Vodič za digitalna prava i bezbjednost mladih

Praktični vodič za škole, omladinske centre i mlade

Sigurno, pametno i odgovorno u digitalnom prostoru

VODIČ ZA DIGITALNA PRAVA I BEZBJEDNOST
Praktični vodič za mlade – Autor Željko Đukić

O VODIČU

Ovaj vodič je kreiran u okviru projekta **„Klik za sigurnost mladih na sjeveru“**, koji je finansiran kroz program **„Zaštita prava i promocija digitalnog građanstva: crnogorski digitalni štit (MDS)“**.

Program sprovodi **Centar za građansko obrazovanje (CGO)**, u partnerstvu sa **SHARE fondacijom** i u saradnji sa **Agencijom za audiovizuelne medijske usluge**, uz finansijsku podršku **Evropske unije** i kofinansiranje **Ministarstva regionalno-investicionog razvoja i saradnje sa nevladinim organizacijama**.

Vodič je namijenjen mladima, školama, omladinskim centrima i svima koji rade sa mladima, sa ciljem da doprinese boljem razumijevanju digitalnih prava, bezbjednog ponašanja na internetu, zaštite ličnih podataka i pravilnog reagovanja u rizičnim situacijama u digitalnom prostoru.

Napomena:
Stavovi, informacije i preporuke objavljene u ovom vodiču isključiva su odgovornost autora/izdavača i ne predstavljaju nužno stavove Evropske unije, Centra za građansko obrazovanje, SHARE fondacije, Agencije za audiovizuelne medijske usluge, Ministarstva regionalno-investicionog razvoja i saradnje sa nevladinim organizacijama, niti drugih partnera uključenih u sprovođenje programa.

SADRŽAJ

Ovaj projekat finansira Evropska unija

1. UVOD

Internet je danas sastavni dio svakodnevnog života mladih. Gotovo da ne postoji oblast života u kojoj digitalne tehnologije nijesu prisutne — od komunikacije sa porodicom, prijateljima i vršnjacima, preko učenja, informisanja i zabave, do izražavanja stavova, kreativnog rada, kupovine, prijavljivanja za različite programe i učestvovanja u društvenom životu. Mladi putem interneta prate vijesti, koriste društvene mreže, gledaju edukativne sadržaje, komuniciraju u grupama, igraju igrice, dijele fotografije i video zapise, istražuju teme koje ih zanimaju i grade svoj digitalni identitet.

Digitalni prostor pruža velike mogućnosti. On mladima omogućava brži pristup informacijama, razvijanje novih znanja i vještina, povezivanje sa ljudima iz različitih sredina, kreativno izražavanje i aktivno učešće u zajednici. Internet može biti prostor učenja, podrške, solidarnosti i stvaranja novih ideja. Zahvaljujući digitalnim alatima, mladi danas mogu lakše da pokrenu inicijative, predstave svoj rad, učestvuju u javnim diskusijama i pronađu prilike za obrazovanje, volontiranje, zapošljavanje ili lični razvoj.

Međutim, pored brojnih prednosti, digitalni prostor nosi i određene rizike. Mladi se na internetu mogu susresti sa neprimjerenim sadržajem, govorom mržnje, nasilnom komunikacijom, lažnim informacijama, prevarama, zloupotrebom ličnih podataka, pritiscima na društvenim mrežama, krađom identiteta ili različitim oblicima digitalnog nasilja. Poseban izazov predstavlja činjenica da se mnoge rizične situacije dešavaju brzo, često neprimjetno i u prostoru u kojem mladi nijesu uvijek sigurni kome mogu da se obrate za pomoć.

Zato je važno da mladi razumiju da internet nije prostor bez pravila. Kao i u stvarnom životu, i u digitalnom okruženju postoje prava, odgovornosti i granice. Svaka mlada osoba ima pravo na privatnost, sigurnost, dostojanstvo, slobodu izražavanja i zaštitu od nasilja i zloupotrebe. Istovremeno, svako ima odgovornost da poštuje druge, ne širi uvredljiv ili štetan sadržaj, ne dijeli tuđe podatke bez dozvole i ne učestvuje u ponašanju koje može ugroziti druge osobe.

Ovaj vodič je kreiran sa ciljem da mladima pruži osnovna, jasna i praktična znanja o digitalnim pravima i bezbjednom ponašanju na internetu. Namijenjen je učenicima, mladima, omladinskim centrima, školama, nastavnicima, roditeljima i svima koji rade sa mladima. Njegova svrha nije da zastraši mlade ili da ih odvrati od korišćenja interneta, već da im pomogne da digitalni prostor koriste pametnije, sigurnije i odgovornije.

U vodiču će biti objašnjeno šta su digitalna prava, zašto je važno čuvati lične podatke, kako prepoznati rizične situacije na internetu, kome se obratiti kada se problem dogodi i kako zaštititi sebe i druge. Posebna pažnja biće posvećena praktičnim savjetima — kako napraviti sigurnu lozinku, kako podesiti privatnost na društvenim mrežama, kako prepoznati prevaru, kako reagovati na digitalno nasilje i zašto je važno razmišljati prije nego što nešto objavimo ili podijelimo.

