DIGICITY

Sufinansira Evropska unija

GAME-BASED DIGITAL CITIZENSHIP

Vodič za razvijanje veština digitalnog građanstva

LogoPsyCom PENS digiQ YuzuPulse

Ovaj vodič je deo materijala za **projektat DigiCity**.

Saznaj više o projektu na vebsajtu: **https://projectdigicity.eu/**

Rukovodilac projekta

Omladinski savez udruženja ‘OPENS’ (Srbija)

Organizacije koje učestvuju

Digitalna Inteligencia (Slovačka)

YuzuPulse (Francuska)

Logopsycom (Belgija)

Sadržaj

I. UVOD

U današnjem povezanom svetu, digitalni prostor je jednako važan deo naših života kao i fizički. Od društvenih mreža do obrazovnih izvora, internet nudi beskrajne mogućnosti za povezivanje, učenje i kreativnost. Međutim, snalaženje u tom ogromnom i dinamičnom prostoru zahteva ne samo tehničke veštine, već i skup vrednosti, ponašanja i znanja koji se kolektivno naziva digitalnim građanstvom.

Svrha ovog vodiča je da mlade nauči najvažnijim veštinama digitalnog građanstva i da im omogući da odgovorno, etički i efikasno učestvuju u digitalnom svetu. Obrađuje ključne teme kao što su onlajn privatnost, odgovorno korišćenje društvenih mreža, dezinformacije i kako ih prepoznati, i šta je digitalni otisak. To nisu samo veštine već životne lekcije koje će pomoći mladima da napreduju u digitalnom društvu.

Zašto smo napisali ovaj vodič?

Vodič za veštine digitalnog građanstva služi kao osnovni stub za osposobljavanje informisanih i odgovornih digitalnih građana. Na sistematičan način daje pregled najvažnijih aspekata digitalnog građanstva koje treneri i omladinske organizacije treba da usvoje. Kroz sveobuhvatan pristup temama kao što su onlajn privatnost, odgovorno korišćenje društvenih mreža i prepoznavanje dezinformacija, ovaj vodič daje trenerima i edukatorima znanje neophodno za efikasno obrazovanje mladih.

Kroz praktične savete i inkluzivne aktivnosti, vodič naglašava važnost kritičkog mišljenja, etičkog ponašanja i odgovorne digitalne komunikacije. Uspostavlja teorijski okvir kroz definisanje ključnih koncepata i pruža strategije koje se mogu preduzeti da bi se načela digitalnog građanstva integrisala u obrazovne prakse.

Zašto je digitalno građanstvo važno?

Internet je moćan alat, ali dolazi sa izazovima. Mladi se često susreću sa problemima poput digitalnog nasilja, dezinformacija, povrede privatnosti i dugoročnih implikacija njihovih onlajn akcija. Bez odgovarajućeg vođenja, ti izazovi mogu loše uticati ne samo na njihov privatni, već i na akademski i profesionalni razvoj.

Ovaj vodič ima za cilj da premosti taj jaz nudeći praktične savete i zanimljive aktivnosti koje su dostupne svima. Stavljajući fokus na kritičko mišljenje, etičko ponašanje i odgovornu komunikaciju, vodič ima svrhu da pomogne mladima da donesu informisane odluke i da razvijaju pozitivne interakcije u digitalnim prostorima.

Za koga je ovaj vodič?

- **Mlade**: Da im pomogne da steknu samopouzdanje da se kreću kroz digitalni svet bezbedno i odgovorno.
- **Edukatore i trenere**: Da im da alate i strategije u pružanju podrške mladima kada je reč o razvijanju veština digitalnog građanstva.
- **Omladinskim organizacijama** : Da poboljša obrazovne prakse integrisanjem načela digitalnog građanstva u njihove programe.

Šta možeš da očekuješ?

Vodič je strukturiran u jasna poglavlja prilagođena različitim čitaocima i svako od njih se fokusira da jedan ključan aspekt digitalnog građanstva:

- **Kako razumeti digitalno građanstvo**: Uvod u načela i vrednosti koji definišu odgovorno učešće u digitalnom svetu.
- **Digitalne kompetencije: osnovne veštine** : Pregled osnovnih veština koje su potrebne za efikasnu i bezbednu digitalnu komunikaciju.

- **Medijska pismenost:** Kako razumeti, prepoznati i upravljati dezinformacijama; alati i strategije za identifikovanje proverenih izvora i izbegavanje širenja lažnih informacija.
- **Odgovorna upotreba društvenih mreža:** Rizici, dobre strane i onlajn ugled – uvid u to kako odgovorno koristiti društvene mreže i napraviti balans između prednosti koje nude i mogućih rizika.
- **Kako razumeti digitalni otisak i kako upravljati njime**: Vodič o tome kako onlajn aktivnosti oblikuju lični ugled i prilike u budućnosti; praktični saveti za zaštitu ličnih informacija i upravljanje podešavanjima za privatnost.
- **Glosar**: Odeljak koji definiše ključne termine i koncepte koji su povezani sa digitalnim građanstvom.

Svako poglavlje ima korisne savete, primere iz svakodnevnog života i inkluzivne aktivnosti kako bi zainteresovalo učenike različitih profila. Vodič je napravljen da bude i edukativan i praktičan, trudeći se da učini načela digitalnog građanstva primenljivim u svakodnevnom kontekstu.

Šta želimo da postignemo?

Ovaj vodič je više od obrazovnog alata; predstavlja posvećenost da se podrži generacija pažljivih, etičkih i odgovornih digitalnih građana. Zajedno možemo da kreiramo bezbednije i inkluzivnije digitalno okruženje gde svi imamo priliku da učimo, razvijamo se i povezujemo.

Hajde da se otisnemo na ovo putovanje ka digitalnom građanstvu i omogućimo mladima da postanu lideri u digitalnoj eri.

II. KAKO RAZUMETI DIGITALNO GRAĐANSTVO

Digitalno građanstvo se odnosi na odgovornu i odgovarajuću upotrebu tehnologija od strane svih koji imaju interakciju sa digitalnim okruženjem. Obuhvata različite načine ponašanja, veštine i znanje kao što su zaštita ličnih podataka, komunikaciju sa poštovanjem i pozitivan doprinos onlajn zajednicama koji su neophodni za bezbedan i efikasan boravak u digitalnom svetu.

Koncept digitalnog građanstva je ključan u današnjem povezanom svetu, gde su digitalne interakcije važan deo svakodnevice. Digitalno građanstvo može značajno da utiče na tvoje onlajn ponašanje na nekoliko načina, na primer tako što će te podstaći da se ponašaš odgovorno u onlajn okruženju i komuniciraš uvažavajući sagovornike. Veća je šansa da će se onlajn korisnici uključiti u interakcije koje su ljubazne i uvažavaju druge, smanjujući na taj način primere digitalnog nasilja i onlajn uznemiravanja. Pored toga, omogućava etičko kreiranje i deljenje sadržaja kako više ljudi postaje svesno zakona o zaštiti autorskih prava i intelektualne svojine .

Sledeći načela digitalnog građanstva, postaješ svesniji kada je reč o zaštiti svoje privatnosti i učiš kako da upravljaš svojim digitalnim otiskom i zaštitiš lične podatke i time smanjiš rizik krađe identiteta i onlajn zloupotrebe . Digitalni građani su bolje opremljeni da prepoznaju i izbegnu onlajn prevare, dezinformacije i potencijalno štetan sadržaj.

S druge strane, obrazovanje u oblasti digitalnog građanstva poboljšava digitalnu pismenost razvijanjem veština kao što je kritičko razmišljanje. Kada naučiš kako da kritički proceniš informacije onlajn lakše ti je da doneseš informisane odluke.

Digitalno građanstvo promoviše i aktivno učešće u onlajn zajednicama. Veća je verovatnoća da ćeš se uključiti u pozitivni onlajn aktivizam, konstruktivno doprineti digitalnim zajednicama i razumeti uticaj onlajn aktivnosti. Podstiče empatiju i razumevanje za druge u digitalnim prostorima.

Prava i odgovornosti digitalnih građana

Jedno od osnovnih prava digitalnih građana je zaštita ličnih podataka. Opšta uredba o zaštiti podataka (poznatija po svojoj engleskog skraćenici GDPR), koju je Evropska unija sprovela 2018. godine, predstavlja važnu regulativu čiji je cilj zaštita privatnosti i ličnih podataka pojedinaca u okviru EU.

KLJUČNI ASPEKTI GDPR-A UKLJUČUJU:

Zaštitu podataka
Obezbeđuje da se lični podaci prikupljaju, obrađuju i čuvaju na bezbedan način.

Pravo na pristup
Pojedincima se omogućava pristup njihovim ličnim podacima i oni razumeju na koji način se koriste.

Saglasnost
Zahteva se jasna i eksplicitna saglasnost pojedinaca pre prikupljanja njihovih podataka.

Pravo na brisanje
Pojedincima se daje pravo da zatraže brisanje svojih ličnih podataka pod određenim uslovima.

GDPR postavlja visoke standarde zaštite i privatnosti, služi kao model za druge regije (uključujući i Zakon o zaštiti podataka o ličnosti Republike Srbije) i potvrđuje prava digitalnih građana.

Više informacija na stranici **GDPR.eu "What is GDPR, the EU's new data protection law?" (Wolford B, n.d.)**

Postoji nekoliko načina na koji ti kao digitalni građanin možeš da tražiš pomoć i podršku kada se suočiš sa problemima u onlajn okruženju:

- **Onlajn zajednice za podršku:** Priključivanje forumima i grupama u kojima pojedinci dele iskustva i savete o tome kako se nositi sa digitalnim izazovima.
- **Službe telefonske pomoći:** Korišćenje službi telefonske pomoći koje su namenjene problemima poput digitalnog nasilja, onlajn uznemiravanja ili digitalne zavisnosti.
- **Mehanizmi za prijavljivanje:** Korišćenje alata za prijavljivanje na društvenim mrežama i sajtovima da se označe neprikladni ili štetni komentari.
- **Obrazovni izvori:** Pristupanje onlajn kursevima i tutorijalima da bi se poboljšala digitalna pismenost i razumevanje digitalnih prava.

Informacije o dostupnim izvorima osnažuju te da se nosiš sa onlajn problemima i efikasno ih rešiš. Više informacija na **Find a Helpline**.

Poštovanje je temelj digitalnog građanstva. Kako bi doprineo onlajn okruženju gde se učesnici odnose s poštovanjem jedni prema drugima, trebalo bi uzeti u obzir:

Sledeći ova načela, doprinosiš pozitivnoj i uvažavajućoj digitalnoj zajednici.

Digitalni građani su odgovorni i za prepoznavanje diskriminacije i štetnog ponašanja onlajn i borbu protiv njih. To uključuje:

PREPOZNAVANJE DISKRIMINACIJE

Budi svestan pristrasnog sadržaja ili sadržaja sa predrasudama koji napadaju pojedince ili grupe na osnovu rase, roda, vere ili drugih karakteristika.

