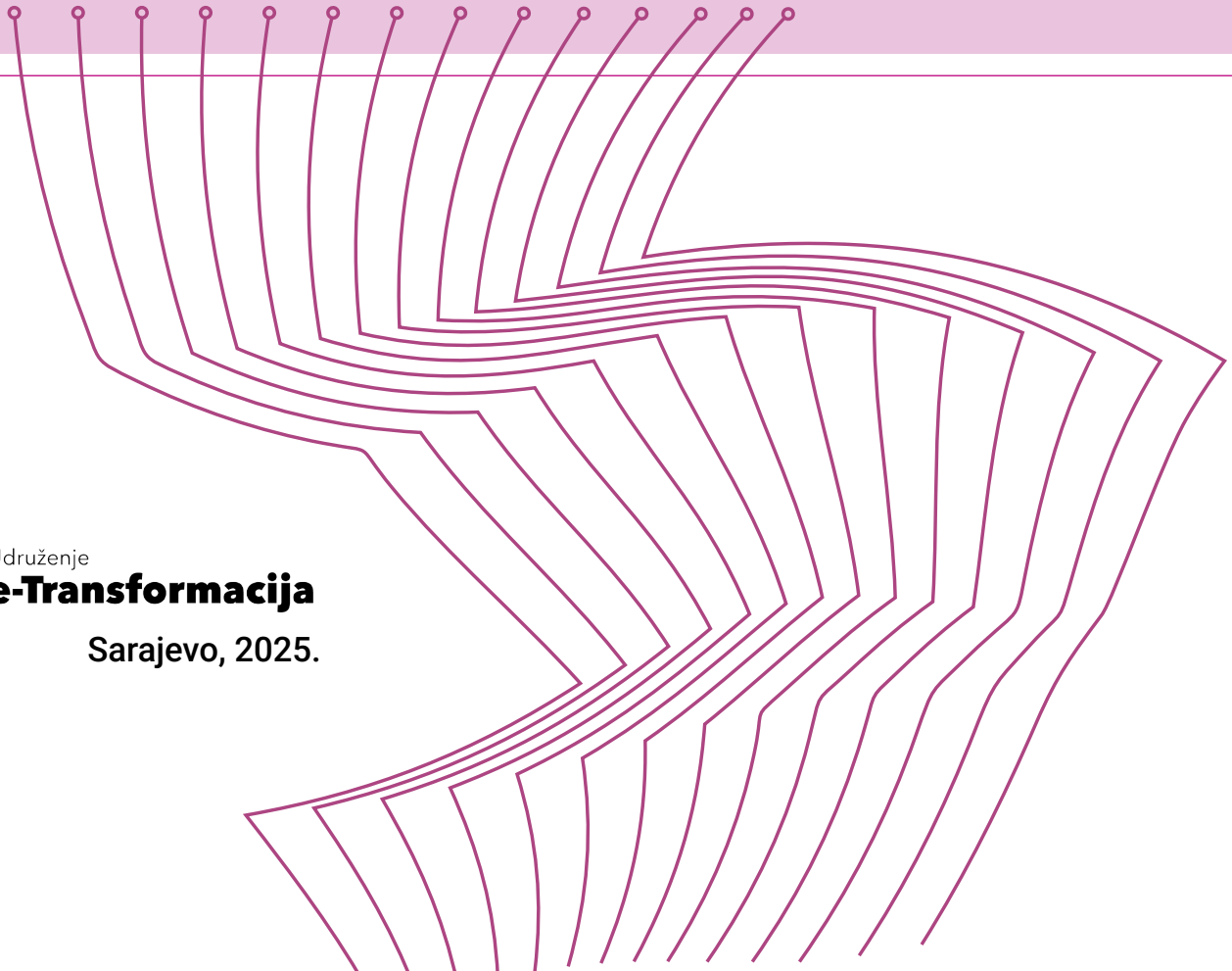
Sufinansira Europska unija
Switzerland.
german cooperation
DEUTSCHE ZUSAMMENARBEIT
Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

INTEGRACIJA TEMA CYBER SIGURNOSTI U NASTAVU

METODOLOŠKI VODIČ



Udruženje
e-Transformacija
Sarajevo, 2025.

Sadržaj

Predgovor

Ova publikacija nastala je kao odgovor na potrebu nastavnika za konkretnim, primjenjivim idejama koje mogu pomoći u oblikovanju smislenih, savremenih i angažovanih časova, posebno u oblastima kao što su informatika, građansko obrazovanje i vannastavne aktivnosti.

U vremenu kada učenici u učionicu dolaze s vrlo različitim predznanjima, iskustvima, interesovanjima i izazovima, zadatak nastavnika nije nimalo jednostavan, ali uz dobar alat, podršku i inspiraciju, može postati zanimljiv i učinkovit.

Metodološki vodič nudi nastavnicima prijedloge aktivnosti koje podržavaju razvoj znanja i vještina te njeguju kritičko mišljenje, odgovorno ponašanje, međusobno uvažavanje i povezanost sa stvarnim svijetom. Ideje predstavljene u ovom vodiču osmišljene su tako da mogu biti fleksibilno prilagođene uzrastu učenika, vremenskom okviru i kontekstu rada. U centru pažnje su učenik i njegovo aktivno učešće kroz istraživanje, diskusiju, analizu situacija, timski rad, igru i refleksiju.

Sadržaji se posebno oslanjaju na teme koje su i obrazovno i društveno značajne: sigurnost na internetu, digitalna pismenost, zaštita ličnih podataka, vršnjačka komunikacija i odgovorno ponašanje u digitalnom prostoru. Međutim, svaki prijedlog časova zamišljen je tako da se ne zadrži isključivo na informisanju, već da otvori prostor za razgovor, propitivanje i izgradnju stavova jer upravo u tome leži snaga obrazovanja.