Bezbjednost na internetu ne znači samo zaštitu od tehničkih prijetnji. Ona podrazumijeva i emocionalnu sigurnost, poštovanje drugih, odgovorno ponašanje, kritičko razmišljanje i sposobnost da se prepoznaju informacije koje mogu biti netačne, manipulativne ili štetne. Zbog toga digitalna pismenost danas nije dodatna vještina, već osnovna potreba svakog mladog čovjeka.

Ovaj vodič treba da bude praktičan oslonac mladima u svakodnevnom korišćenju interneta. Njegova poruka je jednostavna: internet može biti koristan, kreativan i siguran prostor, ali samo ako znamo svoja prava, čuvamo svoje podatke, poštujemo druge i reagujemo na vrijeme kada primijetimo rizik. Digitalna bezbjednost počinje znanjem, a odgovorno ponašanje svakog pojedinca doprinosi sigurnijem internetu za sve.

2. ŠTA SU DIGITALNA PRAVA

Digitalna prava su prava koja imaš dok koristiš internet, digitalne uređaje, aplikacije, društvene mreže, onlajn platforme i druge digitalne usluge. Ona se odnose na tvoju sigurnost, privatnost, slobodu izražavanja, dostojanstvo i zaštitu u digitalnom prostoru. Drugim riječima, digitalna prava znače da i na internetu imaš pravo da budeš zaštićen, poštovan i slobodan da koristiš digitalne tehnologije na način koji ne ugrožava tebe niti druge.

Važno je da razumiješ da internet nije prostor bez pravila. Sve ono što važi u stvarnom životu — pravo na poštovanje, sigurnost, privatnost i zaštitu od nasilja — važi i u digitalnom svijetu. Kada koristiš društvene mreže, šalješ poruke, objavljuješ fotografije, komentarišeš sadržaje, učestvuješ u onlajn nastavi, igraš igrice ili koristiš aplikacije, ti i dalje imaš svoja prava. Ta prava treba da poznaješ kako bi znao/la kako da zaštitiš sebe, ali i kako da poštuješ druge.

Jedno od osnovnih digitalnih prava je **pravo na privatnost**. To znači da imaš pravo da odlučiš koje informacije o sebi želiš da podijeliš, sa kim ih dijeliš i na koji način. Tvoj privatni život ne prestaje kada koristiš internet. Fotografije, poruke, lokacija, kontakti, školske informacije, porodični podaci i druge lične stvari ne bi trebalo da budu dostupne svima. Zato je važno da pažljivo podešavaš privatnost na društvenim mrežama i aplikacijama, da ne prihvataš nepoznate osobe bez razmišljanja i da ne dijeliš podatke koje neko može zloupotrijebiti.

Drugo važno pravo je **pravo na zaštitu ličnih podataka**. Lični podaci su sve informacije koje mogu otkriti ko si ti ili gdje se nalaziš. To mogu biti tvoje ime i prezime, adresa, broj telefona, fotografija, škola koju pohađaš, korisničko ime, lozinka, e-mail adresa, lokacija ili bilo koji drugi podatak koji se odnosi na tebe. Tvoji podaci su vrijedni i ne treba ih davati svakome. Prije nego što uneseš podatke na neku internet stranicu, prijaviš se na aplikaciju ili učestvuješ u nagradnoj igri, važno je da razmisliš da li je ta stranica pouzdana i zašto traži tvoje podatke.

Digitalna prava uključuju i **pravo na slobodu izražavanja**. To znači da imaš pravo da izneseš svoje mišljenje, da postavljaš pitanja, učestvuješ u raspravama, dijeliš ideje i stvaraš sadržaj. Internet mladima pruža mnogo mogućnosti da budu kreativni, da govore o temama koje su im važne i da učestvuju u životu zajednice. Međutim, sloboda izražavanja ne znači da možemo vrijeđati, ponižavati, prijetiti ili širiti neistine o drugima. Tvoje mišljenje je važno, ali je važno i da ga izraziš odgovorno, uz poštovanje drugih osoba.

Još jedno važno pravo je **pravo na sigurnost u digitalnom prostoru**. To znači da imaš pravo da koristiš internet bez straha od uznemiravanja, prijetnji, ucjena, lažnog predstavljanja, govora mržnje, nasilnih poruka ili drugih oblika digitalnog nasilja. Niko nema pravo da te vrijeđa, zastrašuje, dijeli tvoje fotografije bez dozvole, traži od tebe nešto što ti je neprijatno ili te prisiljava da radiš nešto što ne želiš. Ako se takva situacija dogodi, važno je da znaš da nijesi kriv/a i da imaš pravo da potražiš pomoć.

Poznavanje digitalnih prava pomaže ti da bolje razumiješ kada je tvoje pravo ugroženo. Na primjer, ako neko objavi tvoju fotografiju bez tvoje dozvole, to može biti povreda tvoje privatnosti. Ako neko dijeli tvoje lične podatke, to može biti zloupotreba podataka. Ako te neko vrijeđa ili ismijava u grupi, to može biti oblik digitalnog nasilja. Ako ti neka aplikacija traži previše informacija koje nijesu potrebne, treba da budeš oprezan/na. Kada znaš svoja prava, lakše možeš prepoznati problem i reagovati na vrijeme.