EDUKOVANJE DRUGIH

Radi na podizanju svesti o uticaju diskriminacije i promoviši inkluzivnost i raznolikost onlajn.

PRIJAVLJIVANJE ŠTETNOG SADRŽAJA

Koristi alate platformi koji služe za prijavljivanje i uklanjanje štetnog ili uvredljivog sadržaja.

PRUŽANJE PODRŠKE ŽRTVAMA

Pruži podršku i resurse pojedincima koji su iskusili diskriminaciju ili uznemiravanje onlajn.

Aktivnim suprotstavljanjem diskriminaciji i štetnom ponašanju, pomažeš u kreiranju sigurnijeg i pravednijeg digitalnog prostora za sve korisnike.

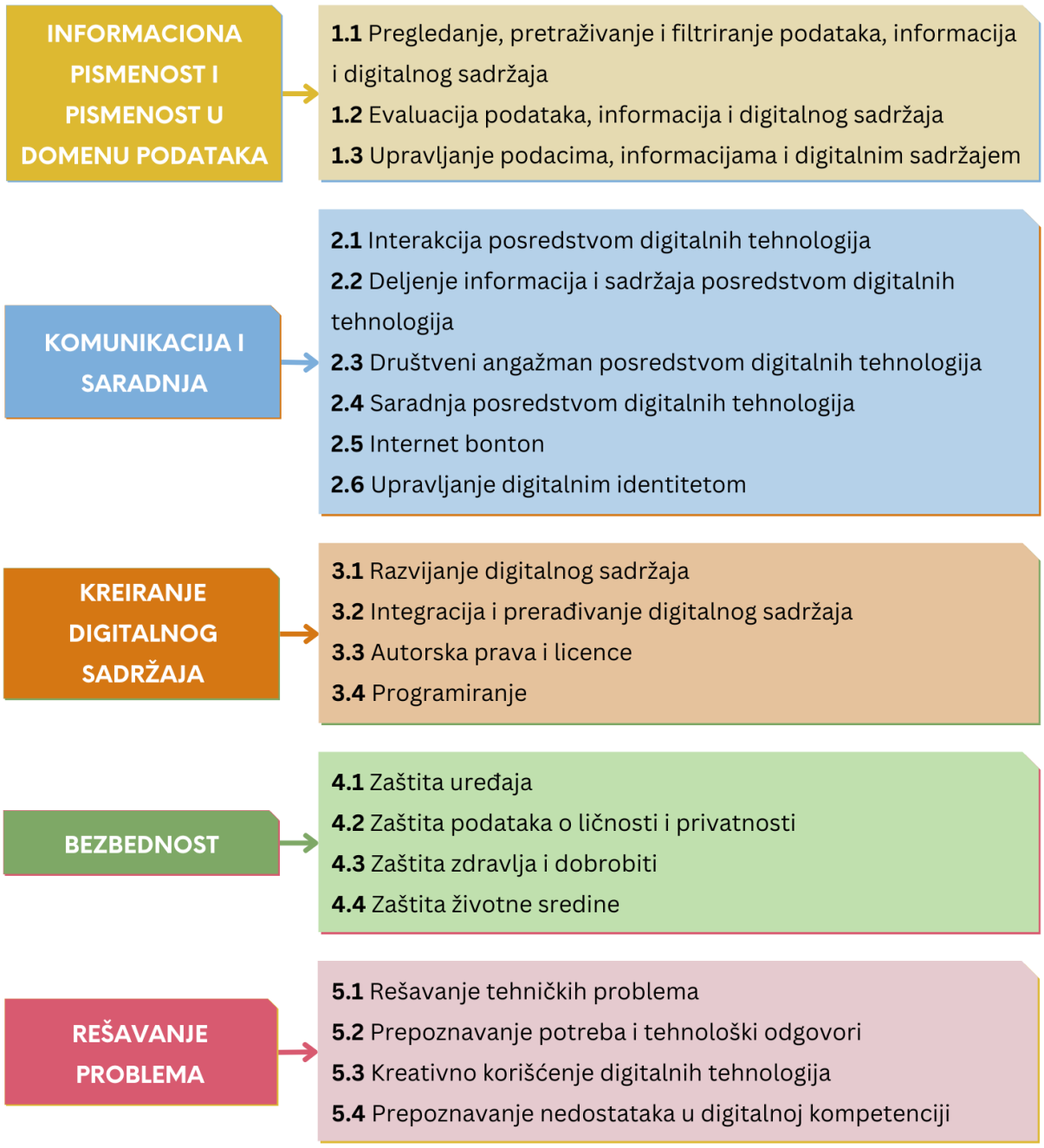
III. DIGITALNE KOMPETENCIJE – OSNOVNE VEŠTINE

Definicija digitalnih kompetencija

Definisane Okvirom digitalnih kompetencija za građane Evropske komisije (**DigComp**), digitalne kompetencije su suštinske za korišćenje digitalnih tehnologija na samopouzdan, kritičan i odgovoran način u različitim kontekstima, uključujući obrazovanje, zapošljavanje i lični život. Uključuju širok spektar veština, od osnovne računarske pismenosti do naprednih sposobnosti u digitalnom rešavanju problema i etičkom korišćenju tehnologije.

Okviri kao što su DigComp omogućavaju ti strukturni pristup u razumevanju višeznačne prirode digitalnih kompetencija. Naglašavaju važnost pristupačnosti, obezbeđujući time da su digitalne kompetencije inkluzivne i primenjive na sve građane, bez obzira na njihovo prethodno znanje ili sposobnosti.

Izvor: DigComp 2.2 - Okvir digitalnih kompetencija građana, Evropska komisija



Informaciona pismenost i kritičko razmišljanje

Pretraga informacija i upravljanje njima

Informaciona pismenost uključuje ne samo pretragu informacija, već i procenjivanje njihovog kvaliteta i značaja. Tehnike kao što su napredna pretraga, kritička procena rezultata pretrage i prepoznavanje verodostojnih izvora ključne su za snalaženje u ogromnom broju podataka koji su dostupni

onlajn. Alati poput **Google Scholar**, akademskih baza podataka i ugledne novinske kuće su primeri izvora koji se mogu koristiti za pouzdane informacije.

Pored toga, upravljanje informacijama obuhvata i znanje kako skladištiti, povratiti i zaštiti podatke. To uključuje korišćenje digitalnih alata za organizovanje informacija, kao što su rešenja za skladištenje na servisima „cloud“ i razumevanje načela za upravljanje podacima, kao što su konvencije o imenovanju fajlova i strategije za rezervne kopije. Uključuje je i prepoznavanje etičkih implikacija korišćenja podataka, kao što je poštovanje prava intelektualne svojine i prava na privatnost.

Procena izvora

Dezinformacija su česte u onlajn svetu, što znači da treba razviješ sposobnost da kritički proceniš izvore informacije na koje naiđeš. To uključuje preispitivanje autorovih kvalifikacija, tačnosti informacija i prisustvo bilo kakve pristrasnosti. Bočno (lateralno) čitanje, provera činjenica kod više izvora i korićenje alata kao što su sajtovi za proveru činjenica (npr. **Snopes**, **FactCheck.org**) su praktične strategije koje ti mogu pomoći u procesu procene.

Pored toga, važno je razumeti uticaj algoritama i personalizovane isporuke sadržaja, koji mogu iskriviti informacije koje ti se predstavljaju na osnovu tvog prethodnog ponašanja i preferencija. Informisanost o uticaju koji imaju algoritmi na tvoje informaciono okruženje može te osnažiti da potražiš različite perspektive i izbegneš efekat eho-komore.

Rešavanje problema i kritička procena

Rešavanje problema u digitalnim kontekstima nije samo tehničko, zahteva i način razmišljanja koji uključuje kritičku procenu i adaptivno razmišljanje. Veštine digitalnog rešavanja problema uključuju prepoznavanje digitalnih potreba, analiziranje mogućih rešenja i odabir najefikasnijih strategija. Na primer, kada se suočiš sa pretnjom po onlajn bezbednost, kao što je „pecanje“ (eng. phishing), treba da proceniš situaciju, prepoznaš pretnju i preduzmeš odgovarajuće korake da prijaviš incident i poboljšaš svoje mere bezbednosti.

Obrazovni pristupi koji obuhvataju digitalne simulacije, igranje uloga i aktivnosti interaktivnog rešavanja problema mogu da pomognu mladima da razviju te kompetencije na zanimljiv i praktičan način. Pružanjem scenarija iz stvarnog života koji zahtevaju kritičku procenu i donošenje odluka, edukatori mogu da bolje pripreme svoje učenike za kompleksnost digitalnog sveta.

Komunikacija i kreiranje sadržaj

Veštine digitalne komunikacije

Digitalna komunikacija je temelj digitalne kompetencije, uključujući veštine koje su potrebne za efikasnu interakciju u različitim onlajn sredinama. Osobe vešte u digitalnoj komunikaciji su sposobne da prilagode svoje poruke publici, odaberu odgovarajuće kanale za komunikaciju i da održe profesionalizam i poštovanje u svojim digitalnim interakcijama.

Usvajanje veština digitalne komunikacije uključuje istraživanje koncepta „netikecije“ (eng. netiquette), ili drugim rečima vodiča za ljubazno i učtivo ponašanje onlajn. Pored toga, uključuje i razgovore o digitalnom otisku i trajnosti onlajn aktivnosti, naglašavajući koliko je važno razmisliti pre objavljivanja i razumeti dugoročni uticaj digitalne komunikacije.

Onlajn alati za saradnju

Saradnja je ključna komponenta modernih okruženja za rad i učenje, i olakšavaju je digitalni alati koji omogućavaju ljudima da rade zajedno bez obzira na to gde se nalaze. Onlajn alati za saradnju, kao što su **Slack**, **Trello** i **Asana**, nude platforme na kojima timovi mogu da komuniciraju, dele dokumente i upravljaju projektima u realnom vremenu. Savladavanje tih

alata smatra se delom digitalne kompetencije jer se koriste i u obrazovanju i u profesionalnim okruženjima da bi poboljšali produktivnost i timski rad.

Ti alati se mogu integrisati u aktivnosti koje se sprovode u učionici kako bi učenici naučili šta je upravljanje projektima, komunikacija i saradnja u digitalnim prostorima. Na primer, grupni projekti koji zahtevaju od učenika da koriste alate za digitalnu saradnju mogu im pomoći da usvoje praktične veštine u menadžmentu, komuniciraju efikasnije i rade zajedno da bi postigli isti cilj.

Osnove kreiranja sadržaja

Kreiranje digitalnog sadržaja obuhvata stvaranje različitih oblika digitalnih medija, kao što su tekst, slike, video-klipovi i interaktivni sadržaj. Ta kompetencija se ne ograničava na tehničke veštine i uključuje kreativnosti, razumevanje potreba publike i uzimanje u obzir etičkih vrednosti, kao što su poštovanje autorskih prava i izbegavanje plagiranja. Osnovne veštine kreiranja sadržaja uključuju i korišćenje digitalnih alata za editovanje, dizajniranje i objavljivanje sadržaja, kao i razumevanje principa digitalnog pripovedanja.