Vodič je namijenjen prvenstveno nastavnicima informatike i građanskog obrazovanja, ali može biti koristan i u radu razrednika, školskih pedagoga, kao i svih onih koji s učenicima rade na razvijanju vještina za život i rad u savremenom digitalnom društvu.

1. Kako koristiti ovaj vodič?

Ovaj metodološki vodič osmišljen je kao praktičan resurs za nastavnike i stručne saradnike koji žele obogatiti svoje časove temama povezanim s digitalnim kompetencijama, građanskim odgojem i razvojem ličnih i socijalnih vještina. Njegova primjena je fleksibilna, a sadržaji se mogu prilagođavati uzrastu učenika, predmetu, vremenskom okviru i konkretnim obrazovno-vaspitnim ciljevima.

Ovaj vodič možete koristiti na više načina:

- Kao inspiracija za pojedinačne časove: kada želite obraditi konkretnu temu (npr. sigurnost na internetu ili govor mržnje);
- Kao tematski dodatak postojećem planu: u okviru redovne nastave informatike, građanskog obrazovanja, maternjeg jezika, i drugih predmeta;
- Za vannastavne aktivnosti: poput radionica, projekata, sekcija, Dana škole ili tematskih sedmica;
- Za međupredmetno povezivanje: kada više nastavnika zajednički planira aktivnosti kroz različite predmete;
- U radu sa manjim grupama ili razrednim odjeljenjem: kao dio odgojno-savjetodavnog rada, razrednih sastanaka ili časova odjeljenske zajednice.

Prilagodljivost i fleksibilnost

Nastavnici su ohrabreni da vodič ne koriste rigidno, već kao alat koji potiče kreativnost. Aktivnosti se mogu proširiti, skratiti, kombinovati ili mijenjati, u skladu s razrednom situacijom. Posebnu pažnju posvetite inkluzivnosti kako bi prilagodili sadržaj učenicima različitih sposobnosti, interesovanja i prethodnih znanja.

2. Šta obuhvata cyber sigurnost u nastavi?

Cyber sigurnost u obrazovanju nije zasebna lekcija, već skup znanja, vještina i stavova koje je važno integrisati u svakodnevni rad s učenicima. U ovom poglavlju predstavljene su ključne tematske cjeline, njihova povezanost sa ishodima učenja i kompetencijama, te metodološki pristupi koji olakšavaju realizaciju sadržaja.

Cyber sigurnost u kontekstu školskog obrazovanja podrazumijeva:

- Prepoznavanje digitalnih prijetnji: phishing, krađa identiteta, štetni softver, lažne informacije.
- Zaštitu ličnih podataka: privatnost na internetu, podešavanje sigurnosnih postavki, sigurne lozinke.
- Digitalno građanstvo i ponašanje: poštovanje drugih na mreži, prepoznavanje i prijavljivanje nasilja, odgovorna komunikacija.
- Samopouzdanje u snalaženju s incidentima: kome se obratiti, kako reagovati, kako pomoći drugima.
- Tehničke mjere zaštite: Osnovne informacije o antivirusima, ažuriranjima sistema, sigurnim postavkama na uređajima i aplikacijama.

Nije cilj uplašiti učenike, već ih osnažiti da prepoznaju rizike i znaju se zaštititi, kao i da razviju empatiju i odgovornost u digitalnom okruženju. Učionica je idealno mjesto za otvaranje ovih tema kroz diskusiju, istraživačke zadatke, simulacije i praktične vježbe. Nastava ne mora imati oblik formalnog tehničkog obrazovanja, naprotiv, najvažnije je povezati teme s realnim životnim iskustvima učenika.

Veza sa ključnim kompetencijama i ishodima učenja

Cyber sigurnost je direktno povezana sa razvojem digitalne kompetencije, ali i sa:

- Socijalnom i građanskom kompetencijom: razumijevanje prava i odgovornosti, empatija, aktivno učešće.
- Kompetencijom za rješavanje problema i donošenje odluka: analiziranje situacija, donošenje sigurnih odluka.
- Komunikacijskom kompetencijom: jasna, nenasilna i odgovorna komunikacija putem digitalnih kanala.

Ova tema se može integrisati u brojne nastavne predmete i oblasti: informatiku, građansko obrazovanje, jezik i komunikaciju, psihologiju, pa i vannastavne aktivnosti, poput učeničkih sekcija, debatnih klubova ili projektne nastave.

Preporučene metode i pristupi

U radu sa učenicima na temama cyber sigurnosti preporučuje se upotreba savremenih, participativnih i iskustvenih metoda koje omogućavaju aktivno učenje. Neke od njih su:

- **Diskusije i debate:** Pomažu učenicima da razvijaju kritičko mišljenje i izražavaju stavove o temama koje se odnose na digitalni svijet.
- **Analiza slučajeva (case studies):** Učenici istražuju stvarne ili simulirane situacije i uče kako reagovati u slučaju sigurnosnih prijetnji.
- **Učenje putem igre:** Korištenje edukativnih igara (digitalnih ili papirnih) koje simuliraju sigurnosne scenarije i promovišu donošenje odgovornih odluka.
- **Projektni rad i istraživanje:** Učenici samostalno ili u timovima razvijaju rješenja za specifične probleme ili izrađuju promotivne materijale (plakate, prezentacije, video zapise) na temu sigurnosti.
- **Igra uloga:** Učenici iz perspektive „žrtve“, „posmatrača“, „počinitelja“ razrađuju incident i mogućnosti reagovanja.
- **Gostujući predavači i radionice:** Uključivanje stručnjaka iz IT sektora, policije ili nevladinih organizacija može dodatno osnažiti učenike i dati praktične uvide.
- **Vježbe sa digitalnim alatima:** Podešavanje privatnosti, kreiranje sigurnih lozinki, provjera izvora.
- **Kritička analiza medijskih sadržaja:** Prepoznavanje dezinformacija, senzacionalizma i manipulacije.
- **Unplugged pristup:** Korištenje aktivnosti koje ne zahtijevaju računar, ali uvode učenike u koncepte digitalne sigurnosti kroz igre uloga, kartice, simulacije i brainstorming.