Digitalna prava nijesu važna samo za tvoju zaštitu, već i za tvoju odgovornost prema drugima. Kao što ti imaš pravo na privatnost, tako i drugi imaju isto pravo. Kao što ti ne želiš da neko dijeli tvoje podatke bez dozvole, ni ti ne treba da dijeliš tuđe podatke. Kao što želiš da tvoje mišljenje bude poštovano, važno je da i ti poštuješ mišljenje drugih, čak i kada se ne slažeš sa njima. Siguran internet se gradi tako što svako od nas poštuje prava drugih ljudi.

Zato je važno da prije svake objave, komentara, poruke ili dijeljenja sadržaja zastaneš i razmisliš: Da li ovim štitim sebe? Da li poštujem drugu osobu? Da li dijelim nešto što može nekoga povrijediti? Da li je ovaj podatak bezbjedno objaviti? Da li bih isto rekao/la ili uradio/la i u stvarnom životu?

VAŽNO:
Tvoja prava online su jednako važna kao i u stvarnom životu. Imaš pravo na privatnost, sigurnost, zaštitu svojih podataka i slobodu izražavanja. Ako se u digitalnom prostoru osjećaš ugroženo, uznemireno ili nesigurno, važno je da se obratiš osobi od povjerenja — roditelju, nastavniku, pedagogu, psihologu, omladinskom radniku ili drugoj odrasloj osobi koja ti može pomoći. Internet treba da bude prostor znanja, komunikacije, kreativnosti i podrške, a ne prostor straha i pritiska.

3. PRIVATNOST I LIČNI PODACI

Privatnost na internetu znači da imaš pravo da kontrolišeš koje informacije o sebi dijeliš, sa kim ih dijeliš i ko ih može vidjeti. Kada koristiš društvene mreže, aplikacije, igrice, e-mail ili druge digitalne platforme, često ostavljaš određene tragove o sebi. Ti tragovi mogu biti tvoji lični podaci.

Lični podaci su sve informacije koje mogu otkriti ko si, gdje živiš, gdje se krećeš ili kako neko može da stupi u kontakt sa tobom. To mogu biti: ime i prezime, adresa stanovanja, broj telefona, e-mail adresa, fotografije, škola koju pohađaš, korisničko ime, lozinka, kao i tvoja trenutna ili česta lokacija.

Važno je da znaš da lični podaci nijesu bezazleni. Ako ih dijeliš javno ili sa nepoznatim osobama, neko ih može zloupotrijebiti. Na primjer, neko može koristiti tvoje fotografije bez dozvole, lažno se predstaviti, kontaktirati te na neprijatan način ili pokušati da dođe do tvojih naloga. Zato je važno da prije svake objave razmisliš: **da li je ovo nešto što zaista želim da svi vide?**

Problem:
Mnogi mladi nesvjesno dijele lične podatke. To se često dešava kroz fotografije, storije, objave iz škole, označavanje lokacije, javne profile ili komunikaciju sa osobama koje ne poznaju dovoljno. Nekada i obična fotografija može otkriti više nego što mislimo — ime škole, ulicu, mjesto gdje se često boravi ili osobe sa kojima se družimo.

Savjeti za zaštitu privatnosti:

Ne dijeli lične podatke sa nepoznatim osobama, posebno adresu, broj telefona, lozinke, fotografije dokumenata ili informacije o tome gdje se trenutno nalaziš.

Provjeri podešavanja privatnosti na društvenim mrežama i vidi ko može da gleda tvoje objave, fotografije, storije i listu prijatelja.

Isključi javno prikazivanje lokacije, posebno kada objavljuješ fotografije ili storije u realnom vremenu.

Ne prihvataj zahtjeve za prijateljstvo od osoba koje ne poznaješ ili koje nemaju jasne i pouzdane profile.

Dobro razmisli prije nego što objaviš fotografiju sebe ili druge osobe. Tuđe fotografije ne treba dijeliti bez dozvole.

Zapamti:
Tvoji lični podaci su vrijedni. Čuvajući njih, čuvaš svoju privatnost, sigurnost i kontrolu nad tim kako se predstavljaš u digitalnom svijetu.

4. DIGITALNA BEZBJEDNOST – OSNOVE

Digitalna bezbjednost znači da znaš kako da zaštitiš sebe, svoje podatke, naloge i uređaje dok koristiš internet. Kao što u stvarnom životu zaključavamo vrata, čuvamo lična dokumenta i pazimo kome vjerujemo, tako i u digitalnom prostoru treba da imamo navike koje nas štite od rizika.

Kada govorimo o digitalnoj bezbjednosti, najčešće mislimo na zaštitu **tvojih podataka**, **tvojih naloga** i **tvojih uređaja**. Podaci su informacije koje dijeliš ili čuvaš online, kao što su ime, fotografije, poruke, lozinke ili broj telefona. Nalozi su tvoji profili na društvenim mrežama, e-mail, aplikacije za komunikaciju, igrice ili platforme za učenje. Uređaji su telefon, tablet, računar ili laptop koje koristiš svakog dana.

Najčešći rizici u digitalnom prostoru su **hakovanje naloga**, **krađa identiteta** i **prevare**. Hakovanje naloga se dešava kada neko neovlašćeno pristupi tvom profilu, e-mailu ili aplikaciji. Krađa identiteta znači da se neko može lažno predstaviti kao ti, koristiti tvoje fotografije, ime ili podatke. Prevare se često pojavljuju kroz lažne poruke, nagradne igre, sumnjive linkove, lažne profile ili ponude koje izgledaju predobro da bi bile istinite.