Trebalo bi da eksperimentišeš sa različitim platformama za kreiranje sadržaja, od pisanja blogova do video produkcije, kako bi razvio svoje veštine i izrazio svoje ideje. Razumevanje osnova kreiranja sadržaja uključuje i prepoznavanje važnosti vizuelnog dizajna i korisničkog iskustva koji su ključni za kreiranje digitalnog sadržaja koji je zanimljiv i dostupan. Pored toga, trebalo bi da istražiš aspekte dostupnosti digitalnog sadržaja, kako bi obezbedio da je tvoj sadržaj inkluzivan i da ga može koristiti različita publika.

IV. MEDIJSKA PISMENOST

Definicija i opseg

Medijska pismenost osnažuje te da pristupiš, analiziraš, proceniš, kreiraš i koristiš medijski sadržaj na različitim platformama. Predstavlja razumevanje prirode medijskih poruka, procesa medijske produkcije i uloge koju mediji imaju u oblikovanju društva. Medijska pismenost uključuje i prepoznavanje dinamike moći u vlasništvu nad medijima i ekonomskim, političkim i kulturološkim uticajima koji pokreću medijski sadržaj.

Opseg medijske pismenosti značajno se proširio u digitalnom dobu, obuhvatajući tradicionalne medije kao što su novine i televizija, kao i digitalne medije poput društvenih mreža, podkasta, blogova i servisi za onlajn gledanje sadržaja. Kako se pojavljuju nove tehnologije (veštačka inteligencija i proširena stvarnost), opseg medijske pismenosti nastavlja da se razvija, zahtevajući stalnu edukaciju i prilagođavanje. Taj širi opseg pokazuje potrebu za sveobuhvatnim pristupom koji integriše medijsku pismenost u različite predmete i aspekte svakodnevnog života.

Razumevanje medijskih poruka

Razumevanje medijskih poruka zahteva sposobnost kritičke analize na koji način mediji kreiraju stvarnost. Medijske poruke nisu neutralne, one odslikavaju namere i pristrasnosti svojih kreatora, koji mogu da utiču na to kako percipiraš i razumeš informacije. Ljudi koji rade u medijima koriste različite tehnike, kao što su kadriranje, odabir izvora, slike i izazivanje jakih emocija da bi oblikovali svoje poruke i uticali na tvoju perceptiju.

Na primer, upotreba dramatičnih vizuala tokom prenošenja vesto može pojačati emotivni uticaj na priču i na taj način potencijalno pojačati javnu zabrinutost i paniku. Slično tome, izuzimanje određenih perspektiva ili glasova može izmeniti razumevanje problema, predstavljajući samo jedan ugao posmatranja. Ako naučiš da dekonstruišeš te poruke možeš identifikovati osnovne pretpostavke i pristrasnost, što može dovesti do boljeg razumevanja medijskog sadržaja.

Te analitičke veštine mogu se razviti kroz aktivnosti koje uključuju poređenje različitih medijskih prikaza istog događaja, razgovor o uticaju vlasništva nad medijima na praćenje vesti i istraživanje kako strategije u reklamiranju utiču na ponašanje kupaca.

Prepoznavanje i upravljanje dezinformacijama

Dezinformacije su čest izazov u današnjem medijskom pejzažu kada brzina i doseg digitalne komunikacije mogu da pojačaj lažne i obmanjujuće informacije. Da bi se prepoznalo i upravljalo uticajem dezinformacija, važno je razumeti njihove različite tipove:

- **Izmišljeni sadržaj:** Obuhvata potpuno lažne informacije koje su kreirane s namenom da nekoga obmanu. Na primer, članak sa lažnim vestima koji tvrdi da je neka poznata ličnost preminula može brzo da se proširi društvenim mrežama i izazove zabunu i uznemirenost.
- **Klikbejt (Clickbait):** Odnosi se na senzacionalističke i obmanjujuće naslove, napisane da privuku klikove i povećaju broj poseta na vebsajtovima, često na uštrb tačnosti. Na primer, naslov poput „Ne možete da poverujete šta je ovaj političar uradio!“ može voditi na članak koji preteruje ili iskrivljuje činjenice da bi privukao čitaoce.
- **Dipfejk (Deepfakes):** Izmenjeni video snimci ili slike koji prikazuju ljude kako govore ili rade nešto što nisu nikada rekli ili uradili napravljeni uz upotrebu

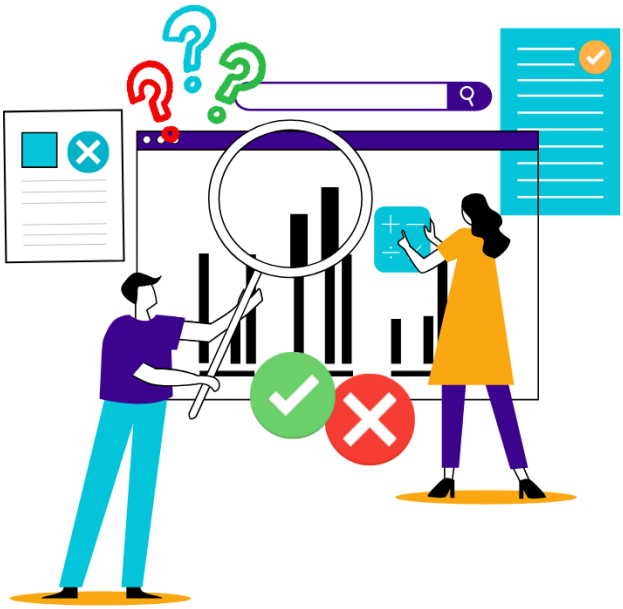
veštačke inteligencije. Primer može biti dipfejk video snimak poznate ličnosti, kao što je političar, koja daje izjavu koju nije u stvari dala, što se može iskoristiti da se raširi lažni narativ ili da se ta ličnost diskredituje.

- **Obmanjujući sadržaj:** Informacije koje iskrivljuju stvarnost ili predstavljaju činjenice na obmanjujući način. Na primer, korišćenje fotografije sa nepovezanog događaja da bi se predstavile trenutne vesti mogu prevariti gledaoce da pomisle da je fotografija povezana sa vešću o kojoj se izveštava.
- **Lažni kontekst:** Prave informacije koje se predstavljaju u obmanjujućem kontekstu, menjajući nameravano značenje. Na primer, stara fotografija sa prošlih protesta se koristi da predstavlja trenutni događaj dajući gledaocima utisak da situacija i dalje traje i da je veća nego što zaista jeste.
- **Sadržaj za prevaru:** Obuhvata sadržaj koji imitira legitimne izvore. Na primer, lažni vebsajtovi koji imitiraju izgled uglednih medijskih kuća da bi širili lažne vesti, što otežava čitaocima da uoče razliku između pravih i lažnih vesti.
- **Satira ili parodija:** Satiričan sadržaj, poput članaka sa sajtova kao što je **The Onion**, namenjeni su zabavi ali neko ih može zameniti za prave vesti ukoliko publika nije svesna njihove satirične prirode.
- **Lažno pripisivanje:** Pripisivanje sadržaja ili citata lažnom ili nepostojećem izvoru. Na primer, pripisivanje izmišljenog citata poznatom naučniku ili javnoj ličnosti da bi tvrdnja dobila nezasluženi kredibilitet..
- **Glasine i obmane:** Neproverene informacije koje se prenose društvenim mrežama, često izazivajući lažne utiske i paniku. Klasičan primer je viralno širenje obmana o opozivu proizvoda ili lažni zdravstveni saveti, kao što je mit da konzumiranje vruće vode može da spreči pojavu virusa COVID-19.

Provera činjenica i verifikacija

Provera činjenica i verifikacija uključuju sistematičnu procenu tačnosti i pouzdanosti informacija konsultovanjem više izvora, proverom dokaza i korišćenjem alata za verifikaciju. Ključni koraci za efikasnu proveru činjenica su:

- **Procena izvora:** Započni sa proverom verodostojnosti izvora informacije. Pouzdani izvori obično imaju transparentne uređivačke standarde, prikazuju informacije o autorima i objavljuju sve moguće sukobe interesa.
- **Unakrsna provera referenci:** Uporedi informacije iz drugih pouzdanih izvora. Usaglašenost informacije iz više pouzdanih izvora povećava verovatnoću da je informacija tačna.
- **Upotreba alata za verifikaciju:** Alati poput **Google Reverse Image Search** mogu biti od pomoći kada proveravaš verodostojnost slika, kao dodaci za pretraživače poput **NewsGuard** pružaju rejting verodostojnosti za novinske sajtove.



- **Provera autorove stručnosti:** Proceni da li je autor kvalifikovan da govori o temi. Veća je verovatnoća da će stručnjaci ili priznati autoriteti u oblasti dati pouzdane informacije.
- **Analiza dokaza:** Potraži dokaze koji potkrepljuju tvrdnje, kao što su rezultati istraživanja ili direktni citati stručnjaka. Pouzdane informacije su obično dobro potkrepljene dokazima koji se mogu nezavisno proveriti.

Etičko korišćenje medija

Etičko korišćenje medija podrazumeva svest o izborima koje pravimo i o uticaju koji ti izbori mogu imati na pojedince i društvo. Zahteva kritički pristup kada je reč o odabiru i deljenju medijskog sadržaja, razmatranje faktora kao što su tačnost, pristrasnost, predstavljanje i moguć uticaj na javni diskurs. Etički korisnici medija su proaktivni u sagledavanju različitih perspektiva, preispitivanju namera koje stoje iza medijskih poruka i izbegavaju širenje neproverenog ili štetnog sadržaja.

Da bi se medijski sadržaji koristili etički, važno je razumeti uticaj algoritama na medije koje koristimo. Algoritmi na društvenim mrežama i pretraživačima često prilagode sadržaj na osnovu tvog ponašanja i na taj način stvaraju eho-komore koje dodatno pojačavaju tvoja postojeća uverenja i ograničavaju izloženost drugim tačkama gledišta. Ako imaš svest o ovim uticaja, možeš preduzeti korake da učiniš svoje korišćenje medija raznolikim tako što ćeš pratiti izvore sa različitim perspektivama, koristiti alate koji prate medijsku pristrasnost ili s namerom potražiti sadržaj koji dovodi u pitanje tvoje pretpostavke.

Odgovorno kreiranje sadržaja

Kao kreator, trebalo bi da imaš u vidu mogući uticaj svog sadržaja i uzmeš u obzir kako može delovati na različitu publiku, pre svega na ranjive i marginalizovane grupe. To uključuje izbegavanje korišćenja jezika ili slika koje promovišu stereotipske stavove, proveravanje tačnosti podataka i poštovanje prava pojedinaca na privatnost i dobijanje njihove saglasnosti za njihovo prikazivanje u medijima. Na primer, kada kreiraš sadržaj koji prikazuje stvarne ljude, važno je da dobiješ saglasnost od njih i daš kontekst kako bi se izbegla pogrešna tumačenja.

