ZAŠTITA



- **Vatrozid** (Firewall) ograničava mrežnu komunikaciju između našeg računala i Interneta, odnosno sprječava i filtrira sadržaje koje razmjenjuje naše računalo s ostalima u mreži.
- **Automatsko ažuriranje** operativnog sustava je preporučljivo kako bi se smanjila mogućnost zaraze računala. malwareom.
- **Pričuvna kopija** (backup) je najsigurniji način na koji možemo zaštititi svoje podatke.
- **Lozinku** je najbolje sastaviti kombinacijom velikih i malih slova, brojeva te znakova te je zadržite samo za sebe (nemojte je dijeliti ni s kim).
- Preporučljiva **lozinka** za bežičnu mrežu je potpuno nasumičan ključ – bez imena, datuma ili bilo čega drugog smislenog.
- Kako možeš znati da je **web stranica sigurna** za vas? Zatražiti savjet roditelja, Centra za sigurniji internet ili odrasle osobe ako ne znaš je li web stranica sigurna
- Zapamtite, kada je riječ o zaštiti računala, **najvažniju ulogu** imaju naše ponašanje i naše odluke.



Ministarstvo socijalne politike i mladih



Potraži nas!

CENTAR ZA NESTALU I ZLOSTAVLJANU DJECU

Josipa Jurja Strossmayera 1/1, 31000 Osijek

Telefon: 031/272-943

E-mail: info@cnzd.org

FB: CENTAR ZA NESTALU I ZLOSTAVLJANU DJECU

YouTube: Centar za nestalu i zlostavljaju djeću

Projekt „*Prepoznaj rizike digitalnog doba*“

Projekt financira

Ministarstvo socijalne politike i mladih

Partneri projekta



SVEUČILIŠTE J. J. STROSSMAYERA U OSIJEKU
FILOZOFSKI FAKULTET
FACULTY OF HUMANITIES AND SOCIAL SCIENCES