Zato je važno da budeš pažljiv/a kada dobiješ poruku od nepoznate osobe, link koji traži da se hitno prijaviš ili ponudu koja obećava poklon, novac, besplatne igrice ili druge pogodnosti. Prevaranti često pokušavaju da izazovu radoznalost, strah ili žurbu kako bi te naveli da klikneš, uneseš lozinku ili podijeliš lične podatke.

Osnovna pravila digitalne bezbjednosti:

Ne klikći sumnjive linkove, posebno ako dolaze od nepoznatih osoba ili ako poruka izgleda neobično, hitno ili previše primamljivo.

Ne otvaraj nepoznate poruke i priloge, jer mogu sadržati štetan sadržaj, lažne zahtjeve ili pokušaje krađe podataka.

Koristi sigurnu Wi-Fi mrežu. Izbjegavaj prijavljivanje na važne naloge preko javnih i nepoznatih mreža, posebno ako unosiš lozinke ili druge osjetljive podatke.

Redovno ažuriraj telefon, računar i aplikacije, jer ažuriranja često popravljaju bezbjednosne propuste.

Koristi jake lozinke i nemoj istu lozinku koristiti za više naloga. Lozinku ne dijeli ni sa prijateljima.

Zapamti:
Digitalna bezbjednost počinje oprezom. Prije nego što klikneš, otvoriš poruku ili uneseš podatke, zastani i razmisli da li je izvor pouzdan. Jedna pažljiva odluka može spriječiti veliki problem.

5. LOZINKE I ZAŠTITA NALOGA

Lozinka je prva linija odbrane tvog digitalnog života. Ona štiti tvoje naloge na društvenim mrežama, e-mail, aplikacije za dopisivanje, igrice, školske platforme i druge servise koje koristiš svakog dana. Ako neko sazna tvoju lozinku, može pristupiti tvom profilu, čitati poruke, objavljivati sadržaj u tvoje ime, mijenjati podatke ili pokušati da prevari druge osobe predstavljajući se kao ti.

Zato lozinku ne treba posmatrati kao običnu riječ koju brzo zapamtimo, već kao ključ koji čuva tvoju privatnost i sigurnost. Kao što ne bi dao/la ključ od kuće nepoznatoj osobi, tako ne treba dijeliti ni lozinku, čak ni sa prijateljima. Lozinka treba da bude samo tvoja.

Loše lozinke su one koje je lako pogoditi. Na primjer:
123456, **password**, tvoje ime, nadimak, datum rođenja, ime kućnog ljubimca ili kombinacija **ime + godina**. Takve lozinke su nesigurne jer ih neko može brzo pretpostaviti, posebno ako te poznaje ili ako su tvoji podaci javno dostupni na društvenim mrežama.

Dobra lozinka treba da bude dovoljno duga i složena. Najbolje je da sadrži kombinaciju velikih i malih slova, brojeva i simbola. Preporučuje se da ima najmanje **8–12 karaktera**, a još bolje je ako je duža. Na primjer, umjesto kratke i očigledne lozinke, bolje je koristiti rečenicu ili kombinaciju riječi koju samo ti možeš povezati, uz dodavanje brojeva i znakova.

Važno je i da ne koristiš istu lozinku za sve naloge. Ako neko otkrije jednu lozinku, može pokušati da je upotrijebi i na drugim profilima. Zato je pametno da za važne naloge — kao što su e-mail, društvene mreže i školske platforme — koristiš različite lozinke.

DODATNO:
Koristi **dvofaktorsku autentifikaciju — 2FA** kad god je dostupna. To je dodatni nivo zaštite koji, osim lozinke, traži još jednu potvrdu da si to zaista ti. Na primjer, aplikacija ili platforma može poslati kod na telefon, e-mail ili posebnu aplikaciju za potvrdu identiteta. Čak i ako neko sazna tvoju lozinku, bez tog dodatnog koda teže će pristupiti tvom nalogu.

Osnovna pravila za zaštitu naloga:

Ne dijeli lozinku ni sa kim.

Ne koristi istu lozinku za više naloga.

Ne čuvaj lozinku na papirićima, javnim računarima ili u porukama.

Promijeni lozinku ako posumnjaš da je neko zna.

Uključi 2FA za važne naloge.

Zapamti:
Jaka lozinka i dodatna zaštita naloga čuvaju tvoje poruke, fotografije, podatke i digitalni identitet. Dobra lozinka nije ona koju je najlakše zapamtiti, već ona koju je drugima teško pogoditi.

6. DRUŠTVENE MREŽE – RIZICI

Društvene mreže su važan dio svakodnevnog života mladih. Koristimo ih za komunikaciju, druženje, informisanje, zabavu, praćenje sadržaja koji nas zanimaju i dijeljenje fotografija, video zapisa i mišljenja. One mogu biti koristan prostor za povezivanje, kreativnost i učenje, ali istovremeno nose i određene rizike ako ih koristimo bez opreza.