Medijska pismenost je ključan skup veština za dobro snalaženje u današnjem kompleksnom medijskom okruženju. Razvijanjem sposobnosti da se kritički odnosiš prema medijskim porukama, prepoznaš i upravljaš dezinformacijama i etički kreiraš sadržaj, osnažuješ sebe i druge za korišćenje medijskog prostora sa samopouzdanjem i integritetom. Kako mediji nastavljaju da evoluiraju, načela medijske pismenosti će postati ključna u promovisanju inkluzivnijeg, pravednijeg i angažovanijeg društva.

V. ODGOVORNA UPOTREBA DRUŠTVENIH MREŽA

Prema podacima za 2023. godinu (Eurostat, 2023), oko 97% mladih u EU koji imaju od 16 do 29 godina koristi internet svaki dan, a 83% koristi društvene mreže. Pošto je korišćenje digitalnih platformi široko rasprostranjeno među mladima, trebalo bi da razumeš prednosti i nedostatke upotrebe društvenih mreža.

Prednosti društvenih mreža

Onlajn kultura omogućava povezivanje i komunikaciju sa drugim digitalnim građanima, a društvene mreže mogu pozitivno da utiču na blagostanje izgradnjom društvenog kapitala. Pružaju i mogućnost da proširiš svoja interesovanja, znanja i veštine, kao i za zabavu i podršku.

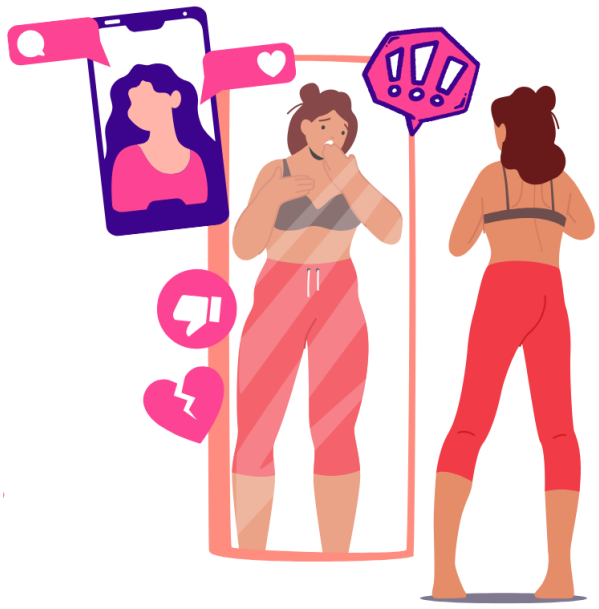
Pored toga, pomažu ti da ostaneš informisan o tome šta se dešava širom sveta. Mnoge novinske kuće imaju svoje profile na društvenim mrežama gde dele najvažnije vesti u sažetom i razumljivom obliku što olakšava da budeš u toku.

Društvene mreže mogu biti posebno korisne mladima kojima treba pomoć – onlajn okruženje uprošćava pristup profesionalnoj pomoći istovremeno obezbeđujući anonimnost. Uz to, od prijatelja i ljudi sa sličnim interesovanjima u onlajn grupama možeš dobiti direktnu emotivnu podršku. Društvene mreže takođe smanjuju osećaj usamljenosti i izolovanosti. Onlajn zajednice koje vode stručnjaci u oblasti mentalnog zdravlja su od posebne važnosti – stvaraju bezbedno okruženje za razgovor o emocijama i dobijanje vršnjačke podrške. Neki blogeri i influenseri pričaju o problemima koji se odnose na mentalno zdravlje i nude prostor gde pojedinci mogu da podele svoja iskustva. Ako pratiš nekoga ko deli svoju priču o oporavku možeš se osetiti snažnije da se nosiš sa sopstvenim izazovima.

Rizici koje nose društvene mreže

Iako društvene mreže imaju svojih dobrih strana, treba biti svestan različitih zamki na internetu koje mogu predstavljati rizik i pretnju. Statistički gledano, izloženost riziku se povećava što si češće onlajn i što je veći intenzitet tvoje interakcije. Spektar faktora, uključujući starost, pol, nivo obrazovanja i kultura iz koje dolaziš, utiču na tvoju ranjivost kada je reč o rizicima i njihovim posledicama.

Što više koristiš komunikacijske alate, društvene mreže i platforme za video igrice, veći je rizik na se susretneš sa onlajn uznemiravanjem, digitalnim nasiljem, digitalnim uhođenjem, uvredama, govorom mržnje, neprimerenim zbližavanjem (eng. grooming), kao i krađom identiteta. Virtuelni svet sadrži i različit štetni sadržaj nasilne ili seksualne prirode, dezinformacije, rasizam, antisemitizam i mnogo toga što može imati ozbiljne posledice na mentalno zdravlje kako mladih tako i društva uopšte.



Pored toga, tinejdžerke su posebno izložene onlajn napadima koji se baziraju na društvenim normama fizičke privlačnosti i lažnim standardima lepote. Društvene mreže su preplavljene slikama na kojima pojedinci koriste ulepšavajuće filtere i retuširanje da bi stvorili nerealne prikaze savršenih tela i lica. Zbog velike izloženosti takvim sadržaju, žene su podložnije osećaju nezadovoljstva zbog svog izgleda i negativnom samoopažanju, što je dalje povezano sa niskim samopouzdanjem i može za rezultat imati probleme sa mentalnim zdravljem i poremećaje u ishrani.

Pored toga, kul objave sa događaja, putovanja i festivala mogu izazvati strah od propuštanja (eng. fear of missing out ili FOMO), ljubomoru i osećaj da

nismo dovoljno dobri. Često smetnemo s uma da su mnoge od tih objava inscenirane i da ne odražavaju stvarni život korisnika društvenih mreža.

Zabava na onlajn platformama dozvoljava ti da „pobegneš“ iz stvarnog sveta. Jureći dopamin, kao digitalni građani, često prekomerno konzumiramo onlajn sadržaj, što može za rezultat imati zavisnost od njega. Takvo ponašanje oduzima puno vremena i ima negativan uticaj na psihičko zdravlje, društvene odnose, koncentraciju i produktivnost, što može dovesti do lošijeg učinka na fakultetu ili poslu. Pored toga, prekomerno konzumiranje onlajn sadržaja izaziva psihološku nelagodu i ima posledice po zdravlje. Društvene mreže se povezuju i sa poremećajima sna i anksioznošću.

Treba da obratiš pažnju i na to da nije sve što se nalazi onlajn istina i da mnogi profili dele dezinformacije koje mogu biti opasne ako se uzmu kao istinite.

Kontroverzni aspekti društvenih mreža: Uloga algoritama

Algoritmi, kao skupovi pravila, proračuna i procesa za donošenje odluka koje platforme koriste za razvrstavanje, preporuku i prikazivanje sadržaja korisnicima, napravljeni su da u prvi plan stave sadržaj sa kojim će se korisnici najverovatnije povezati na osnovu prethodnih podataka o njihovom ponašanju kao što su sviđanja, deljenja i vreme provedeno na određenom sadržaju.

Pozitivna strana algoritama koje koriste društvene mreže je poboljšano korisničko iskustvo pošto je sadržaj prilagođen, smanjuje preopterećenost informacijama i prikazuje informacije koje su značajne korisnicima. Na primer, algoritmi ti pomažu da pronađeš zajednice i informacije koje su prilagođeni tvojim interesovanjima, što čini platforme više orijentisane ka korisnicima.

Međutim, velika mana algoritama je stvaranje eho-komora, gde si izložen prvenstveno sadržaju koji se poklapa sa tvojim postojećim stavovima. Algoritmi daju prednost i senzacionalističkom sadržaju, pojačavajući efekat dezinformacija, pošto takav sadržaj povećava reakcije korisnika. Ukoliko nisi svestan takvih manipulacija, možeš lako upasti u eho-komore koje

pojačavaju predrasude i promovišu dezinformacije, što može dovesti do polarizacije i radikalizacije.

Psihološki efekti tih algoritama su takođe dalekosežni. Stalna izloženost emocionalno nabijenom sadržaju može dovesti do anksioznosti, depresije ili osećaja izolovanosti. Pored toga, zavisnička priroda platformi koje su zasnovane na algoritmima doprinosi prekomernoj upotrebi društvenih mreža, gde se možeš naći u beskrajnim ciklusima skrolovanja bez svesti o tome kolike emocionalne posledice to ima po tebe.

Efekti evropskog zakonodavstva na digitalne pružaoce usluga prema kojima platforme moraju da objave svoje algoritme za preporučivanje tek treba da se sagledaju.

Svesni klik: saveti za odgovorno korišćenje društvenih mreža

Onlajn prostor bi trebalo da bude bezbedan i da učini da se svi korisnici osećaju opušteno. Ljudi koriste društvene platforme za druženje, profesionalno umrežavanje ili aktivizam, ali način na koji učestvuju u onlajn interakcijama može imati trajne posledice na njihove lične živote i društvo. Kompetencije kao što su kritičko razmišljanje, empatija, digitalna, medijska i informatička pismenost su ključni za korišćenje društvenih mreža u okviru načela digitalnog građanstva. Da bismo postali odgovorni digitalni građani, trebalo bi poslušati sledeće savete:

- **Razmisli pre nego što okačiš nešto:** Društvene mreže često podstiču impulsivno kačenje sadržaja. Objave okačene u besu ili frustraciji mogu te prikazati u lošem svetlu i drugi ljudi ih mogu loše protumačiti. Svestan

pristup kada je reč o deljenju sadržaja može sprečiti nerazumevanje ili urušavanje tvog onlajn ugleda.

- **Razumej posledice deljenja ličnih podataka**: Deljenje ličnih podataka, kao što su informacije koje omogućavaju ličnu identifikaciju (eng. Personal Identifiable Information - PII), lokacija, planovi za putovanje, i sl. može biti rizično. Takve objave mogu se iskoristiti da prate tvoje aktivnosti, ugroze tvoju privatnost ili da dovedu do krađe identiteta.
- **Budi svestan mogućih kriminalnih radnji:** Važno je ostati oprezan kada je reč o tehnološkim i ljudskim rizicima u digitalnim prostorima. Treba na vreme prepoznati i izbeći „pecanje" i pokušaje krađe identiteta kao i onlajn napade. Izbegavaj da klikneš na nepoznate ili sumnjive linkove i da skidaš fajlove sa nepouzdanih sajtova.
- **Pre deljenja proveri činjenice:** Pre nego što podeliš članak ili objavu, proveri da li informacije dolaze iz pouzdanih izvora. Trebalo bi da razviješ kritičko razmišljanje kako bi odvojio činjenice od glasina ili klikbejta. Netačne i obmanjujuće objave mogu ne samo loše uticati na tvoj kredibilitet već naneti štetu čitavom društvu.
- **U onlajn interakcijama vodi se poštovanjem i empatijom:** Društvene mreže mogu biti prostor za zdrav i konstruktivan dijalog. Izbegavaj onlajn rasprave i lične napade, jer te situacije često brzo eskaliraju i ostavljaju trajne negativne utiske. Uvežbavaj se da koristiš digitalnu empatiju i saslušaj suprostavljena mišljenja s poštovanjem jer to utiče na pozitivno onlajn okruženje.
- **Učestvuj na aktivan i pozitivan način:** Tvoj digitalni ugled može porasti uz smislene doprinose. Bilo da su to profesionalni forumi ili društvene mreže, doprinos u smislu vrednih uvida i korišćenje digitalne empatije mogu ti pomoći u oblikovanju snažnog i pozitivnog digitalnog identiteta. To obuhvata učestvovanje u vrednim diskusijama, deljenje smislenog sadržaja i pružanje podrške inicijativama koje promovišu inkluzivnost i društvenu odgovornost onlajn.
- **Imaj u vidu svoju publiku**: Društvene mreže su često javne ili polujavne, što znači da tvoja publika može biti šira nego što misliš. Objave namenjene

tvojim prijateljima mogu lako stići i do budućih poslodavaca, akademskih institucija ili neželjenih gledalaca. Održavanje odgovarajućeg, pristojnog i učtivog tona i korišćenje netikecije čuvaju tvoj onlajn ugled.

