Sveučilište u Zagrebu

Fakultet hrvatskih studija

Pedagoško-psihološko-metodičko-didaktičko obrazovanje nastavnika

Kolegij: Praktičnih vježbi predmetne metodike

PRIPREMA ZA SAT RAZREDNIKA

Radionica:

Online sigurnost – kako se zaštititi i odgovorno ponašati na internetu

26. rujna 2026.

Srednja škola: _____

Tema, cilj i ishodi učenja, struktura i trajanje

- **Tema**: Online sigurnost – kako se zaštititi i odgovorno ponašati na internetu

- **Cilj radionice**: Razvijati kod učenika svijest o sigurnom, odgovornom i kritičkom korištenju interneta te ih osposobiti za prepoznavanje potencijalno rizičnih situacija u online okruženju i primjenu osnovnih načela zaštite osobnih podataka, privatnosti i digitalnog identiteta.

- **Ishodi učenja**: Učenici će moći:
  - ✓ objasniti pojam online sigurnosti i navesti njezine osnovne sastavnice;
  - ✓ prepoznati potencijalno rizične situacije na internetu;
  - ✓ razlikovati sigurne i nesigurne načine dijeljenja osobnih podataka;
  - ✓ objasniti važnost korištenja snažnih i različitih lozinki te dodatne autentifikacije;
  - ✓ prepoznati pokušaje prijevare, krađe podataka i manipulacije na internetu;
  - ✓ objasniti što učiniti u slučaju uznemiravanja, prijetnji ili drugog neprimjerenog ponašanja na internetu;
  - ✓ procijeniti vlastite navike korištenja interneta i predložiti načine za njihovo poboljšanje.
  - ✓ Zaključiti o kvaliteti i korisnosti provedene radionice i novih saznanja o online sigurnosti

- **Teorijska razrada**:

  Internet i digitalne tehnologije važan su dio svakodnevnog života djece i adolescenata. Digitalno okruženje mladima omogućuje komunikaciju, učenje, zabavu, stvaranje sadržaja i održavanje odnosa s vršnjacima, ali istodobno može biti povezano s različitim rizicima. Zbog toga se online sigurnost ne odnosi samo na tehničku zaštitu uređaja, nego i na razvoj znanja i vještina potrebnih za **zaštitu privatnosti i osobnih podataka, sigurno korištenje digitalnih računa, kritičko procjenjivanje sadržaja te odgovorno ponašanje prema drugim korisnicima.**

  Livingstone (2014) ističe da je za sigurno sudjelovanje mladih u digitalnom okruženju važna **društvena i digitalna pismenost**. Djeca i adolescenti nisu samo pasivni korisnici

interneta, već aktivno komuniciraju, stvaraju i dijele sadržaje te stupaju u različite društvene odnose. Zbog toga trebaju razvijati sposobnost prepoznavanja mogućnosti i rizika pojedinih online situacija te razumijevanja posljedica vlastitog ponašanja. Autorica posebno naglašava važnost toga da djeca nauče sama procjenjivati što je u određenoj digitalnoj situaciji rizično i zašto je rizično (Livingstone, 2014).

Jedno od temeljnih područja online sigurnosti jest **zaštita osobnih podataka i privatnosti**. Učenici trebaju osvijestiti da informacije koje objavljuju na internetu mogu ostaviti trajni digitalni trag. To se odnosi na fotografije, videozapise, komentare, lokaciju, adresu, broj telefona, podatke o školi i druge osobne informacije. UNICEF Europe and Central Asia, (n. d.) preporučuje razgovor s djecom o tome što objavljuju, s kim dijele informacije i tko može vidjeti njihove objave. Također ističe važnost korištenja postavki privatnosti te promišljanja prije objavljivanja fotografija, videozapisa i drugih sadržaja.

Zaštita privatnosti povezana je i s **digitalnim identitetom.** Digitalni identitet oblikuje se kroz različite informacije i sadržaje koji su povezani s pojedincem u digitalnom prostoru. Ono što osoba objavljuje, ali i ono što drugi objavljuju o njoj, može utjecati na način na koji je drugi doživljavaju. UNICEF Europe and Central Asia, (n. d.) posebno upozorava da jednom podijeljen sadržaj može biti teško u potpunosti ukloniti i kontrolirati njegovo daljnje širenje. Zbog toga je učenike važno poticati da prije objavljivanja razmisle o mogućim posljedicama vlastitog ponašanja.