Ključno je da aktivnosti budu prilagođene uzrastu učenika, njihovom digitalnom iskustvu i kontekstu škole. Nastavnik pritom ima ulogu facilitatora koji učenike podstiče na razmišljanje, postavljanje pitanja i donošenje odgovornih odluka.

3. Prijedlozi za časove i aktivnosti

Informatika

U okviru nastave informatike, tema cyber sigurnosti može se prirodno integrisati kroz sadržaje koji se odnose na zaštitu ličnih podataka, prepoznavanje prijetnji na internetu i odgovorno digitalno ponašanje. Ispod su prikazane preporučene teme i prijedlozi aktivnosti koji se mogu realizovati kao zasebni časovi ili kao moduli unutar šireg tematskog bloka. Svaki prijedlog tema uključuje cilj, kratak opis, prijedlog aktivnosti i preporučene metode rada.

Tema: Digitalne prijetnje

Cilj: Učenici prepoznaju najčešće prijetnje u digitalnom okruženju (npr. lažne poruke, nepoznati linkovi, prevare, sumnjivi kontakti, zlonamjerni softver).

Opis: Kroz niz praktičnih i interaktivnih aktivnosti učenici istražuju najčešće oblike digitalnih prijetnji, analiziraju stvarne ili simulirane primjere i razvijaju strategije za zaštitu sebe i drugih u online okruženju. Aktivnosti uključuju diskusije, igre uloga i timski rad, uz poseban naglasak na razvoj kritičkog mišljenja i digitalne odgovornosti.

Prijedlog aktivnost:

Igra "Sumnjiva poruka" (učenje kroz igru uloga)

Cilj je da učenici prepoznaju elemente sumnjive poruke (npr. nepoznati pošiljalac, hitnost, zahtjev za ličnim podacima). Za ovu aktivnost je potrebno pripremiti 6–8 primjera poruka, e-mail i/ili poruke na društvenim mrežama (neke su bezopasne, neke imaju elemente *phishinga*[1]). Učenici (ili grupe) glume „primaoce" i diskutuju: da li biste otvorili ovu poruku? Zašto da / zašto ne? Mogu glasati tako da podignu crvenu karticu ako je sumnjiva, zelenu ako je sigurna.

Digitalni slučaj

Svaka grupa dobija „digitalni slučaj[2]" koji treba analizirati i otkriti u čemu je prijetnja (npr. phishing poruka putem e-maila kojom se traži da se klikne na ponuđeni link koji vodi na

---

[1] *Phishing je oblik digitalne prevare u kojem napadač pokušava navesti osobu da dobrovoljno otkrije osjetljive podatke poput korisničkog imena, lozinke, broja bankovne kartice ili drugih ličnih informacija. To se najčešće postiže putem poruka koje izgledaju kao da dolaze od pouzdanih izvora (npr. banka, škola, pošta, društvene mreže), a sadrže lažne linkove ili privitke.*

[2] *Digitalni slučaj je simulirana situacija koja prikazuje realan problem ili prijetnju u digitalnom okruženju, s ciljem da učenici analiziraju informacije, otkriju rizike i predlože ispravne reakcije. Služi kao studija slučaja prilagođena uzrastu i iskustvu učenika.*

zlonamjernu stranicu; poruka na društvenim mrežama od nepoznate osobe za npr. saradnju u gejmerskom turniru putem koje se traži broj telefona i adresa za slanje "nagrade" s turnira; lažne nagradne igre za npr. "besplatni mobilni uređaj" koji je dobijen kroz nagradnu igru, a uslov je da se proslijedi još 5 osoba i da se unesu lični podaci, i sl.)

Kratka debata

Debata može biti na temu „Da li je internet sigurno mjesto?" sa argumentima za i protiv.

Mapa rizika

Učenici kreiraju vizualnu mapu s prijetnjama i savjetima za prevenciju. Mapa se može izraditi na velikom hamer papiru, digitalno (Canva, Jamboard, MindMup) ili kao mentalna mapa, infografika, oblak riječi, dijagram ili ploča opasnosti i sigurnosti.

Kviz „Istina ili laž?"

Edukativna aktivnost osmišljena kako bi učenici naučili prepoznavati pouzdane i nepouzdane informacije na internetu. Cilj kviza je razvijanje kritičkog mišljenja i digitalne pismenosti kroz interaktivnu igru. Kviz se može realizovati uz pomoć kartica s oznakama „ISTINA" i „LAŽ" tako da učenici dižu kartice u zrak s odgovorima; na tabli ili papiru s označenim tvrdnjama (A, B, C...), pa učenici zaokružuju odgovore; diskusijom nakon svakog odgovora: Zašto je nešto tačno ili netačno? ili uz pomoć besplatnih alata za kvizove: Kahoot, Quizizz, Mentimeter, Google Forms.

Preporučene metode rada: učenje putem igre/igra uloga, analiza slučaja, grupni rad, vođena diskusija, debata, kreativno izražavanje/vizualna prezentacija, kviz, brainstorming.