- **Izbegavaj prekomerno korišćenje društvenih mreža:** Ograniči upotrebu društvenih mreža tako što ćeš imati svest o vremenu koje provodiš pred ekranom. Mnogi pametni telefoni sada omogućavaju korisnicima da podese vremenska ograničenja za aplikacije, uključujući i društvene mreže, i pošalju obaveštenje kada se to ograničenje prekorači. Ta funkcionalnost pomaže u upravljanju vremenom koje se provodi pred ekranom i podstiče svest o mogućem prekomernom korišćenju.

Onlajn ugled: kako komunicirati i kako se predstaviti onlajn

Način na koji te ljudi vide onlajn, drugim rečima tvoj onlajn ugled, direktno odslikava tvoje onlajn prisustvo. Onlajn prisustvo je tesno povezano sa onlajn bezbednošću i etičkim ponašanjem u virtuelnim okruženjima. Onlajn prisustvo nije samo pasivno onlajn učešće jer uključuje i aktivno upravljanje digitalnim otiskom kroz interakcije, stvaranje sadržaja i etičko ponašanje, ističući važnost digitalne pismenosti i samosvesti u oblikovanju svoje javne persone.

Tvoj onlajn identitet može se oblikovati s namerom i nehotice. Oblikovanje identiteta s namerom uključuje profile, slike, objave i lične informacije koje odlučiš da postaviš onlajn. Faktore koji nehotice utiču na tvoj identitet određuju drugi ljudi koji okače nešto o tebi, na primer kada te označe na

fotografiji ili objavi. Danas platforme obaveštavaju korisnike kada ih neko označi i daju mogućnost da se ta oznaka odbije ili potvrdi. Ta mogućnost ti daje određen nivo kontrole kada je reč o tvom indirektnom onlajn identitetu.

Sve što se podeli onlajn ostavlja trag, zbog toga je ključno biti imati na umu šta se deli i koje su moguće implikacije. Digitalni ugled koji oblikuješ može lako biti revidiran onlajn pretragama uz upotrebu tvog imena ili drugih informacija koje omogućavaju ličnu identifikaciju. Rezultati pretrage mogu uključivati objave na društvenim mrežama, komentare, profesionalne profile i bilo koji javni sadržaj koji je povezan sa tvojim identitetom. Pozitivno onlajn prisustvo, kao što su profesionalna postignuća ili konstruktivno uključivanje na forumima, povećava tvoj ugled. S druge strane, negativan sadržaj, kao što je nedolično ponašanje na društvenim mrežama, kontroverzni komentari ili širenje dezinformacija može naneti štetu tvom ugledu i imati negativan uticaj na buduće prilike za zapošljavanje. Na primer, prijave za posao mogu biti odbijene nakon što se uradi pregled društvenih mreža kandidata.

VI. KAKO RAZUMETI DIGITALNI OTISAK I KAKO UPRAVLJATI NJIME

U današnjem povezanom svetu, svaka naša onlajn aktivnost ostavlja trag koji se naziva digitalni otisak.

Digitalni otisak se odnosi na podatke koji se generišu dok koristiš internet. Obuhvata sve informacije o tvojim onlajn aktivnostima, interakcijama i prisustvu na različitim digitalnim platformama. Postoje dva tipa digitalnih otisaka – aktivni i pasivni.

Aktivni digitalni otisak podrazumeva podatke koje s namerom podeliš onlajn, kojih si svestan i koje kontrolišeš. To uključuje sve informacije koje objaviš ili dostaviš, kao što su objave na društvenim mrežama (na platformama kao što su Fejsbuk, X ili Instagram), onlajn recenzije koje napišeš za proizvode ili usluge, registracije naloga, uključujući informacije koje dostaviš kada otvoriš nalog na različitim sajtovima.

Pasivni digitalni otisak su informacije koje se prikupljaju o tebi bez tvog direktnog uključivanja. Obuhvataju istoriju pretraga koje zapamte sajtovi, zapisi IP adresa, podaci o lokaciji sa mobilnih uređaja i podaci koje prikupljaju aplikacije koje rade u pozadini.

Svaka tvoja aktivnost onlajn ostavlja tragove i nekada digitalni otisci mogu biti tamo gde ih ne očekuješ. Evo nekih primera digitalnih otisaka kako bi ti bilo lakše da osvestiš svoje aktivnosti koje ih proizvode:

Veza između digitalnog otiska i onlajn ugleda je važna, pošto digitalni otisak predstavlja osnov nečijeg onlajn ugleda. Kao što je već rečeno, digitalni otisak obuhvata sve podatke i tragove koje pojedinac ostavi svojim onlajn aktivnostima, bilo namerno ili slučajno. To podrazumeva objave na društvenim mrežama, komentare, onlajn kupovinu i istoriju pretrage između ostalog.

Digitalni otisak direktno utiče na onlajn ugled jer odslikava vrednosti, interesovanja i ponašanje svakog od nas. Potencijalni poslodavci, poslovni partneri, čak i lični poznanici često procenjuju naš onlajn ugled na osnovu digitalnog otiska. Pozitivan digitalni otisak može pozitivno da utiče na tvoju profesionalnu i ličnu sliku, pokazujući stručnost i pouzdanost. Suprotno tome, negativan digitalni otisak, kao što su neprimereni komentari ili kontroverzna mišljenja, mogu loše uticati na kredibilitet i pouzdanost i na taj način dovesti da ti izmaknu neke prilike.

Upravljanje svojim digitalnim otiskom je važno za održavanje dobrog onlajn ugleda. To znači da moraš imati na umu kakav sadržaj deliš onlajn, da proveriš podešavanja za privatnost i da redovno pratiš svoje onlajn prisustvo kako bi ga uskladio sa željenom ličnom i profesionalnom slikom.

Potencijalne zamke

Digitalni otisci koji se prepuste slučaju mogu dovesti do različitih rizika pored negativnog onlajn ugleda:

- **Rizici po privatnost:** Digitalni otisak te može izložiti rizicima po privatnosti koji uključuju digitalno uhođenje, uznemiravanje i fizičke pretnje. Drugi ljudi mogu zloupotrebiti lične podatke koje deliš onlajn, što može dovesti do neželjene pažnje i mogućih opasnih situacija.
- **Pretnje po bezbednost:** Sajber kriminalci mogu iskoristiti digitalne otiske za krađu identiteta, „pecanje" i lažiranje naloga. Lični podaci koji su dostupni onlajn, kao što su korisničko ime i lozinka mogu biti iskorišćeni za neovlašćen pristup tvojim nalozima, što može dovesti do finansijskih gubitaka i druge štete.
- **Ciljano oglašavanje i iskorišćavanje podataka:** Kompanije koriste digitalne otiske da bi pratile ponašanje i preferencije korisnika što im olakšava ciljano oglašavanje. Iako ovo može da poboljša korisničko iskustvo, istovremeno izaziva i brigu zbog privatnosti podataka i mere u kojoj se lični podaci koriste bez eksplicitne saglasnosti.
- **Uticaj na životnu sredinu:** Skladištenje i obrada digitalnih podataka doprinosi većoj potrošnji energije i emisiji ugljen-dioksida. Ako imaš u vidu da tvoj digitalni otisak može pomoći i u smanjenju uticaja na životnu sredinu.

Ekološki aspekt

Ekološki aspekt digitalnog otiska je sve važnija tema kako naše onlajn aktivnosti nastavljaju da se povećavaju. Digitalne aktivnosti troše veliku količinu energije jer centri podataka i mreže koje napajaju onlajn servise emituju oko 1% ukupnih svetskih gasova sa efektom staklene bašte.

Pored toga, konzumiranje digitalnog sadržaja proizvodi značajan ugljenički otisak. Kako se digitalni servisi i tehnologije poput igranja video igara na servisima „cloud", blokčejna i virtuelne stvarnosti razvijaju, očekuje se da uticaj digitalnih otisaka na životnu sredinu naglo poraste. Kako bi se

odgovorilo na ove rizike po životnu sredinu, stručnjaci preporučuju promovisanje praksi digitalne svesnosti za smanjenje nepotrebne digitalne konzumacije, pored drugih strategija.

Razumevanje i upravljanje ekološkim aspektima digitalnih otisaka je ključno da bi se obezbedila održiva digitalna budućnost.

Kako smanjiti rizike koje donosi digitalni otisak?

Upravljanje svojim digitalnim otiskom počinje sa upravljanjem ličnim podacima. Naredni saveti ti mogu pomoći da smanjiš rizik od curenja ličnih podataka:

Još jedan koristan savet je da naučiš više o sledećim alatima i o tome šta oni mogu da urade:

- **VPN (Virtual Private Networks - virtuelne privatne mreže):** Maskiraj svoju IP adresu i izvrši enkripciju svojih onlajn aktivnosti
- **Softveri za blokiranje reklama:** Smanji praćenje tako što ćeš blokirati reklame i softvere tragače.
- **Bezbedni pretraživači:** Koristi pretraživače sa ugrađenim funkcionalnostima za privatnost.
- **Pretraživači koji su fokusirani na bezbednost:** Odaberi pretraživače koji ne pamte tvoje upite za pretragu.
- **Alati za uklanjanje podataka:** Koristi servise koji ti pomažu da ukloniš svoje lične podatke sa sajtova koji posreduju podacima.
- **Bezbedne mreže:** Postaraj se da je tvoj kućni internet zaštićen kako bi se smanjio rizik od izloženosti.
- **Ažuriranje softvera:** Redovno ažurirajte softvere i antivirus programe na svojim uređajima.

Ako se potrudiš da razumeš šta je digitalni otisak i sprovedeš gore navedene strategije, možeš bolje zaštiti svoje onlajn prisustvo i smanjiti rizike koji su povezani sa tvojim digitalnim aktivnostima.