Važan dio online sigurnosti jest i **zaštita korisničkih računa**. Lozinke predstavljaju jedan od osnovnih načina zaštite pristupa digitalnim računima, ali same po sebi nisu dovoljna zaštita. Prema Nacionalnom institutu za standarde i tehnologiju (National Institute of Standards and Technology [NIST], 2025), preporučuje se korištenje dugih lozinki odnosno zaporki, izbjegavanje ponavljanja iste lozinke na različitim računima te korištenje višefaktorske autentifikacije kada je dostupna. NIST posebno naglašava da ponovna uporaba iste lozinke predstavlja rizik jer kompromitiranje jednog računa može ugroziti i druge račune na kojima se koristi ista lozinka (NIST, 2025).

Učenici također trebaju razviti sposobnost prepoznavanja **phishinga i drugih oblika internetskih prijevara**. Phishing uključuje pokušaje da se korisnika navede na otkrivanje osjetljivih podataka, primjerice korisničkog imena i lozinke, često putem lažnih poruka i internetskih stranica koje izgledaju kao da pripadaju poznatim i pouzdanim organizacijama (NIST, 2025). Učenike je zato korisno poučiti da budu oprezni prema

porukama koje stvaraju osjećaj hitnosti, traže osobne podatke, zahtijevaju klikanje na poveznicu ili nude neuobičajene nagrade.

Online sigurnost obuhvaća i **odgovorno ponašanje prema drugim osobama**. Posebno područje predstavlja **elektroničko nasilje ili cyberbullying**. Hrabri telefon (n. d.) navodi primjere elektroničkog nasilja poput širenja neugodnih informacija, neovlaštenog objavljivanja fotografija ili videa te stvaranja lažnih profila. U slučaju nasilja preporučuje se ne uzvraćati nasilnim ponašanjem, sačuvati dokaze i obratiti se odrasloj osobi od povjerenja. Cyberbullying je različit od klasičnog bullyinga zbog specifičnih dinamika koje virtualno okruženje omogućuje. Dok je tradicionalno nasilje prostorno-vremenski ograničeno na prostore poput školske zgrade, elektroničko nasilje briše te granice. Žrtva je izložena napadima unutar vlastitog doma koji bi trebao predstavljati primarno sigurno okruženje. Nadalje, specifičnost je i u tome što "osobe koje se ponašaju nasilno mogu ti biti poznate ili nepoznate" (Hrabri telefon, n.d., odjeljak Što je elektroničko nasilje?), što počiniteljima omogućuje skrivanje iza prividne anonimnosti ekrana. Ta anonimnost dramatično pojačava osjećaj bespomoćnosti i straha kod žrtve jer se moć počinitelja u cyber prostoru više ne očituje kroz fizičku snagu, već kroz mogućnost brzog i masovnog širenja kompromitirajućeg sadržaja.

Posebno je važno razvijati **kritičko procjenjivanje informacija i sadržaja**. Učenici svakodnevno dolaze u kontakt s različitim informacijama, reklamama, objavama na društvenim mrežama, videozapisima i drugim digitalnim sadržajima. Livingstone (2014) naglašava da digitalna pismenost uključuje sposobnost razumijevanja i procjenjivanja različitih sadržaja i situacija u kojima se mladi susreću s mogućnostima i rizicima digitalnog okruženja. Učenike je stoga korisno poticati da razmisle o **tome tko je objavio određeni sadržaj, s kojom namjerom, odakle informacija dolazi i postoje li drugi pouzdani izvori koji je potvrđuju.**

Pri poučavanju online sigurnosti važno je pronaći ravnotežu između **zaštite učenika i razvoja njihove samostalnosti.** Livingstone i suradnici (2017), na temelju istraživanja provedenog na 6400 roditelja djece u dobi od 6 do 14 godina iz osam europskih zemalja, razlikuju restriktivnije i omogućavajuće oblike roditeljskog posredovanja. Rezultati upućuju na to da restriktivniji pristupi mogu biti povezani s manjim izlaganjem nekim online rizicima, ali istodobno mogu ograničiti određene online mogućnosti i razvoj digitalnih kompetencija. Autori stoga ističu važnost pristupa koji, uz sigurnosne mjere,

uzima u obzir i razvoj djetetovih digitalnih vještina i samostalnosti (Livingstone i sur., 2017).