Upute za nastavnike – simulacija phishing poruke: Simulaciju prepoznavanja phishing poruke moguće je izvesti na više načina, u zavisnosti od uzrasta učenika, dostupne opreme i ciljeva časa. Jedna od opcija je unplugged aktivnost, odnosno varijanta bez korištenja računara, pogodna za mlađe uzraste ili u situacijama kada tehnička oprema nije dostupna. Nastavnik može prikazati primjer lažne poruke (npr. phishing e-mail) bilo odštampane na papiru, podijeljene učenicima, ili projicirane na tabli. Uz poruku, učenici dobijaju i kopiju formulara koji napadač navodno traži da ispune. Njihov zadatak je da prepoznaju šta im u poruci djeluje sumnjivo (npr. neobična e-mail adresa, hitan ton poruke, traženje JMBG-a), da argumentuju da li bi unijeli tražene podatke i da predlože kako bi provjerili vjerodostojnost poruke. Ova metoda podstiče analitičko razmišljanje, diskusiju i kritički pristup informacijama.

Druga opcija uključuje korištenje tehnologije, kroz interaktivnu simulaciju phishing poruke putem digitalnog formulara. Ova verzija je prikladnija za starije učenike. Nastavnik može kreirati jednostavan formular koji izgleda realistično, kao što bi to učinili napadači, koristeći alate poput Google Forms ili Microsoft Forms. Učenicima se "šalje" link kao da dolazi od poznate institucije (npr. škola, banka, online platforma). Zadatak učenika je da procijene da li bi kliknuli na taj link, da li bi unijeli podatke i da obrazlože šta ih je eventualno navelo da posumnjaju. Nakon toga, nastavnik obavezno pojašnjava da se radi o simulaciji i objašnjava razliku između legitimnih i sumnjivih poruka.

Napomena: Važno je napomenuti da tokom ove aktivnosti ne treba prikupljati stvarne lične podatke. Učenicima se može reći da unesu izmišljene informacije (npr. "Unesi bilo koji broj") kako bi se očuvala sigurnost i etičnost aktivnosti. Takođe, ako koristite Google Forms, preporučuje se isključivanje opcije za automatsko prikupljanje e-mail adresa

kako bi simulacija bila što vjerodostojnija. Po završetku simulacije, ključno je voditi refleksivnu diskusiju sa učenicima o tome šta su naučili i kako ubuduće mogu prepoznati i izbjeći slične prijetnje.

Tema: Moji podaci na mreži

Cilj: Učenici razumiju koje informacije ne treba dijeliti online i razvijaju svijest o digitalnom identitetu.

Opis: Ova tema pomaže učenicima da razviju svijest o tome koje lične informacije ne treba dijeliti online, kako oblikuju svoj digitalni identitet i koji su potencijalni rizici nepromišljenog objavljivanja sadržaja. Aktivnosti je moguće prilagoditi različitim uzrastima, a nastavnici mogu birati između vizualnih, analitičkih i interaktivnih pristupa, u zavisnosti od vremena i tehničkih mogućnosti.

Prijedlog aktivnosti:

Igra „Profilna slagalica“

Ova igra je pogodna kao uvod u temu. Učenici dobijaju kartice s različitim informacijama (npr. ime, adresa, omiljeni sport, lokacija, fotografija zgrade/kuće, lozinka, broj kartice). Njihov zadatak je da kartice podijele u dvije grupe: sigurno za dijeljenje i nije preporučljivo dijeliti. Ova aktivnost može se realizovati fizički s isprintanim karticama, ili digitalno u alatima poput Padleta ili Jamboarda.

Digitalni slučaj

Analiza profila izmišljenih likova na društvenim mrežama (simulirani profili). Šta sve otkrivaju i koje rizike nose? Potrebno je da nastavnici unaprijed pripreme nekoliko lažnih profila (može i kao PowerPoint slajdovi) koji prikazuju različite vrste objava: od benignih (hobiji, kućni ljubimci) do problematičnih (javna lokacija, broj škole, fotografije s drugima bez dozvole). Učenici u grupama analiziraju šta ti profili otkrivaju o osobi, koje podatke bi napadači mogli iskoristiti i koje su moguće posljedice.

Diskusija

Diskusiju možete organizovati kroz pitanja poput: *Zašto bi neko dijelio privatne informacije?*, *Šta može poći po zlu ako objavim svoju adresu ili fotografiju druge osobe bez dozvole? Kako štitimo tuđe podatke online?* Ova diskusija podstiče kritičko promišljanje, empatiju i razvoj odgovornosti.

Izrada mini vodiča ili liste pravila „5 stvari koje nikad ne objavljujem online“

Učenici na kreativan način prave listu od 5 stvari koje nikad ne bi trebali objaviti online. Aktivnost može biti individualna ili grupna, uz korištenje alata poput Canve, PowerPointa ili papira i flomastera, u zavisnosti od dostupnih resursa.

Preporučene metode rada: učenje putem igre, analiza slučaja, rad u parovima/grupni rad, vođena diskusija, kreativno izražavanje/vizualna prezentacija, brainstorming.

Napomena za nastavnike: Istaknuti dvojak motiv: identitet/prisutnost i zaštita/bezopasnost. Dati učenicima osjećaj da kontrolišu svoju digitalnu prisutnost.

Tema: Lozinka kao ključ

Cilj: Učenici će razumjeti važnost kreiranja jake lozinke i naučiti pravila za sigurno upravljanje lozinkama.

Opis: Kroz niz interaktivnih i problemski usmjerenih aktivnosti, učenici istražuju ulogu lozinki u digitalnoj sigurnosti. Uče prepoznati slabe i jake lozinke, pravila sigurnog upravljanja lozinkama i posljedice neodgovornog ponašanja. Aktivnosti potiču saradnju, razmjenu mišljenja i kreativno izražavanje.