Bezbednost: zašto je zaštita ličnih podataka važna

Osetljive informacije kao što su imena, adrese, identifikacioni brojevi, finansijski podaci, pa čak i preferencije i navike postali su vredna roba, ne samo za pojedince već i za korporacije, treća lica i neizbežno za kriminalce. Zaštita ličnih podataka je ključna da bi se izbeglo kršenje privatnosti poput krađe identiteta i drugih zlonamernih aktivnosti koje su posledica curenja podataka. Curenje podataka postalo je sve češće, što znači da bi trebalo da razumeš kako se tvoji lični podaci prikupljaju i skladište, kao i rizike koji su povezani sa ličnim podacima kako bi se pravilno zaštitio (Savet Evrope 2019).

Pravo na privatnost je osnovno ljudsko pravo i njegova važnost je sve izraženija u modernom digitalnom okruženju. Evropska unija je 2018. godine usvojila Opštu uredbu o zaštiti podataka (GDPR) koja reguliše prikupljanje, skladištenje i upotrebu ličnih podataka (Sharma 2022). Ta zakonska regulativa pruža ljudima više kontrole nad njihovim ličnim podacima i omogućava im da upravljaju svojim digitalnim prisustvom na efikasniji način.

Rizici koji nastaju zbog dostupnosti ličnih podataka

U mnogim slučajevima, korisnici nisu svesni rizika koji mogu nastati deljenjem podataka. Naizgled bezazlene aktivnosti, kao što je objava fotografije ili deljenje lokacije na društvenim mrežama, mogu nehotice otkriti više nego što nameravaš i izložiti te riziku.

Posledice curenja ličnih podataka mogu biti dalekosežne i ozbiljne. Jedna od najozbiljnijih je krađa identiteta, kada zlonamerni ljudi ukradu i koriste lične podatke kao što su identifikacioni brojevi, podaci za prijavljivanje ili finansijski podaci za neovlašćenu kupovinu ili otvaranje naloga na ime žrtve. Dodatni rizik je da neko može da kreira lažne profile na društvenim mrežama da bi te oponašao, što može imati višestruke negativne posledice. Osoba koja se pretvara da si ti može uraditi nešto nelegalno ili naneti štetu tvojoj reputaciji tako što će prevariti tvoje prijatelje ili kolege. Pored toga, takvi nalozi često mogu dovesti do narušavanja privatnosti, izlaganja ličnih podataka i kontakata. To može omogućiti napade „pecanjem“ ili krađu identiteta gde osoba koja se pretvara koristi lažan profil da bi dobila neovlašćen pristup osetljivim podacima, finansijskim nalozima ili drugim onlajn platformama i na taj način da ti nanese ozbiljnu štetu.

Na sve ovo, lični podaci koji procure mogu narušiti ugled, posebno kada se lični podaci izlože u neprikladnom kontekstu ili ih treća lica zloupotrebe. Ako se osetljive lične informacije poput ličnih poruka, fotografija ili video snimaka učine dostupnim onlajn, mogu se iskoristiti da naštete ugledu pojedinca, što

negativno utiče i na lične i profesionalne odnose i može za rezultat imati, na primer, uznemiravanje ili digitalno nasilje. U ekstremnim slučajevima, lični podaci koji procure mogu dovesti do pretnji u stvarnom svetu, kao što su uhođenje ili ucena.

Pored toga, narušavanje privatnosti može izazvati emocionalni stres, čineći da se žrtve osećaju ranjivo, napadnuto i u strahu od mogućih posledica. Takav psihološki danak može ozbiljno da utiče na fizičko i mentalno zdravlje, kao i osećaj bezbednosti pojedinca. Narušavanje privatnosti često izaziva osećanje bespomoćnosti jer žrtve shvataju da više nemaju kontrolu nad svojim ličnim podacima. Taj gubitak kontrole može da za rezultata ima povećanje anksioznosti, stres i stalni osećaj straha od toga šta je sledeće što može da se desi. Žrtve mogu patiti od insomnije, paranoje ili depresije, jer narušavanje privatnosti može loše uticati na njihovo poverenje u digitalne sisteme i ljude oko njih. Takva osećanja se pojačavaju kada se manifestuju posledice narušavanja privatnosti, kao što su finansijske prevare ili krađa identiteta. Osećaj ranjivosti se pogoršava kada osetljive informacije, kao što su privatne fotografije ili prepiska, postanu dostupne onlajn. Ta izloženost može dovesti do narušavanja ugleda, digitalnog nasilja, uznemiravanja i pretnji po fizičku bezbednost. Mogu se javiti i problemi sa mentalnim zdravljem, kao što su posttraumatski stresni poremećaj (poznatiji po svojoj engleskoj skraćenici PTSD), posebno kada osetljivi podaci poput medicinskih kartona ili intimnih fotografija postanu dostupni onlajn.

Uticaj na osećaj sigurnosti je isto kritičan. Ljudi koji su iskusili narušavanje privatnosti često se osećaju nesigurno i u digitalnim i u fizičkim okruženjima, plašeći se ponovnog iskorišćavanja ili napada. Taj nedostatak sigurnosti može dovesti do povlačenja iz društvenog života jer žrtve počinju da izbegavaju digitalne prostore i smanjuju broj svojih interakcija kako bi smanjili dalju

izloženost. Psihosocijalni teret se dakle ne ograničava na trenutak narušavanja privatnosti, već je prisutan i dalje i utiče na razne aspekte svakodnevnog života.

Da bi se to izbeglo, veoma je važno prepoznati značaj zaštite ličnih podataka i preduzeti odgovarajuće korake da se smanje rizici. Digitalni građani moraju preduzeti efikasne mere da bi osigurali da njihovim ličnim podacima nije moguće neovlašćeno pristupiti i zloupotrebiti ih.

Budi bezbedan onlajn: praktični saveti za čuvanje privatnosti

Pošto su lični podaci stalno u riziku od izlaganja onlajn ili zloupotrebe, važno je razumeti i sprovesti efikasne strategije za njihovu zaštitu. Dajemo ovde nekoliko navika koje će ti pomoći da bolje sačuvaš svoju privatnosti u digitalnom prostoru:

Ograniči deljenje informacija i proveri podešavanja privatnosti

Deljenje ličnih podataka onlajn bi trebalo raditi oprezno. Može se desiti da nenamerno podeliš više informacija nego što je neophodno, kao što su lokacija u realnom vremenu ili lične navike. Smanjenje količine ličnih informacija koje deliš, bilo na društvenim mrežama ili drugim platformama, može te zaštiti od rizika poput digitalnog uhođenja ili krađe identiteta. Na primer, izbegavaj da objavljuješ planove za putovanje ili informacije o svojim rutinama koje te mogu izložiti uhođenju ili nekim drugim zlonamernim aktivnostima.

Prilagođavanjem podešavanja privatnosti možeš kontrolisati ko ima pristup ličnim podacima i time smanjiš rizik od neželjenog izlaganja podataka. Preporuka je da praviš privatne profile i da ne dozvoliš strancima da te prate. Pored toga, pravljenje listi „bliskih prijatelja“ na platformama kao što su

Instagram ili korišćenje podešavanja privatnosti na Fejsbuku koje ograničavaju vidljivost objava mogu sprečiti neželjeno izlaganje.

Redovno ažuriraj podešavanja privatnosti

Kako se tehnologija i prakse za zaštitu privatnosti razvijaju, važno je redovno revidirati i ažurirati podešavanja privatnosti na aplikacijama i onlajn nalozima. To obezbeđuje da se lični podaci dele prema tvojim preferencijama. Trebalo bi i da onemogućiš funkcionalnosti za deljenje lokacije i da ukineš nepotrebne dozvole aplikacijama i servisima kojima više ne treba pristup tvojim podacima.

Informiši se o zakonima za zaštitu podataka

Opšta uredba o zaštiti podataka (GDPR) usvojena je kako bi zaštitila privatnost pojedinaca tražeći od vebsajtova da zatraže eksplicitnu saglasnost pre sakupljanja ličnih informacija. Informisanost o takvim zakonima omogućava ti da bolje razumeš rizike i bolje kontrolišeš svoj digitalni otisak. Na primer, GDPR daje korisnicima pravo da zatraže brisanje svojih podataka ili da zatraže da se podaci ne dele sa trećim licima.

Upravljanje kolačićima i podešavanja pretraživača

Većina vebsajtova koristi kolačiće, male fajlove koje se skladište na uređaje korisnika, i najčešće su automatski omogućeni u pretraživačima. Možeš podesiti podešavanja tako da prihvatiš ili odbiješ kolačiće.

Dok su neki kolačići neophodni za funkcionisanje vebsajtova, ostali mogu da prate tvoje aktivnosti preko različitih sajtova. Podešavanja kolačića u pretraživaču ti mogu pomoći da kontrolišeš koje tipove kolačića želiš da dozvoliš i time sprečiš nepotrebno praćenje. Pored toga, povremeno čišćenje kolačića i podataka koje generišu pretraživači mogu unaprediti privatnost.

Razvij osnovna tehnološka znanja

Osnovno razumevanje tehnoloških koncepta, poput enkripcije, kolačića i IP adresa može značajno da utiče na zaštitu tvoje onlajn privatnosti. Na primer, ako znaš kako funkcioniše enkripcija to ti može pomoći da odabereš

bezbednije načine komunikacije, a razumevanje IP adresa ti može omogućiti da budeš svesniji kako se tvoja lokacija može pratiti onlajn. Informisanje o tehnologijama koje unapređuju privatnost, poput servisa VPN i bezbednih pretraživača, može te osnažiti da zaštitiš svoje podatke efikasnije i da povećaš svoju anonimnost kada si onlajn.

Obazrivo koristi javni bežični internet i deljene uređaje

Javno dostupan bežični internet, iako je vrlo praktičan, predstavlja velik bezbednosni rizik jer nema enkripciju. To olakšava digitalnim kriminalcima da presretnu lične podatke. Kako bi bezbedno koristio javni bežični internet, izbegavaj osetljive transakcije kao što su elektronsko bankarstvo i kupovina. Bezbednija alternativa je da koristiš VPN koji enrkiptuje tvoju internet vezu i štiti tvoje podatke od presretanja. Slično tome, korišćenje javnih ili deljenih uređaja, kao što su računari univerzitetskih biblioteka, predstavlja bezbednosni rizik. Lični podaci, kao što su korisničko ime i lozinka za nalog ili istorija pretrage, mogu biti slučajno sačuvani i kasnije im mogu pristupiti drugi korisnici.

Koristi jake lozinke i dvofaktorsku verifikaciju (2FA)

Jedan od najdirektnijih načina da zaštitiš svoje onlajn naloge je korišćenje jake i jedinstvene lozinke. Jaka lozinka obično kombinuju velika i mala slova, cifre i posebne znakove. Važno je i da izbegneš korišćenje istih lozinki na različitim platformama. Dvofaktorska verifikacije (2FA) je dodatni nivo bezbednosti koji zahteva drugi oblik identifikacije, kao što je šifra putem tekstualne poruke ili aplikacija za verifikaciju, što značajno smanjuje šanse za neovlašćeni pristup.