Prema tome, cilj edukacije o online sigurnosti nije samo učenicima ponuditi popis zabrana, nego ih **osposobiti za samostalno prepoznavanje rizika, procjenjivanje situacija i odgovorno donošenje odluka**. U školskom kontekstu stoga je korisno koristiti konkretne i učenicima bliske primjere, problemske situacije, raspravu i praktične zadatke. Na taj se način učenici ne zadržavaju samo na usvajanju informacija, nego imaju priliku primijeniti naučena pravila na situacije koje se mogu pojaviti u njihovom svakodnevnom korištenju interneta.

Struktura radionice i vremenski raspored aktivnosti

Aktivnost	**Trajanje**
1. „Koliko si siguran/sigurna?“ – uvodna aktivnost	5 min
2. „Sigurno ili rizično?“ – kartice situacija	5 min
3. „Detektivi za internet“ – prepoznaj prijevaru	10 min
4. „Što bi ti napravio/la?“ – problemske situacije	10 min
5. „Moj digitalni štit“ – osobni plan sigurnosti	7 min
6. Zaključak – „5 pravila online sigurnosti“	5 min
7. Evaluacija	3 min
Ukupno	**45 min**

Potrebni materijali

- **Nastavna sredstava i pomagala:** računalo, projektor/pametna ploča, prezentacija, ploča i markeri, kartice sa situacijama i primjerima online poruka, radni list „Moj digitalni štit“, papiri/plakati i pribor za pisanje.

Sadržaj (opis aktivnosti)

Uvodni dio

a) ***„Koliko si siguran/sigurna?“***

Ishodi učenja:

- Procijeniti vlastite navike korištenja interneta i predložiti načine za njihovo poboljšanje.

Potrebni materijali:

Tijek aktivnosti: Nastavnik pročita nekoliko tvrdnji. Učenici se izjašnjavaju tako da iskorače naprijed ukoliko se tvrdnja odnosi na njega/nju.

Primjeri:

„Moja lozinka je ista na više računa.“

„Prihvaćam zahtjeve za praćenje samo od osoba koje poznajem.“

„Prije klikanja na poveznicu provjerim tko ju je poslao.“

„Ako mi prijatelj traži lozinku, mogu mu je dati.“

„Fotografiju prijatelja mogu objaviti bez njegovog dopuštenja ako je smiješna.“

Nakon svake tvrdnje nastavnik kratko pita:

„Zašto misliš da je to sigurno/nesigurno?“

Središnji dio

a) „Sigurno ili rizično?“

Ishodi učenja:

- Prepoznati potencijalno rizične situacije na internetu.
- Razlikovati sigurne i nesigurne načine dijeljenja osobnih podataka
- Objasniti važnost korištenja snažnih i različitih lozinki te dodatne autentifikacije.

Potrebni materijali: kartice sa situacijama, dva papira/plakata „SIGURNO“ i „RIZIČNO“

Tijek aktivnosti: Učenici se podijele u male skupine od 3–4 učenika.

Svaka skupina dobije kartice sa situacijama.

Primjeri kartica:

A

„Ana objavljuje fotografiju na kojoj se vidi njezina škola i lokacija na kojoj se trenutno nalazi.“

B

„Marko koristi različitu lozinku za e-mail i društvene mreže.“

C

„Luka dobije poruku: 'Čestitamo! Osvojio si mobitel. Klikni ovdje i upiši svoje podatke.'“

D

„Mia prije objave fotografije prijatelja pita prijatelja smije li je objaviti.“

E

„Ivan šalje svoju lozinku najboljem prijatelju jer mu vjeruje.“

F

„Sara dobije neugodnu poruku, napravi screenshot i pokaže ga odrasloj osobi kojoj vjeruje.“

Zadatak

Skupina treba kartice podijeliti u dvije kategorije:

☻ SIGURNO

☠ RIZIČNO

Nakon toga odabiru jednu rizičnu situaciju i odgovaraju:

„Što bi osoba trebala napraviti drugačije?“

b) „Detektivi za internet“

Ishodi učenja:

- Prepoznati potencijalno rizične situacije na internetu.
- Prepoznati pokušaje prijevare, krađe podataka i manipulacije na internetu

Potrebni materijali: računalo, PowerPoint prezentacija, projektor, papiri, olovke

Tijek aktivnosti: Učenici ostaju u skupinama. Svaka skupina dobije primjer sumnjive online poruke.