Prijedlog aktivnosti:

Edukativna igra "Crvenkapa: Slučaj ukradene lozinke"

Učenici u manjim grupama prate zanimljivu priču u kojoj otkrivaju koje su greške Crvenkapa i njena baka napravile prilikom kreiranja i čuvanja lozinki. Kroz niz zadataka i scenarija, učenici uče prepoznati loše lozinke, razumiju zašto nisu sigurne i zajednički predlažu bolja rješenja. Igra je dostupna na sljedećem linku: https://zuns.me/sites/interaktivni-materijal/slucaj-ukradene-lozinke/

Diskusija

Nakon igre se preporučuje organizovati vođenu diskusiju u kojoj učenici dijele svoja zapažanja, iskustva i zajednički formulišu zaključke o naučenom.

Takmičenje „Lozinka izazov"

Takmičenje „Lozinka izazov" može dodatno motivisati učenike. Cilj je osmisliti najsigurniju lozinku uz pomoć digitalnih alata kao što je passwordmeter.com. Učenici mogu testirati više verzija i ocjenjivati jedni drugima izmišljene lozinke prema kriterijima sigurnosti (dužina, kombinacija brojeva, slova i simbola, nepredvidivost). Ova aktivnost može biti individualna ili timska. Objasniti učenicima da se ne preporučuje unos stvarnih lozinki na bilo koju online stranicu za testiranje jačine lozinki, čak ni one koje izgledaju pouzdano.

Mini poster „Moja tajna lozinka"

Za kreativno izražavanje, možete organizovati izradu mini postera „Moja tajna lozinka". Učenici kreiraju postere s pravilima kojih će se ubuduće pridržavati kada kreiraju lozinke (npr. Ne koristim ime ljubimca, Ne dijelim lozinke s prijateljima, Svaka platforma treba da ima svoju lozinku). Posteri se mogu praviti ručno ili digitalno, koristeći alate kao što su Canva ili PowerPoint.

Escape room igra „Tajna soba"

Dodatno, možete pripremiti igru „Tajna soba" – jednostavnu escape room simulaciju u učionici. Učenici rješavaju niz zadataka (npr. anagrame, poruke skrivene u QR kodovima, logičke zagonetke) čiji odgovori vode do pravilno kreirane lozinke. Tek kada otkriju ispravnu lozinku, "izlaze" iz sobe. Ova aktivnost jača timski rad, logičko razmišljanje i primjenu znanja u praksi.

Preporučene metode rada: učenje putem igre, grupni rad/timski rad, vođena diskusija, takmičenje kao oblik aktivnog učenja/problemski zadatak, kreativno izražavanje/vizuelna prezentacija, brainstorming.

Građansko obrazovanje i odjeljenska zajednica

U okviru građanskog obrazovanja i odjeljenske zajednice, teme iz oblasti cyber sigurnosti mogu se obraditi iz perspektive digitalnih prava, odgovornosti i međuljudskih odnosa u online okruženju. Fokus je na izgradnji kritičkog razmišljanja, digitalne etike i razvijanju empatije kod učenika u virtualnim interakcijama.

Tema: Digitalno društvo – moja prava i odgovornosti na internetu

Cilj: Učenici razvijaju razumijevanje za sigurno, odgovorno i etičko ponašanje u digitalnom prostoru kroz saradnički rad i diskusiju.

Opis: Ova tema pomaže učenicima da razumiju kako njihova ponašanja u digitalnom prostoru utiču na druge, kao i koja su njihova prava i odgovornosti kao digitalnih građana. Kroz analizu primjera, diskusije i zajednički rad, učenici razvijaju osjećaj za pravednost, sigurnost, poštovanje i etičnost u online okruženju. Aktivnosti su osmišljene tako da podstiču timsku saradnju, kritičko mišljenje i uključivanje svakog učenika u proces donošenja pravila.

Prijedlog aktivnosti:

Analiza slučaja – digitalni izazov

Učenici rade u manjim grupama. Svaka grupa dobija konkretan primjer digitalnog izazova ili problema poput vrijeđanja u grupnom četu, doxinga[3] ili ignorisanja osnovnih pravila netiketiranja. Zadaci se mogu pripremiti unaprijed na papirima ili digitalno (npr. kao slajdovi). Grupa analizira situaciju, razgovara o mogućim posljedicama za pojedinca i zajednicu, te predlaže kako bi se trebalo pravilno reagovati.

Izrada pravila odgovornog ponašanja na internetu

Svaka grupa osmišljava i kreira 3 do 5 pravila za sigurno i odgovorno ponašanje u digitalnom okruženju. Pored svakog pravila, učenici zapisuju kratko objašnjenje – zašto je to pravilo važno, kome pomaže i kako doprinosi sigurnijoj online zajednici.

Prezentacija i zajednička diskusija

Grupe predstavljaju svoja pravila cijelom razredu. Nastavnik facilitira diskusiju – poredе se prijedlozi, razgovara se o sličnostima, razlikama i zajednički se biraju najbolja i najrelevantnija pravila. Kroz ovaj proces, učenici uče uvažavati tuđe mišljenje i zajednički donositi odluke.

Izrada plakata/postera "Digitalni etički kodeks"

Na osnovu prijedloga svih grupa, zajedno se sastavlja razredni „Digitalni etički kodeks" na kojem će se nalaziti skup najvažnijih pravila koja učenici prihvataju kao svoja. Kodeks se može zapisati na veliki papir, ilustrovati i postaviti na vidljivo mjesto u učionici, kao podsjetnik na prava i obaveze u digitalnom prostoru. Kodeks može biti i digitalno dizajniran koristeći alate poput Canva, PowerPoint ili Padlet, u zavisnosti od tehničkih mogućnosti škole.