Koristi sigurne vebsajtove (HTTPS)

Kada deliš lične informacije ili kupuješ onlajn, uvek proveri da je vebsajt siguran tako što ćeš potvrditi da je postoji prefiks HTTPS u adresi sajta (URL sajta). Slovo „S“ u HTTPS dolazi od engleske reči za bezbedno – „secure“, što

pokazuje da vebsajt koristi enkripciju da zaštiti podatke od presretanja. Obrati pažnju i da li postoji ikonica katanca ili preklopno dugme (eng. toggle) pored adrese sajta kako bi potvrdio da je veza bezbedna.

Praćenje ovih praktičnih saveta može značajno poboljšati tvoju privatnost i bezbednost kada si onlajn, što nije samo neophodnost već i odgovornosti. Kombinacija proaktivnog upravljanja privatnošću i tehnološke osvešćenosti može značajno umanjiti rizike koji se dovode u vezu sa deljem ličnih podataka onlajn.

VII. ZAKLJUČAK

Kako digitalni svet postaje sve prisutniji u našim svakodnevnim životima, podučavanje mladih ljudi veštinama i vrednostima digitalnog građanstva nikad nije bilo važnije. Prema podacima Eurostat (2023), 97% mladih između 16 i 29 godina u EU koristi internet svakodnevno, dok je 83% aktivno na društvenim mrežama. Ta statistika podvlači koliko su digitalne tehnologije prisutne u oblikovanju načina na koji mladi uče, povezuju se i komuniciraju sa svetom.

Digitalni prostor služi kao „prozor u svet", pružajući prilike za usvajanje novih znanja i veština. Međutim, da bi se iskoristile te prilike a izbegli mogući rizici, mladima je potrebna dobra osnova u oblasti digitalnog građanstva. Ovaj vodič, koji je u skladu sa Okvirom digitalnih kompetencija za građane Evropske komisije, postavlja tu osnovu naglašavajući kritičko razmišljanje, etičko ponašanje i ključne kompetencije za budućnost.

Digitalno građanstvo je više od tehničkog znanja; digitalno građanstvo je podrška informisanom, učtivom i odgovornom učešću u digitalnim okruženjima. Ugrađujući načela onlajn privatnosti, medijske pismenosti, odgovornog korišćenja društvenih mreža i upravljanja digitalnim otiskom, ovaj vodič daje mladima alate da donose promišljene odluke i pozitivno doprinesu digitalnoj zajednici.

Kompetencije navedene u ovom vodiču ne samo da su ključne za snalaženje u današnjem digitalnom svetu, već su važne i za budući uspeh u svetu koji se sve više digitalizuje. Kako edukatori, treneri i organizacije sprovode te prakse, oblikovaće generacije sposobne da se nose sa izazovima i maksimalno iskoriste prilike digitalnog doba.

Hajde da zajedno nastavimo da promovišemo digitalno građanstvo kao temelj obrazovanja, i podržimo mlade da mogu bezbedno, etički i efikasno da istražuju bezgranične mogućnosti digitalnog sveta.

GLOSAR

Autorove kvalifikacije	Iskustvo, obrazovanje i stručnost koje pojedinac ima u vezi sa temom o kojoj pišu.
Dezinformacija	Namerno konstruisanu lažnu ili obmanjujuću informaciju koja se širi s namerom da se drugi ljudi prevare ili da se njima manipuliše.
Digitalna (onlajn) zajednica	Grupa koja komunicira, deli sadržaje i sarađuju u okviru digitalnih platformi i onlajn prostora.
Digitalna kompetencija	Skup veština, znanja i stavova koji su potrebni za efikasno i odgovorno korišćenje digitalnih tehnologija u različitim aspektima života uključujući lični, obrazovni i profesionalni kontekst.
Digitalna pismenost	Sposobnost da se efikasno, bezbedno i odgovorno koriste digitalne tehnologije, alati i platforme za pristupanje, procenu, kreiranje i deljenje informacija.
Digitalna prava	Prava i slobode koje pojedinci imaju u digitalnom svetu, uključujući mogućnost da pristupe digitalnom sadržaju i informacijama i da ih koriste, kreiraju i dele, a da istovremeno zaštite svoje lične podatke i privatnost.
Digitalna trgovina (e-commerce)	Kupovinu i prodaju robe i usluga na internetu.

Digitalna zavisnost	Prekomerno i kompulsivno korišćenje digitalnih tehnologija, kao što su pametni telefoni, računari, društvene mreže, video igre ili internet do mere u kojoj to negativno utiče na različite aspekte ličnog života, kao što su odnosi, posao, zdravlje ili opšte blagostanje.
Digitalne veštine	Sposobnost da se efikasno koriste tehnologija, alati i platforme.
Digitalni alati	Softver, platforme, aplikacije ili uređaje koji koriste digitalne tehnologije da bi rešili zadatke ili probleme, komunicirali ili olakšali aktivnosti.
Digitalni građanin	Pojedinac koji koristi digitalne tehnologije i internet odgovorno, etički i efikasno da bi se uključio u društveni, politički, obrazovni i kulturni život.
Digitalni otisak	Trag podataka ili informacija koje osoba pojedinac ostavi iza sebe kada koristi digitalne uređaje ili komunicira onlajn.
Digitalni prostor	Okruženje ili platformu koja postoji onlajn ili je pokreću digitalne tehnologije, gde korisnici komuniciraju međusobno i koriste sadržaje ili usluge.
Digitalni sadržaj	Informacije ili materijale koji se kreiraju, skladište, dele ili konzumiraju u digitalnom formatu.
Digitalni svet	Globalni ekosistem koji kreiraju digitalne tehnologije, gde se razmena informacija, komunikacija i aktivnosti obavljaju elektronski i onlajn.
Digitalno	Bilo šta što se odnosi na predstavljanje, skladištenje ili obradu informacija u diskretnim binarnim formatima (npr.

	nule i jedinice) nasuprot kontinuiranim analognim signalima. Digitalna tehnologija je osnova modernog računarstva i telekomunikacija.
Digitalno građanstvo	Odgovorno, etičko i informisano korišćenje tehnologija, pre svega interneta, da bi se na efikasan način učestvovalo u društvu.
Digitalno nasilje	Upotreba digitalnih tehnologija za uznemiravanje, pretnje, ponižavanje ili da bi se nekome naškodilo.
Digitalno okruženje	Virtualni prostor ili ekosistem gde se odvijaju digitalna komunikacija, aktivnosti i procesi.
Digitalno pripovedanje	Praksu korišćenje digitalnih alata i platformi za kreiranje i deljenje priča.
Digitalno rešavanje problema	Sposobnost da se koriste digitalni alati, tehnologije i resursi kako bi se prepoznala, analizirala i pronašla rešenja za probleme ili izazove u različitim kontekstima, kao što je posao, lični život ili obrazovanje.
Digitalno uhođenje	Upotrebu interneta, društvenih mreža ili drugih onlajn platformi za uhođenje i uznemiravanje pojedinaca ili grupa.
Društvene mreže	Digitalne platforme i aplikacije koje omogućavaju korisnicima da kreiraju, dele i razmenjuju sadržaje, ideje i informacije sa drugima putem virtuelnih zajednica i mreža.
Društveni kapital	Koncept koji opisuje vrednost dobijenu iz društvenih odnosa i veza koje pojedinci imaju sa svojim zajednicama, organizacijama ili društvima.

Eho-komora	Okruženja, najčešće u okviru medija ili društvenih mreža, gde su pojedinci izloženi informacijama, stavovima ili idejama koje podržavaju njihova postojeća uverenja ili stavove i ne izlažu ih različitim perspektivama.
Empatija	Sposobnost da se razumeju osećanja, misli ili iskustva druge osobe i da se sa njima poistoveti.
Imejl (email)	Način razmene digitalnih poruka između ljudi koji koriste elektronske uređaje, pre svega putem interneta.
Informaciona pismenost	Sposobnost da se pronađu, procene i koriste informacije na efektivan, efikasan i etički način.
Inkluzija	Praksu stvaranja okruženja, sistema i zajednica koje prihvataju raznolikost i obezbeđuju da svi pojedinci, bez obzira na njihovo poreklo, identitet ili sposobnosti, imaju jednak pristup prilikama, jednaku mogućnost da učestvuju i jednako poštovanje.
Krađa identiteta	Neovlašćeno prisvajanje i korišćenje nečijih drugih ličnih informacija, najčešće zbog prevare.
Kritička procena	Proces pažljive procene i analize nečega – bilo da je reč o ideji, argumentu, radu, teoriji ili izvoru informacije – tako što se preispituju jake strane, slabosti, važnost, tačnost i opšta validnost.
Kritičko razmišljanje	Proces aktivne i objektivne analize, procene i sinteze informacija da bi se donele obrazložene i informisane odluke.
Lažiranje naloga	Na lažiranje naloga ili identiteta osobe koji stvarno postoje sa ciljem da se obmanu drugi ljudi.

Lične informacije ili informacije koje omogućavaju ličnu identifikaciju	Podatke ili informacije koje mogu biti iskorišćene za identifikaciju i lociranje pojedinca ili stupanje u kontakt s njim, bilo neposredno ili posredno.
Medijska pismenost	Sposobnost da se pristupi medijima, da se oni analiziraju, procene i kreiraju u različitim oblicima.
Neprimereno zbližavanje (grooming)	Proces u kojem pojedinac gradi odnos sa detetom ili osobom iz ranjive grupe sa ciljem da njima manipuliše, da ih iskoristi ili zlostavlja.
Onlajn aktivizam	Digitalne alate i platforme koji se bave društvenim, političkim, ekološkim ili ekonomskim problemima.
Onlajn uznemiravanje	Korišćenje digitalnih platformi i tehnologija kako bi se pojedinci ili grupe namerno povredili, zastrašili, omalovažavali ili da bi im se uputile pretnje.
Onlajn zloupotreba	Korišćenje interneta ili digitalnih platformi za nepravedno iskorišćavanje pojedinaca, često putem manipulacije, prinude ili obmane zbog lične, finansijske ili seksualne koristi.
Opšta uredba o zaštiti podataka (GDPR)	Sveobuhvatni zakon o zaštiti podataka koji je donela Evropska unija (EU). Stupio je na snagu 25. maja 2018. godine i uređuje obradu ličnih podataka pojedinaca u okviru EU i Evropskog ekonomskog prostora (EEP).
Pecanje (phishing)	Tip digitalnog napada u kojem napadači oponašaju institucije ili pojedince kako bi naveli žrtve da im otkriju osetljive informacije, kao što su lozinke, brojeve kreditnih kartica, lične identifikacione brojeve i druge lične podatke.