Jedan od najčešćih problema je **dijeljenje previše informacija**. Mladi često objavljuju fotografije, lokacije, informacije o školi, mjestu boravka, planovima, prijateljima ili porodici, ne razmišljajući ko sve to može vidjeti. Čak i kada objava izgleda bezazleno, ona može otkriti mnogo podataka o tebi. Na primjer, fotografija ispred škole, označena lokacija ili objava iz kuće mogu otkriti gdje se nalaziš, kuda se krećeš i sa kim provodiš vrijeme.

Drugi rizik je **kontakt sa nepoznatim osobama**. Na društvenim mrežama nije uvijek lako znati ko se zaista nalazi iza nekog profila. Neki profili mogu biti lažni, a osobe se mogu predstavljati drugačije nego što jesu. Zato je važno da ne prihvataš zahtjeve za prijateljstvo ili praćenje od osoba koje ne poznaješ u stvarnom životu ili za koje nijesi siguran/na ko su. Posebno treba biti oprezan ako nepoznata osoba traži tvoje lične podatke, fotografije, susret uživo ili pokušava da te nagovori na nešto što ti nije prijatno.

Društvene mreže mogu stvoriti i **pritisak**. Mladi se često porede sa drugima, prate broj lajkova, komentara i pregleda, ili osjećaju potrebu da stalno budu online. To može uticati na samopouzdanje, raspoloženje, koncentraciju i odnos prema sebi. Važno je znati da ono što vidimo na društvenim mrežama često nije cijela stvarnost. Ljudi uglavnom objavljuju samo odabrane trenutke, uređene fotografije i sadržaje koji ne prikazuju sve probleme, emocije i svakodnevni život.

Još jedan problem može biti **prekomjerno korišćenje društvenih mreža**. Ako stalno provjeravaš telefon, teško se odvajaš od aplikacija, zapostavljaš učenje, san, druženje uživo ili

druge obaveze, to može biti znak da treba napraviti pauzu i postaviti granice. Društvene mreže treba da služe tebi, a ne da ti oduzimaju kontrolu nad vremenom i pažnjom.

Pravila za sigurnije korišćenje društvenih mreža:

Profil neka bude privatan. Tako bolje kontrolišeš ko može da vidi tvoje objave, fotografije, storije i lične informacije.

Prihvataj samo osobe koje poznaješ. Ne moraš prihvatiti svaki zahtjev za prijateljstvo ili praćenje.

Razmisli prije nego što objaviš. Zapitaj se: da li bih želio/željela da ovu objavu vidi nastavnik, roditelj, budući poslodavac ili osoba koju ne poznajem?

Ne dijeli lokaciju u realnom vremenu, posebno ako si sam/a ili na mjestu gdje često boraviš.

Ne odgovaraj na poruke koje te uznemiravaju, plaše ili traže nešto neprijatno. Sačuvaj dokaz, blokiraj osobu i obrati se osobi od povjerenja.

Zapamti:
Društvene mreže mogu biti korisne i zabavne, ali je važno da ih koristiš pažljivo. Tvoj profil, tvoje fotografije, tvoje vrijeme i tvoji podaci pripadaju tebi. Prije svake objave, zahtjeva ili poruke — zastani, razmisli i zaštiti sebe.

7. DIGITALNO NASILJE

Digitalno nasilje je svako ponašanje na internetu kojim se druga osoba vrijeđa, ponižava, zastrašuje, ucjenjuje ili namjerno povređuje. Može se dešavati na društvenim mrežama, u grupnim četovima, komentarima, privatnim porukama, tokom igranja online igrica, preko e-maila ili bilo koje digitalne platforme.

Digitalno nasilje može uključivati **vrijeđanje**, **prijetnje**, **širenje laži**, ismijavanje, slanje neprijatnih poruka, isključivanje iz grupa, lažno predstavljanje, dijeljenje privatnih fotografija ili objavljivanje sadržaja bez dozvole osobe na koju se odnosi. Nekada se nasilje dešava javno, pred većim brojem ljudi, a nekada kroz privatne poruke. U oba slučaja, ono može ozbiljno uticati na osobu koja ga doživljava.

Važno je da znaš da digitalno nasilje nije šala ako nekoga povređuje, plaši ili ponižava. Čak i kada neko kaže „samo sam se šalio/la“, odgovornost postoji ako je druga osoba uznemirena ili povrijeđena. Internet ne smije biti prostor u kojem se vrijeđanje, prijetnje i ponižavanje smatraju normalnim ponašanjem.

VAŽNO:
Digitalno nasilje nije „normalno ponašanje“ – to je nasilje. Niko nema pravo da te vrijeđa, zastrašuje, ucjenjuje, širi neistine o tebi ili objavljuje tvoje fotografije, poruke i druge sadržaje bez tvoje dozvole. Ako se to desi, nijesi kriv/a i imaš pravo da potražiš pomoć.

KAKO REAGOVATI:

Ne odgovaraj agresivno.
Kada dobiješ uvredljivu ili prijeteću poruku, prirodno je da se uznemiriš ili poželiš da odmah odgovoriš. Ipak, agresivan odgovor često može pogoršati situaciju. Najbolje je da zastaneš, ne ulaziš u raspravu i ne šalješ poruke zbog kojih bi kasnije mogao/la imati problem.