Preporučene metode rada: analiza slučaja, grupni rad, razgovor i vođena diskusija, brainstorming, zajednička prezentacija i vizualizacija (plakat, infografika, digitalni poster).

---

3 *Doxxing je objavljivanje tuđih ličnih podataka na internetu bez dozvole.*

Tema: Cyber nasilje i podrška vršnjacima

Cilj: Učenici razvijaju sposobnost prepoznavanja i razumijevanja tuđih emocija, te postaju svjesni važnosti reagovanja u situacijama nasilja. Uče da pasivno posmatranje doprinosi problemu, te da svako ima odgovornost da reaguje i pruži podršku vršnjacima koji su izloženi nasilju.

Opis: Kroz kreativne i interaktivne aktivnosti učenici istražuju različite uloge u situacijama cyber nasilja, razvijaju empatiju i prepoznaju kako njihovo ponašanje može utjecati na digitalnu zajednicu. Aktivnosti potiču saradnju, refleksiju i osnaživanje za pozitivnu reakciju i podršku vršnjacima.

Prijedlog aktivnosti:

Kreativna radionica "U tuđim cipelama"

Učenici se dijele u manje grupe i osmišljavaju kratke scene ili stripove koji prikazuju situaciju cyber nasilja iz perspektive žrtve, posmatrača i počinitelja. Fokus je na izražavanju emocija likova i njihovim reakcijama, što pomaže učenicima da bolje razumiju različite aspekte problema.

Vođena diskusija

Nakon predstavljanja scena ili stripova, organizuje se moderirana diskusija s pitanjima poput: *Kako se osjećala osoba koja je bila meta?* Šta je *moglo biti učinjeno drugačije? Ko je mogao reagovati i na koji način?* Diskusija jača kritičko mišljenje i osvještava važnost aktivnog reagovanja u borbi protiv cyber nasilja.

Scenario i uloga "Reagujmo zajedno"

Organizuje se igra uloga gdje učenici simuliraju situacije u kojima svjedoče cyber nasilju i zajedno osmišljavaju načine reagovanja i pružanja podrške. Aktivnost razvija socijalne vještine, samopouzdanje i osjećaj odgovornosti.

Izrada plakata "Podrška vršnjacima"

Učenici u grupama kreiraju plakate s porukama podrške i savjetima kako pomoći vršnjacima koji su izloženi cyber nasilju. Plakati mogu biti ručni ili digitalni (Canva, PowerPoint), a cilj je vizualno predstaviti ideje o empatiji, hrabrosti i zajedništvu.

Preporučene metode rada: učenje putem igre, igra uloga, grupni/timski rad, vođena diskusija, kreativno izražavanje, brainstorming.

Tema: Online reputacija – kakav digitalni trag ostavljam?

Cilj: Osvijestiti dugoročan uticaj online ponašanja i potaknuti odgovorno upravljanje ličnim digitalnim identitetom.

Opis: Kroz analizu izmišljenih online profila, refleksivne vježbe i diskusije, učenici preispituju svoje digitalno ponašanje i razumiju kako njihove objave, komentari i interakcije oblikuju način na koji ih drugi vide. Aktivnosti potiču kritičko mišljenje, samoprocjenu i izgradnju odgovorne online reputacije.

Prijedlog aktivnosti:

Analiza slučaja "Profil u ogledalu"

Nastavnik priprema nekoliko izmišljenih online profila (npr. prikazi društvenih mreža, komentara ispod objava, fotografija). Učenici u grupama analiziraju profile i vode diskusiju uz pitanja: *Kakvu sliku ta osoba ostavlja? Da li biste joj vjerovali, sprijateljili se s njom, zaposlili je? Koje su moguće posljedice objavljenih sadržaja*? Ova aktivnost razvija vještine digitalne pismenosti i promišljanja o posljedicama digitalnih izbora.

Lični digitalni otisak – refleksivna vježba

Učenici samostalno i refleksivno razmišljaju o vlastitom digitalnom prisustvu bilježeći odgovore na pitanja poput: *Na kojim platformama su prisutni? Kakav sadržaj najčešće objavljuju? Kako bi ih neko drugi mogao doživjeti na osnovu tih tragova?* Nastavnik može ponuditi upitnik za vođeno samoprocjenjivanje.

Zajednička diskusija: Kako bih volio/voljela da me drugi vide online?

U opuštenoj atmosferi, učenici dijele svoja razmišljanja o tome kakav digitalni imidž žele graditi. Diskusija podstiče svijest o autentičnosti, dosljednosti i balansu između privatnog i javnog online prostora.

Kreativni zadatak: Digitalni ID karton

Učenici izrađuju „Digitalni ID" – zamišljenu karticu koja prikazuje kako žele da ih drugi dožive online (npr. 3 ključne osobine, primjer pozitivne objave, "pravilo koje uvijek poštujem na internetu"). Rad može biti vizualan (ručno ili digitalno), a cilj je artikulisati vlastite vrijednosti i principe ponašanja u digitalnom prostoru.

Preporučene metode rada: analiza slučaja (simulirani profili), grupni rad, vođena refleksija, zajednička diskusija, kreativno izražavanje.

Napomena za nastavnike: Aktivnost se može realizovati i u okviru informatike, odjeljenske zajednice ili kao zasebna radionica. Poželjno je učenicima dati siguran prostor za dijeljenje mišljenja i iskustava, bez prosuđivanja.