Podkast	Digitalni audio ili video program koji se može gledati onlajn ili skinuti sa interneta, i koji se obično objavljuje u epizodama.
Prava intelektualne svojine	Pravnu zaštitu koja se dodeljuje stvaraocima i vlasnicima intelektualne svojine, koja uključuju nematerijalne tvorevine uma.
Pravičnost	Načelo poštenja i pravde u raspoređivanju resursa, prilika i postupanja kojim se obezbeđuje da pojedinci i grupe dobiju ono što im je neophodno da bi se postigla jednakost ishoda.
Pristrasnost	Sklonost ili preferenciju koja utiče na rasuđivanje, percepciju ili ponašanje pojedinca na način koji je nefer, iskrivljen ili jednostran.
Proširena stvarnost (augmented reality – AR)	Tehnologija koja postavlja digitalne informacije preko slika, zvukova ili drugih podataka u stvarnom okruženju i realnom vremenu.
Provera činjenica (fact-checking)	Proces provere tačnosti i istinitosti informacija, tvrdnji ili izjava, najčešće putem unakrsnog proveravanja pouzdanih i verodostojnih izvora.
Servisi za onlajn gledanje sadržaja (streaming)	Platforme ili tehnologije koje omogućavaju korisnicima da pristupe medijskom sadržaju (kao što je muzika, video-snimci, TV serije, filmovi i prenosi uživo) putem interneta u stvarnom vremenu, bez potrebe da se taj sadržaj prvo skine na uređaj.
Učešće	Aktivno uključivanje pojedinaca u aktivnosti, procese donošenja odluka ili događaje.

Veštačka inteligencija (artificial intelligence – AI)	Simulaciju ljudske inteligencije u mašinama koje su programirane da razmišljaju, uče i izvršavaju zadatke koji obično zahtevaju ljudsko razmišljanje, kao što je razumevanje jezika, prepoznavanje šablona, rešavanje problema i donošenje odluka.
Virtuelna stvarnost (virtual reality – VR)	Računarski generisana simulacija okruženja koje uranja korisnike u potpuno virtuelni svet, obično putem slušalica, senzora i dodatne opreme kao što su rukavice ili kontrolne ručice.
Vređanje (flaming)	Objavljivanje ili slanje napadnih, emotivno obojenih i uvredljivih komentara onlajn sa namerom da se drugi ljudi isprovociraju, da se izazove bes ili započne konflikt.
Zakon o autorskim pravima	Pravni okvir koji stvaraocima originalnih dela daje pravo upotrebe, reprodukovanja, distribucije i prilagođavanja njihovih dela.

BIBLIOGRAFIJA

Sve slike su preuzete sa platforme **Canva**.

Aboujaoude, E. (2022). "Protecting Privacy to Protect Mental Health: The New Ethical Imperative". *Journal of Medical Ethics*. **https://doi.org/10.1136/medethics-2018-105313**

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild". *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674-689. **https://dl.acm.org/doi/10.1145/2660267.2660347**

Baltacı, Ö., Bektas, M., & Kutlu, F. (2021). "Internet addiction, social anxiety, and coping strategies among university students: A cross-sectional study". *Journal of Research in Adolescence*, 31(3), 565-575.

Better Internet for Kids. (2020). *Insafe insights on...online reputation*. **https://www.betterinternetforkids.eu/practice/awareness/article?id=6668871**

Bucher, T. (2018). "If...Then: Algorithmic Power and Politics". *Oxford Studies in Digital Politics, New York, 2018; online edn, Oxford Academic*. **https://doi.org/10.1093/oso/9780190493028.001.0001**

Carrascal, J.P., et al. (2013). "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." *Computers in Human Behavior*, vol. 29, no. 2, 2013, pp. 340–349. **https://arxiv.org/abs/1112.6098**

Cataldo, I., Lepri, B., Neoh, M. J.-Y., & Esposito, G. (2021). "Social media usage and development of psychiatric disorders in childhood and adolescence: A review". *Frontiers in Psychiatry, 11*. **https://doi.org/10.3389/fpsyt.2020.508595**

Cyber Citizenship. (2023). *Digital Citizenship 101: Responsible Online Behavior*. **https://www.cybercitizenship.org/digital-citizenship-guide/**

ENISA. (2017). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. **https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines**

eSafety Commissioner. (2024). *Digital reputation*. **https://www.esafety.gov.au/key-topics/staying-safe/digital-reputation**

European Data Protection Supervisor. (2020). Guidelines on the Protection of Personal Data. **https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en**

Eurostat. (2024). *Young people - digital world.* **https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/39761.pdf**

Fardouly, J., Magson, N. R., Rapee, R. M., Johnco, C. J., & Oar, E. L. (2020). "The use of social media by Australian preadolescents and its links with mental health". *Journal of Clinical Psychology*, *76*(7), 1304–1326. **https://doi.org/10.1002/jclp.22936**

Gillespie, T. (2018). "Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media". *Yale University Press*. **http://dx.doi.org/10.12987/9780300235029**

Helberger, N. (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism*, *8*(6), 842–854. **https://doi.org/10.1080/21670811.2020.1773888**

Isin, E., & Ruppert, E. (2015). *Being Digital Citizens.* Rowman & Littlefield International, Ltd. ISBN/9781786614490. **https://rowman.com/WebDocs/Being_Digital_Citizens_Second_Ed_Open_Access.pdf**

Kaspersky. (2024). *What is a Digital Footprint?*. **https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint**

Kotobee Blog. (2024). *Game-Based Learning: What It Is and How to Apply It*. **https://blog.kotobee.com/game-based-learning/**

Kozyreva, A., Wineburg, S., Lewandowsky, S., Hertwig, R. (2022). "Critical Ignoring as a Core Competence for Digital Citizens." *Current Directions in Psychological Science* 32 (1): 81–88. Crossref. **https://journals.sagepub.com/doi/full/10.1177/09637214221121570**

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report 2009.* EU Kids Online Network. **http://eprints.lse.ac.uk/24372/**

McCrae, N., Gettings, S., & Purssell, E. (2017). "Social media and depressive symptoms in childhood and adolescence: A systematic review". *Adolescent Research Review*, 2, 315–330. **https://doi.org/10.1007/s40894-017-0053-4**

Netsafe. (2018). *From literacy to fluency to citizenship: Digital citizenship in education (2nd ed.)*. Wellington, NZ. **https://www.researchgate.net/publication/332886585**

Nolan, S., Hendricks, J., Ferguson, S., & Towell, A. (2017). "Social networking site (SNS) use by adolescent mothers: Can social support and social capital be enhanced by online social networks? – A structured review of the literature". *Midwifery*, 48, 24–31. **https://doi.org/10.1016/j.midw.2017.03.002**

OECD. (2022). *Is digital media literacy the answer to our disinformation woes?* The OECD Education Podcast. **https://www.oecd-ilibrary.org/education/is-digital-media-literacy-the-answer-to-our-disinformation-woes_326b63bf-en**

Oxford Dictionary. (n.d.). *Definition of 'digital citizenship.* **https://dictionary.cambridge.org/dictionary/english/digital-citizenship**

Popat, A., & Tarrant, C. (2023). "Exploring adolescents' perspectives on social media and mental health and well-being – a qualitative literature review". *Clinical Child Psychology and Psychiatry*, 28, 323–337. **https://doi.org/10.1177/13591045221092884**

Pretorius, C., Chambers, D., & Coyle, D. (2019). "Young People's Online Help-Seeking and Mental Health Difficulties: Systematic Narrative Review". *Journal of medical Internet research*, *21*(11), e13873, **https://doi.org/10.2196/13873**

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook*. Council of Europe. **https://rm.coe.int/16809382f9**

Ringrose, J., Gill, R., Livingstone, S. & Harvey, L. (2012). "A qualitative study of children, young people and 'sexting': A report prepared for the NSPCC". London: NSPCC. **https://www.researchgate.net/publication/265741962**

Sala, A., Porcaro, L., & Gómez, E. (2024). "Social Media Use and adolescents' mental health and well-being: An umbrella review". *Computers in Human Behavior Reports*, *14*, 100404. **https://doi.org/10.1016/j.chbr.2024.100404**

Scheinin, M. (2009). "Law and Security: Facing the Dilemmas". *SSRN Electronic Journal*. **http://dx.doi.org/10.2139/ssrn.1555686**

Secure Privacy. (2022). *The Ultimate Guide to Cookie Consent*. **https://secureprivacy.ai/blog/the-ultimate-guide-to-cookie-consent**

Senekal, J. S., Groenewald, G. R., Wolfaardt, L., Jansen, C., & Williams, K. (2023). "Social media and adolescent psychosocial development: A systematic review". *South African Journal of Psychology*, 53, 157–171. **https://doi.org/10.1177/00812463221119302**

Sharma, A. (2022). "Teaching Digital Privacy: Navigating the Intersection of Technology, Education, and Privacy." *Kanpur Historians*. Vol. IX, Issue II. **https://www.researchgate.net/publication/381952547_Teaching_Digital_Privacy_Navigating_the_Intersection_of_Technology_Education_and_Privacy**

Sheldon, R. (2023). *Navigating the Digital World: Online Reputation and Online Etiquette*. Igniyte. **https://www.igniyte.com/blog/navigating-the-digital-world-online-reputation-and-online-etiquette/**

Techopedia. (2023). *How to Protect Your Privacy Online*. **https://www.techopedia.com/how-to/how-to-protect-your-privacy-online**

Twenge, J. M., Haidt, J., Lozano, J., & Cummins, K. M. (2022). "Specification curve analysis shows that social media use is linked to poor mental health, especially among girls". *Acta Psychologica*, *224*, 103512. **https://doi.org/10.1016/j.actpsy.2022.103512**

UNICEF. (2023). *Digital civic engagement by young people*. **https://www.unicef.org/innocenti/reports/digital-civic-engagement-young-people**

G, V. (2024, July 31). *How can your digital footprint affect you in business opportunities?* Reputation Sciences. **https://www.reputationsciences.com/how-can-your-digital-footprint-affect-you/**

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills, and attitudes*. Publications Office of the European Union. **https://data.europa.eu/doi/10.2760/115376**

Webster, D., Dunne, L., & Hunter, R. (2021). „Association between social networks and subjective well-being in adolescents: A systematic review". *Youth & Society*, 53, 175–210. **https://doi.org/10.1177/0044118X20919589**

Wolford B, (n.d.), *What is GDPR, the EU's new data protection law?*, GDPR.eu, **https://gdpr.eu/what-is-gdpr/**

DIGICITY

GAME-BASED DIGITAL CITIZENSHIP

www.projectdigicity.eu

Sufinansira Evropska unija

Ovaj veb-sajt je finansiran sredstvima Evropske unije. Izraženi stavovi i mišljenja su, međutim, stavovi i mišljenja autora i ne odražavaju nužno stavove Evropske unije i nacionalne agencije Fondacija Tempus. Ni Evropska unija ni nacionalna agencija Fondacija Tempus ne mogu biti odgovorne za njih.

Kod projekta: 2023-2-RS01-KA220-YOU-000170562

LogoPsyCom PENS digiQ YuzuPulse