Sačuvaj dokaze.
Nemoj odmah brisati poruke, komentare, profile ili objave. Napravi screenshot, sačuvaj link, datum, vrijeme i ime profila sa kojeg je sadržaj poslat. Dokazi mogu biti važni ako budeš prijavljivao/la nasilje roditeljima, školi, platformi ili nadležnim institucijama.

Blokiraj osobu.
Ako te neko uznemirava, vrijeđa ili ti šalje neprijatne poruke, imaš pravo da ga blokiraš. Blokiranje nije slabost, već način da zaštitiš sebe i prekineš kontakt sa osobom koja se ponaša nasilno.

Prijavi sadržaj.
Društvene mreže i aplikacije imaju opcije za prijavu uvredljivog, prijetećeg ili neprimjerenog sadržaja. Prijavi poruku, komentar, profil ili objavu. Ako se nasilje nastavi, obrati se osobi od povjerenja — roditelju, nastavniku, pedagogu, psihologu, omladinskom radniku ili drugoj odrasloj osobi.

Zapamti:
Nasilje na internetu nije tvoja krivica. Ne moraš sam/a da rješavaš problem. Najvažnije je da ne ćutiš, da sačuvaš dokaze i da se obratiš nekome ko ti može pomoći. Siguran digitalni prostor počinje time što prepoznajemo nasilje, reagujemo na vrijeme i štitimo sebe i druge.

8. LAŽNE VIJESTI I DEZINFORMACIJE

Lažne vijesti i dezinformacije su netačne, nepotpune ili namjerno pogrešno predstavljene informacije koje se šire putem interneta, društvenih mreža, portala, poruka, video snimaka ili fotografija. One mogu izgledati kao prave vijesti, ali njihov cilj često nije da informišu, već da zbune, uplaše, izazovu jaku reakciju, povećaju broj klikova ili utiču na mišljenje ljudi.

Važno je da znaš da nije sve što vidiš na internetu tačno. Neke informacije mogu biti slučajno pogrešne, jer osoba koja ih dijeli nije provjerila podatke. Međutim, dezinformacije se često šire namjerno, kako bi se ljudi naveli da povjeruju u nešto što nije istina. Zbog toga je važno da ne vjerujemo odmah svemu što pročitamo, posebno ako vijest djeluje šokantno, previše dramatično ili izaziva strah i ljutnju.

Lažne vijesti se često mogu prepoznati po **senzacionalnim naslovima**. To su naslovi koji koriste riječi poput: „šokantno“, „nevjerovatno“, „ovo kriju od vas“, „hitno“, „svi moraju znati“ i slično. Njihov cilj je da te natjeraju da odmah klikneš, bez razmišljanja. Naslov može biti dramatičan, a tekst ispod njega često nema dovoljno dokaza ili ne potvrđuje ono što naslov tvrdi.

Drugi znak opreza su **nepoznati izvori**. Ako ne znaš ko je objavio informaciju, ko je autor teksta ili da li je portal pouzdan, treba biti pažljiv. Pouzdani mediji obično imaju jasno navedene autore, izvore, datum objave i kontakt podatke. Ako tekst nema autora, nema izvore ili dolazi sa stranice koja izgleda neprofesionalno, moguće je da informacija nije provjerena.

Treći znak su informacije koje **nemaju dokaze**. Ako neko tvrdi nešto ozbiljno, a ne navodi dokumente, izjave, zvanične podatke, fotografije, video dokaze ili pouzdane izvore, ne treba odmah vjerovati takvoj objavi. Takođe, treba biti oprezan sa fotografijama i video snimcima, jer se oni mogu izvući iz konteksta, montirati ili prikazati kao da su nastali na drugom mjestu ili u drugo vrijeme.

Kako provjeriti informaciju:

Provjeri više izvora. Ako je informacija važna, pogledaj da li su je objavili i drugi pouzdani mediji ili zvanične institucije.

Koristi pouzdane portale i izvore. Prednost daj medijima koji navode autore, izvore, datum objave i dokaze za ono što tvrde.

Ne dijeli odmah. Prije nego što podijeliš vijest, zastani i razmisli: da li znam ko je objavio ovu informaciju, da li postoje dokazi i da li je možda riječ o manipulaciji?

Provjeri datum objave. Nekada se stare vijesti ponovo dijele kao da su nove, što može stvoriti pogrešan utisak.

Obrati pažnju na emocije. Ako te neka objava odmah naljuti, uplaši ili šokira, to može biti znak da je napravljena da izazove brzu reakciju.

Zapamti:
Dijeljenjem neprovjerenih informacija možeš nesvjesno pomoći širenju laži. Zato je važno da prije svakog dijeljenja provjeriš izvor, sadržaj i dokaze. Pametno korišćenje interneta znači da ne budeš samo čitalac, već i odgovoran korisnik koji razmišlja prije nego što povjeruje i podijeli informaciju.

9. KAKO SE ZAŠTITITI – PRAKTIČNI SAVJETI

Zaštita na internetu počinje svakodnevnim navikama. Nije potrebno biti stručnjak za tehnologiju da bi koristio/la internet sigurnije. Dovoljno je da znaš osnovna pravila, da budeš pažljiv/a i da razmisliš prije nego što klikneš, objaviš, podijeliš informaciju ili odgovoriš na poruku.