Međupredmetna povezanost – medijska i informacijska pismenost

Teme iz oblasti cyber sigurnosti i odgovornog ponašanja na internetu ne tiču se samo jednog nastavnog predmeta. S obzirom na sveprisutnost digitalnih tehnologija u životu djece i mladih, važno je da škole pristupe ovim temama sistemski i integrisano. Kritičko promišljanje, zaštita privatnosti, prepoznavanje manipulacije i razumijevanje digitalnog identiteta samo su neke od vještina koje zahtijevaju kombinaciju tehničkog znanja, etičkog promišljanja i razvijenih komunikacijskih kompetencija.

Zato je važno prepoznati potencijal za međupredmetno povezivanje, čime se učenicima omogućava da sagledaju temu iz više perspektiva, razviju dublje razumijevanje i bolje prenose znanja u stvarne životne situacije.

U nastavku prikazujemo orimjer jedne nastavne teme koja se može uspješno integrisati i realizovati kroz više predmeta: informatiku, građansko obrazovanje, jezičke predmete i odjeljensku zajednicu, u skladu s ciljevima tih nastavnih oblasti i uz prilagodbu uzrastu učenika.

Tema: Kritička analiza medijskih sadržaja – Prepoznavanje dezinformacija, senzacionalizma i manipulacije

Cilj: Učenici razvijaju sposobnost kritičkog promišljanja o medijskim sadržajima, razlikuju tačne od netačnih informacija i prepoznaju elemente manipulacije u digitalnim medijima.

Opis: U okviru ove teme učenici uče kako prepoznati dezinformacije, senzacionalizam i pristrasne izvore u digitalnom prostoru. Kroz analizu konkretnih primjera vijesti, objava i komentara na internetu, učenici uče postavljati prava pitanja: Ko je izvor? Zašto je ovo objavljeno? Da li je informacija potvrđena? i sl. Aktivnosti podstiču razvoj medijske i informacione pismenosti, što je ključno za odgovorno digitalno društvo.

Prijedlog aktivnosti:

Analiza naslova

Učenicima se daju naslovi iz online medija (mogu biti stvarni, lažno senzacionalistički ili kombinovani). Njihov zadatak je da procijene koji su naslovi vjerodostojni, a koji prenaglašeni ili obmanjujući. Diskutuje se zašto su neki naslovi napisani tako da izazovu emocije, klikove ili širenje dezinformacija.

Uporedi i ocijeni

Učenici upoređuju dvije verzije iste vijesti s različitih portala (npr. profesionalni medij vs. neprovjerena stranica/blog). Analiziraju ton, izvore, činjenice i komentare. Cilj je identifikovati razlike u pristupu, vjerodostojnosti i mogućem uticaju na čitaoca.

"Dezinformacija ili činjenica?" – interaktivna aktivnost

Pripremiti kratke tekstove, tvrdnje ili slike (npr. viralan tvit, naslov, izjava) – neki su tačni, neki lažni. Učenici u parovima ili grupama donose odluku: **ČINJENICA** ili DEZINFORMACIJA i objašnjavaju svoju odluku. Mogu koristiti telefone/tablete za provjeru izvora (fact-

checking portali, Google, sl.). Aktivnost se završava diskusijom: Zašto smo povjerovali u nešto netačno? Kako možemo provjeravati informacije?

Mini istraživanje i prezentacija

Učenici biraju jedan viralni mit, dezinformaciju ili teoriju zavjere (npr. o tehnologiji, zdravlju, slavnima) i istražuju šta je istina. Pripremaju kratku prezentaciju: Šta je tvrdnja? Ko je izvor? Koji su dokazi za/ protiv? Kako se širila? Šta možemo naučiti?

Izrada postera: „Kako prepoznati dezinformaciju?"

Kao završna aktivnost, učenici u grupama izrađuju vizualni prikaz pravila/provjera za razotkrivanje lažnih informacija (npr. „Pročitaj više od naslova", „Provjeri izvor", „Ne vjeruj viralnom bez dokaza"). Posteri se mogu izraditi digitalno (Canva, PowerPoint) ili ručno (plakati).

Preporučene metode rada: Kritička analiza sadržaja, rad u paru i grupni rad, vođena diskusija, brainstorming, mini istraživanje, kreativno izražavanje (vizualna prezentacija), analiza slučaja, kviz.

Vannastavne aktivnosti i tematski dani

Vannastavne aktivnosti i tematski dani omogućavaju dodatnu fleksibilnost i kreativnost u radu sa učenicima, uz veće uključivanje zajednice, roditelja i stručnjaka. Teme vezane za digitalnu sigurnost mogu biti osnova za projekte, kampanje ili školske događaje.

Cilj: Učenici preuzimaju aktivnu ulogu u promociji sigurnog ponašanja online i podršci vršnjacima.

Prijedlog aktivnosti:

Formiranje školskog tima/sekcije „Digitalna patrola"

Odabrana grupa učenika (po prijavi, izboru ili preporuci) djeluje kao promotivni i savjetodavni tim u školi. Njihove glavne uloge uključuju: planiranje i realizaciju kampanja i edukativnih događaja; saradnju s nastavnicima, bibliotekarima, roditeljima i lokalnim stručnjacima (npr. IT stručnjaci, policija).

Izrada promotivnih materijala

Članovi tima osmišljavaju i kreiraju plakate, brošure, infografike, video poruke, digitalne postove i podcast epizode s porukama o sigurnosti, podršci, prevenciji nasilja i važnosti jakih lozinki, digitalne reputacije i odgovornog ponašanja. Materijali se dijele putem oglasnih tabli, školskog sajta, društvenih mreža i na događajima.

Kutija povjerenja

Postavljanje fizičke ili digitalne kutije putem koje učenici mogu anonimno prijavljivati situacije digitalnog nasilja, uvreda, prijetnji ili drugih neugodnih iskustava. Digitalna patrola uz podršku nastavnika i stručnih saradnika (pedagog, socijalni pedagog, psiholog) analizira prijave i pokreće preventivne aktivnosti.