Primjer

„*HITNO!!! Vaš račun bit će ugašen danas! Potvrdite svoj račun klikom na poveznicu i unesite korisničko ime i lozinku. Imate samo 10 minuta!“*

Ispod poruke:

Zadatak detektiva:

Pronađite najmanje tri znaka upozorenja.

Učenici trebaju uočiti:

- poruka stvara osjećaj panike i hitnosti;
- traži lozinku;
- traži klikanje na poveznicu;
- ne znamo tko je stvarno poslao poruku;
- koristi prijetnju („račun će biti ugašen“).

Zatim skupine predstavljaju svoje odgovore.

Nastavnik zaključuje:

STOP – RAZMISLI – PROVJERI

STOP – ne reagiraj impulzivno.

RAZMISLI – što poruka traži od mene?

PROVJERI – tko je pošiljatelj i je li poruka vjerodostojna?

c) „Što bi ti napravio/la?“

Ishodi učenja:

- Prepoznati potencijalno rizične situacije na internetu.
- Objasniti što učiniti u slučaju uznemiravanja, prijetnji ili drugog neprimjerenog ponašanja na internetu.
- Razlikovati sigurne i nesigurne načine dijeljenja osobnih podataka.

Potrebni materijali: računalo, PowerPoint prezentacija, projektor, kanta za smeće, papirići, olovke

Tijek aktivnosti: Svaka skupina dobije jednu problemsku situaciju.

Situacija 1 – cyberbullying

„U razrednoj grupi netko objavi uvredljivu fotografiju učenika. Ostali počinju komentirati i dijeliti fotografiju.“

Pitanje: Što bi napravio/la?

Situacija 2 – nepoznata osoba

„Nepoznata osoba preko društvene mreže počinje razgovarati s učenikom i traži njegovu fotografiju i adresu.“

Pitanje: Kako reagirati?

Situacija 3 – ukradeni račun

„Netko je ušao u tvoj profil i promijenio lozinku.“

Pitanje: Koji su prvi koraci?

Situacija 4 – neugodan sadržaj

„Prijatelj ti pošalje fotografiju druge osobe i kaže: 'Nemoj nikome reći, ali pošalji još nekome.'“

Pitanje: Što napraviti?

Skupine imaju nekoliko minuta za dogovor, a zatim svaka kratko predstavlja svoje rješenje.

Nastavnik nakon odgovora daje zajednički zaključak:

Ne uzvraćaj nasiljem → sačuvaj dokaz → blokiraj/prijavi → obrati se odrasloj osobi kojoj vjeruješ.

d) „Moj digitalni štit“

Ishodi učenja:

- Procijeniti vlastite navike korištenja interneta i predložiti načine za njihovo poboljšanje.
- Objasniti važnost korištenja snažnih i različitih lozinki te dodatne autentifikacije.
- Objasniti što učiniti u slučaju uznemiravanja, prijetnji ili drugog neprimjerenog ponašanja na internetu.

Potrebni materijali: radni list „Moj digitalni štit“ (Prilog 1.)

Tijek aktivnosti: Učenici individualno dobivaju mali radni list. Nakon ispunjavanja nekoliko učenika, ako žele, mogu podijeliti svoje odgovore. Ova aktivnost omogućuje učeniku da sadržaj radionice poveže sa svojim stvarnim ponašanjem, a ne da ostane samo na usvojenim pravilima.

Završni dio

a) ***„5 pravila online sigurnosti“***

Ishodi učenja:

- Objasniti pojam online sigurnosti i navesti njezine osnovne sastavnice
- Procijeniti vlastite navike korištenja interneta i predložiti načine za njihovo poboljšanje.

Potrebni materijali: računalo, PowerPoint prezentacija

Tijek aktivnosti: Na završnom slajdu nastavnik zajedno s učenicima oblikuje pet ključnih pravila:

1. Čuvaj svoje podatke.

Ne dijeli nepotrebno adresu, lokaciju, lozinke i druge privatne informacije.

2. Zaštiti svoje račune.

Koristi snažne i različite lozinke te dodatnu autentifikaciju kada je dostupna.

3. Ne vjeruj svakoj poruci.

Provjeri poveznice, pošiljatelja i zahtjeve za osobnim podacima.

4. Razmisli prije objave.

Poštuj svoju i tuđu privatnost.