Prvi korak je korišćenje **jakih lozinki**. Lozinka treba da bude dovoljno duga i da sadrži kombinaciju slova, brojeva i simbola. Izbjegavaj jednostavne lozinke kao što su datum rođenja, ime, nadimak ili „123456“. Takođe, nemoj koristiti istu lozinku za sve naloge, jer ako neko otkrije jednu lozinku, može pokušati da uđe i na druge profile.

Drugi važan korak je uključivanje **dvofaktorske autentifikacije — 2FA**. To znači da, osim lozinke, moraš potvrditi svoj identitet dodatnim kodom ili obavještenjem. Na taj način tvoj nalog je sigurniji čak i ako neko sazna lozinku.

Veoma je važno da **ne dijeliš lične podatke** sa nepoznatim osobama. Adresa, broj telefona, lozinke, lokacija, fotografije dokumenata i privatne poruke ne treba da budu dostupni svima. Prije nego što nešto pošalješ ili objaviš, razmisli da li bi taj podatak mogao biti zloupotrijebljen.

Sigurno korišćenje interneta podrazumijeva i da **provjeravaš informacije**. Ne vjeruj odmah svemu što vidiš na društvenim mrežama ili portalima. Provjeri ko je objavio informaciju, da li

postoje dokazi i da li istu vijest prenose pouzdani izvori. Lažne vijesti se često šire brzo, ali ih možeš zaustaviti tako što ih nećeš dijeliti bez provjere.

Ako naiđeš na vrijeđanje, prijetnje, lažne profile, uznemiravanje ili objavljivanje sadržaja bez dozvole, važno je da **prijaviš nasilje**. Sačuvaj dokaze, blokiraj osobu i obrati se nekome kome vjeruješ — roditelju, nastavniku, pedagogu, psihologu ili drugoj odrasloj osobi.

Na kraju, najvažnije pravilo je: **razmisli prije objave**. Internet pamti. Ono što danas objaviš može ostati dostupno i kasnije, čak i ako ga obrišeš. Zato se prije svake objave zapitaj: da li je ovo tačno, bezbjedno, pristojno i potrebno?

Zapamti:
Pametno ponašanje na internetu štiti tvoju privatnost, tvoje naloge, tvoje podatke i tvoj ugled. Svaka pažljiva odluka doprinosi sigurnijem digitalnom prostoru za tebe i za druge.

10. GDJE POTRAŽITI POMOĆ

Ako se na internetu dogodi nešto što te uznemiri, uplaši ili povrijedi, važno je da znaš da ne moraš sam/a da rješavaš problem. Digitalni prostor može djelovati zbunjujuće, posebno kada se neprijatna situacija desi brzo — kroz poruku, komentar, objavu, lažni profil, prijetnju ili dijeljenje sadržaja bez dozvole. U takvim trenucima najvažnije je da ne ćutiš i da se obratiš osobi, instituciji ili službi koja ti može pomoći.

Prva osoba kojoj se možeš obratiti može biti **roditelj ili staratelj**. Roditelji su tu da te zaštite i podrže, čak i ako se plašiš da ćeš biti kritikovan/a zbog nečega što se desilo online. Važno je da im objasniš šta se dogodilo, pokažeš poruke, objave ili profil koji te uznemirava i kažeš kako se osjećaš.

Pomoć možeš potražiti i od **nastavnika, razrednog starješine, pedagoga ili psihologa u školi**. Škola ima važnu ulogu u zaštiti učenika, posebno ako se problem dešava među vršnjacima ili utiče na tvoju sigurnost, učenje i svakodnevni život. Razgovor sa odraslom osobom u školi može pomoći da se problem zaustavi i da dobiješ podršku.

Ako je riječ o ozbiljnoj prijetnji, ucjeni, krađi identiteta, širenju privatnih fotografija, lažnom predstavljanju ili drugom obliku ugrožavanja sigurnosti, potrebno je obratiti se **policiji**. U takvim situacijama važno je sačuvati dokaze: poruke, komentare, linkove, screenshotove, datume, vrijeme i naziv profila sa kojeg je sadržaj poslat.

U slučaju računarsko-bezbjednosnih incidenata, zloupotreba naloga, sumnjivih linkova, sajber napada, pokušaja krađe podataka ili drugih ozbiljnih problema u digitalnom prostoru, važno je znati da postoji i **CIRT državne uprave**. CIRT je zadužen za odgovor na računarsko-bezbjednosne incidente u sajber prostoru i može imati važnu ulogu u prepoznavanju, prijavljivanju i rješavanju ozbiljnih sajber prijetnji. https://cirt.gov.me/

Problem možeš prijaviti i samoj **platformi** na kojoj se dogodio — Instagramu, TikToku, Facebooku, YouTubeu ili drugoj aplikaciji. Većina platformi ima opcije za prijavu profila, komentara, poruke, fotografije ili video snimka. Takođe, možeš blokirati osobu koja te uznemirava i podesiti privatnost profila kako bi smanjio/la rizik od daljeg kontakta.

VAŽNO:
Nijesi sam/a. Ako se suočiš sa problemom na internetu, potraži pomoć na vrijeme. Razgovor sa osobom od povjerenja nije slabost, već odgovoran korak da zaštitiš sebe i druge. Internet treba da bude prostor komunikacije, učenja i podrške, a ne mjesto straha, pritiska ili nasilja.