Intervju sa stručnjakom: Digitalni svijet iz prve ruke

Učenici se organizuju u grupe i pripremaju pitanja za gostujuću osobu – to može biti inspektor za cyber kriminal, IT stručnjak, administrator mreža, pravnik ili psiholog koji

se bavi digitalnim temama. Intervju se može realizovati uživo (u školi, zajednici) ili online (npr. putem Google Meet-a). Svaka grupa dobija određenu temu za istraživanje (npr. zaštita podataka, prevencija online nasilja, uloga policije u borbi protiv digitalnog kriminala) i vodi jedan dio intervjua. Nakon intervjua slijedi zajednička refleksija: Šta smo naučili? Šta nas je iznenadilo? Kako se to znanje može primijeniti u svakodnevnom digitalnom ponašanju?

Debata: „*Privatnost vs. sigurnost* – šta je važnije?“

Učenici se dijele u dvije debatne grupe: jedna zastupa pravo na privatnost, druga važnost sigurnosti. Priprema uključuje istraživanje zakona, primjera iz stvarnog života, tehnoloških aspekata i moralnih dilema. Organizuje se strukturisana debata sa jasno definisanim pravilima, ulogama moderatora, publike i sudija. Nakon debate slijedi kratka diskusija u kojoj svi učenici mogu iznijeti svoje lično mišljenje bez obaveze zauzimanja strana.

4. Preporučeni alati i digitalni resursi

U nastavku slijedi niz korisnih digitalnih alata i platformi koje mogu pomoći nastavnicima u izvođenju aktivnosti, kao i učenicima u učenju o digitalnoj sigurnosti:

Alati za kvizove i diskusiju

Kahoot! – Interaktivni kvizovi, odlični za provjeru znanja i uvod u temu.

Mentimeter – Alat za izradu anonimnih anketa, oblačića riječi, pitanja i refleksija.

Padlet – Digitalna tabla za grupno izražavanje mišljenja, postavljanje sadržaja, komentara i ideja.

Google Forms – Kreiranje online upitnika i testova.

Alati za kreativno izražavanje

Canva – Jednostavan alat za pravljenje postera, stripova, brošura i prezentacija.

Storyboard That – Alat za kreiranje stripova i vizualizaciju scenarija.

Powtoon / Animaker – Alati za kreiranje kratkih animiranih video sadržaja.

Audacity – Besplatan program za snimanje i uređivanje zvuka, koristan za snimanje podcast epizoda.

PhotoPea – Online alternativa Photoshopu, radi bez instalacije.

Alati za testiranje sigurnosti lozinki

PasswordMeter (www.passwordmeter.com) – Alat za testiranje jačine lozinke uz detaljnu analizu i preporuke.

How Secure Is My Password? (www.security.org/how-secure-is-my-password/) – Prikazuje koliko bi vremena bilo potrebno hakeru da probije lozinku.

Primjena: Učenici mogu testirati izmišljene lozinke, analizirati faktore sigurnosti i naučiti kako kreirati jake lozinke. Ne preporučuje se unos stvarnih lozinki.

Alati za izradu i korištenje QR kodova

QR Code Generator (www.qr-code-generator.com) – Alat za izradu QR kodova koji vode ka edukativnim sadržajima, kvizovima, pravilima ponašanja ili posterima.

QR Code Monkey (www.qrcode-monkey.com) – Omogućava kreiranje personalizovanih QR kodova sa bojama, logotipom i više opcija formata.

Canva QR Code opcija – Korisno za uključivanje QR kodova direktno u promotivne materijale (plakati, brošure).

Primjena: QR kodovi se mogu koristiti za escape room tragove, pristup kvizovima, online materijalima, pravilima i savjetima za digitalnu sigurnost.

Alati za escape room igre i simulacije

Google Forms + QR kodovi – Mogu poslužiti za kreiranje zadataka i tragova unutar digitalnog escape rooma (npr. pitanja, zagonetke, lozinke za pristup sljedećem koraku).

Flippity (www.flippity.net) – Platforma za pravljenje digitalnih igara i zadataka, uključujući kvizove, anagrame i interaktivne escape room izazove.

Genially – Napredniji alat za izradu vizualno atraktivnih interaktivnih escape igara i edukativnih prezentacija.

Wordwall / LearningApps – Za zadatke tipa spajanja pojmova, višestrukog izbora, sortiranja informacija itd.

Edukativne platforme i materijali

Better Internet for Kids (www.betterinternetforkids.eu) – Evropski portal sa brojnim edukativnim resursima za nastavnike, roditelje i djecu.

Centar za sigurni internet (www.sigurnodijete.ba) – Platforma na bosanskom jeziku s priručnicima, video lekcijama i savjetima.

Common Sense Education (www.commonsense.org/education) – Priznati resurs za digitalnu pismenost i građanstvo, sa gotovim lekcijama i planovima.

Google Be Internet Awesome – Interaktivna igra „Interland“ i materijali za poučavanje djece sigurnosti na internetu.

NetSmartz / NSTeens – Edukativne animacije, video i kvizovi o online rizicima.

Ova publikacija je objavljena u sklopu implementacije projekta Cyber Security education program a u okviru SEDEP programa, koji sufinansiraju Njemačko savezno ministarstvo za ekonomsku saradnju i razvoj (BMZ), Evropska unija i Švicarska vlada. Sadržaj ove publikacije isključiva je odgovornost Udruženja e-Transformacija i ne odražava nužno stavove njemačke vlade, švicarske vlade ili Evropske unije.