5. Ako se dogodi problem – reagiraj. Sačuvaj dokaz, prijavi sadržaj i obrati se odrasloj osobi kojoj vjeruješ.

Na samom kraju nastavnik pita:

„Koje jedno pravilo ćete od danas pokušati primjenjivati?“

Učenici mogu odgovoriti jednom riječju ili kratkom rečenicom.

b) ***Evaluacija radionice***

Ishodi učenja:

- Zaključiti o kvaliteti i korisnosti provedene radionice i novih saznanja o online sigurnosti

Potrebni materijali: računalo, PowerPoint prezentacija, projektor, pametni telefoni/ankete

Tijek aktivnosti: Razrednik podijeli link (Prilog 2.) ankete u razrednu online platformu koji učenici otvore na svojim pametnim telefonima ili u slučaju da nemaju svi pametne telefone,

podijeli isprintane ankete učenicima te ih zamoli da ju ispune i iskreno odgovore koliko su zadovoljni radionicom u kojoj su sudjelovali, je li im ista bila zanimljiva i/ili korisna i sl. Ukoliko su učenici ispunjavali isprintane ankete, nakon što su završili, razrednik pokupi sve ispunjene ankete te im i u tom slučaju, i u slučaju ispunjavanja online ankete, po završetku zahvali na sudjelovanju. Predviđeno trajanje učeničkih evaluacija je oko 3 minute.

Literatura

Hrabri telefon. (n.d.). *Cyberbullying - nasilje na internetu.* Tinejdžeri Hrabri telefon. https://tinejdzeri.hrabritelefon.hr/clanci/cyberbullying/

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283–303. https://doi.org/10.1515/commun-2014-0113

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. Journal of Communication, 67(1), 82–105. https://doi.org/10.1111/jcom.12277

National Institute of Standards and Technology. (2025, 20. kolovoza). *How do I create a good password?* https://www.nist.gov/cybersecurity-and-privacy/how-do-i-create-good-password

UNICEF Europe and Central Asia. (n. d.). *How to keep your child safe online.* https://www.unicef.org/eca/how-keep-your-child-safe-online

Prilozi

Prilog 1. Radni listić za aktivnost *Moj digitalni štit*

MOJ DIGITALNI ŠTIT

Tema: *Online sigurnost – kako se zaštititi i odgovorno ponašati na internetu*

Ime i prezime: _____

Razred: _____

Datum: _____

1. Koliko sam siguran/sigurna na internetu?

Označi tvrdnju koja te najbolje opisuje.

Tvrdnja	***DA***	***NE***	***PONEKAD***
Koristim različite lozinke za različite račune.	☐	☐	☐
Ne dijelim svoje lozinke s drugima.	☐	☐	☐
Pazim koje osobne podatke objavljujem.	☐	☐	☐
Provjerim poveznicu prije nego što kliknem na nju.	☐	☐	☐
Ne prihvaćam zahtjeve za praćenje od nepoznatih osoba.	☐	☐	☐
Razmislim prije nego što nešto objavim ili pošaljem.	☐	☐	☐
Znam kome se mogu obratiti ako doživim problem na internetu.	☐	☐	☐

2. Moj digitalni štit

Jednu stvar koju već dobro radim na internetu:

_____

_____

Jednu stvar na koju trebam više paziti:

_____

_____

3. Što ću promijeniti?

Od danas ću pokušati:

☐ *bolje čuvati svoje osobne podatke*

☐ *koristiti sigurnije/različite lozinke*

☐ *uključiti dodatnu autentifikaciju gdje je dostupna*

☐ *pažljivije provjeravati poruke i poveznice*

☐ *više paziti što objavljujem i dijelim*

☐ *odgovornije reagirati na online nasilje*

☐ *nešto drugo:* _____

4. Ako se dogodi problem...

Ako me netko uznemirava, prijeti mi, pokušava prevariti ili objavljuje moj sadržaj bez dopuštenja, mogu se obratiti (npr. osoba od povjerenja, osoba u školi,...):

1. _____

2. _____

3. _____

Zapamti

STANI – RAZMISLI – PROVJERI – ZAŠTITI SE – POTRAŽI POMOĆ

Nije sramota tražiti pomoć ako se na internetu dogodi nešto neugodno, zastrašujuće ili nesigurno.

Prilog 2. Poveznica za online evaluacijsku anketu o radionici (*google forms link*)