11. PREPORUKE ZA MLADE

Internet je prostor koji mladima pruža mnogo mogućnosti — za učenje, komunikaciju, kreativnost, zabavu i povezivanje sa drugima. Ipak, da bi korišćenje interneta bilo korisno i sigurno, važno je razvijati dobre digitalne navike. To znači da internet treba koristiti pametno, odgovorno i svjesno, uz razumijevanje da svaka objava, poruka, komentar ili dijeljenje sadržaja može imati posljedice.

Prva preporuka je da **koristiš internet pametno**. Prije nego što klikneš na link, objaviš fotografiju, prihvatiš zahtjev za prijateljstvo ili odgovoriš na poruku, zastani i razmisli. Pitaj sebe: da li je ovo bezbjedno, da li je potrebno, da li može nekoga povrijediti i da li bih isto uradio/la i u stvarnom životu? Pametno korišćenje interneta znači da imaš kontrolu nad svojim ponašanjem online.

Važno je i da se **informišeš iz pouzdanih izvora**. Ne treba vjerovati svakoj objavi, komentaru, videu ili naslovu koji vidiš na internetu. Lažne vijesti i dezinformacije mogu se brzo širiti, posebno na društvenim mrežama. Zato provjeri ko je objavio informaciju, da li postoje dokazi, datum objave i da li istu vijest prenose drugi pouzdani izvori.

Posebno treba da **štitiš svoju privatnost**. Ne dijeli lične podatke sa nepoznatim osobama i vodi računa ko može da vidi tvoje objave, fotografije i storije. Adresa, broj telefona, lozinke, lokacija i privatne poruke nijesu informacije koje treba da budu dostupne svima. Tvoja privatnost je važna i imaš pravo da je čuvaš.

Ako primijetiš da je neko drugi ugrožen, važno je da **pomogneš**. To ne znači da treba sam/a da rješavaš problem, već da možeš pružiti podršku, ne širiti uvredljiv sadržaj, sačuvati dokaze i ohrabriti osobu da se obrati roditelju, nastavniku, školi, policiji, platformi ili drugoj službi podrške.

Na kraju, nastavi da **učiš o digitalnoj bezbjednosti**. Internet se stalno mijenja, a sa njim se mijenjaju i rizici. Što više znaš o zaštiti naloga, privatnosti, prepoznavanju prevara, digitalnom nasilju i provjeri informacija, to ćeš sigurnije koristiti digitalni prostor.

Zapamti:
Siguran internet počinje odgovornim korisnicima. Svaka tvoja pametna odluka doprinosi boljem, sigurnijem i podržavajućem digitalnom okruženju za tebe i druge.

12. ZAKLJUČAK

Internet je moćan alat koji mladima pruža mnogo mogućnosti. Pomoću njega možeš da učiš, komuniciraš, istražuješ, stvaraš, zabavljaš se, pokrećeš dobre ideje i povezuješ se sa ljudima iz različitih sredina. Digitalni prostor može biti mjesto znanja, kreativnosti, podrške i razvoja. Međutim, internet je koristan i siguran samo onda kada ga koristiš odgovorno, pažljivo i svjesno.

Odgovorno korišćenje interneta znači da znaš svoja prava, ali i da poštuješ prava drugih. Imaš pravo na privatnost, zaštitu ličnih podataka, slobodu izražavanja i sigurnost u digitalnom prostoru. Istovremeno, važno je da i ti svojim ponašanjem ne ugrožavaš druge — da ne dijeliš tuđe podatke bez dozvole, ne širiš uvrede, ne učestvuješ u nasilju i ne dijeliš neprovjerene informacije.

Znanje o digitalnim pravima i bezbjednosti pomaže ti da prepoznaš rizike i da reaguješ na vrijeme. Kada znaš kako da zaštitiš lozinku, kako da podesiš privatnost, kako da prepoznaš lažne

vijesti, kako da reaguješ na digitalno nasilje i kome da se obratiš za pomoć, internet koristiš sigurnije i sa više samopouzdanja.

Takvo znanje **štiti tebe**, jer čuva tvoje podatke, naloge, privatnost, ugled i osjećaj sigurnosti. Ono **štiti druge**, jer te uči da poštuješ tuđe granice, da ne širiš štetan sadržaj i da pružiš podršku kada je neko ugrožen. Na kraju, ono **čini internet boljim mjestom**, jer svaki odgovoran korisnik doprinosi sigurnijem, pravednijem i korisnijem digitalnom prostoru.

Važno je zapamtiti da sigurnost na internetu nije jednokratna odluka, već svakodnevna navika. Svaki put kada razmisliš prije objave, provjeriš informaciju, ne klikneš na sumnjiv link, prijaviš nasilje ili pomogneš nekome ko ima problem, ti doprinosiš bezbjednijem internetu.

Zaključna poruka:
Internet može biti prostor velikih mogućnosti, ali njegova vrijednost zavisi od načina na koji ga koristimo. Koristi ga pametno, štiti sebe, poštuj druge i nastavi da učiš. Digitalna bezbjednost počinje znanjem, a bolji internet počinje odgovornim ponašanjem svakog od nas.