



Arnela Šabanović

05.09.2026. 22:23

Viewed: 4 times

Sigurnost i zaštita na internetu

Čas obuhvata uvodni "QR izazov" o oprezu pri unosu ličnih podataka, razgovor o pojmu sigurnosti na internetu, rad u parovima na povezivanju cyber pojmova (phishing, scam, spam, doxxing, deepfake i dr.), grupnu analizu digitalnih situacija.

Organizacijski oblik nastave

Predmetna nastava 8. razred

Vrsta nastavnog procesa

Osnovna vrsta nastave - Redovna nastava

Suradnja škole sa roditeljima i zajednicom te razvoj školskog kolektiva

Aktivnosti sa učenicima

Trajanje

45 minuta

Oblasti

Digitalni svijet/Područje tehnike i informacionih tehnologija

Predmet

Informatika

Ključne kompetencije

Digitalna kompetencija

Ciljevi i ishodi učenja i poučavanja

Cilj: Upoznati učenike s osnovnim pravilima sigurnog korištenja interneta te razvijati odgovorno ponašanje, kritičko mišljenje i svijest o zaštiti ličnih podataka u digitalnom okruženju.

Ishodi učenja i poučavanja

Učenik/učenica:

- objašnjava pojam sigurnosti na internetu i osnovne prijetnje
- prepoznaje rizične situacije u online okruženju
- razlikuje sigurno i nesigurno ponašanje na internetu
- primjenjuje osnovna pravila zaštite ličnih podataka te
- razvija odgovoran i kritički odnos prema online sadržajima i komunikaciji

Detaljan opis realizacije

Aktivnost 1 – QR izazov

QR izazov: Čas započinje prikazom QR koda na pametnoj tabli. Nastavnik učenicima daje kratku uputu da u narednih 30 sekundi skeniraju kod i urade ono što se traži. QR kod vodi na pripremljenu simuliranu stranicu koja oponaša obrazac za unos ličnih podataka (ime i prezime, adresa, broj telefona ili e-mail), bez stvarnog prikupljanja ili pohranjivanja podataka. Nakon kratkog vremena nastavnik prekida aktivnost i postavlja pitanja: Ko je pokušao skenirati kod? Da li ste provjerili gdje vas link vodi? Da li biste unijeli svoje podatke? Učenici iznose svoja mišljenja i obrazlažu postupke. Nastavnik usmjerava razgovor prema zaključku da je u digitalnom okruženju važno biti oprezan, provjeriti sadržaj prije reagovanja i zaštititi lične podatke. Aktivnost služi kao uvod u temu sigurnosti na internetu i razvijanje kritičkog razmišljanja.

Aktivnost 2 – Šta predstavlja sigurnost na internetu?

Šta predstavlja sigurnost na internetu?: Nastavnik povezuje prethodnu aktivnost s novom temom kroz pitanja: Šta za vas znači sigurnost na internetu? Jeste li se susreli sa sumnjivim porukama ili linkovima? Učenici iznose iskustva i navode primjere iz svakodnevnog korištenja interneta, poput nepoznatih poruka, lažnih nagrada ili zahtjeva za ličnim podacima. Nastavnik njihove odgovore usmjerava i uvodi pojam sigurnosti na internetu kao zaštite ličnih podataka, uređaja i digitalnog identiteta.

Aktivnost 3 – Razumijevanje pojmova i prepoznavanje prijetnji

Razumijevanje pojmova i prepoznavanje prijetnji: Nastavnik na pametnoj tabli prikazuje ključne

pojmove iz oblasti sigurnosti na internetu: lozinka, digitalni otisak, phishing, scam, spam, cyber nasilje, doxxing i deepfake sadržaj. Učenici rade u parovima i dobijaju radni list na kojem trebaju povezati pojmove sa odgovarajućim objašnjenjima ili primjerima situacija. Tokom rada nastavnik ih usmjerava pitanjima: Na osnovu čega ste zaključili? Gdje ste se mogli susresti s ovakvom situacijom? Nakon provjere učenici zajedno s nastavnikom pojašnjavaju pojmove i zaključuju da njihovo razumijevanje doprinosi sigurnijem korištenju interneta.

Aktivnost 4 – "Digitalni detektivi"

„Digitalni detektivi”: Učenici rade u grupama od 3–4 člana i dobijaju zadatak da analiziraju određenu digitalnu situaciju. Svaka grupa dobija kartice ili materijale koji prikazuju primjer nesigurnog ponašanja na internetu (sumnjiva poruka, e-mail, lažni profil, zahtjev za unos podataka ili sumnjivi link). Učenici analiziraju slučaj i odgovaraju na pitanja: Koji znakovi ukazuju na opasnost? Koji rizik postoji? Koji cyber pojam povezujemo s ovom situacijom? Kako pravilno postupiti? Nakon rada grupe predstavljaju zaključke, a ostali učenici dopunjuju odgovore i učestvuju u diskusiji. Nastavnik usmjerava učenike ka pravilima sigurnog ponašanja na internetu.

Aktivnost 5 – Završna refleksija

Završna refleksija: Na kraju časa nastavnik vodi kratku diskusiju kroz pitanja: Šta ste danas naučili o sigurnosti na internetu? Koja situacija vam je bila najznačajnija? Kako ćete ubuduće prepoznati sumnjive sadržaje? Učenici iznose zaključke i navode promjene koje mogu primijeniti u svom digitalnom ponašanju. Nastavnik povezuje odgovore i naglašava da sigurno korištenje interneta zahtijeva znanje, oprez i odgovornost. Na kraju učenicima se može podijeliti edukativni letak kao podsjetnik na ključna pravila sigurnosti.

Potrebni resursi

- Računar i projektor/pametna tabla sa pristupom internetu
- QR kod sa linkom na simuliranu stranicu za unos podataka
- Simulirana stranica (npr. Google Forms)
- Tableti ili mobiteli za učenike
- Prezentacija sa ključnim pojmovima i primjerima situacija
- Radni listovi za povezivanje cyber pojmova i značenja
- Kartice za aktivnost „Digitalni detektivi”
- Tabla i markeri
- Edukativni letak o sigurnosti na internetu

Praćenje i procjenjivanje

Praćenje se vrši kroz rad na radnim listovima (povezivanje pojmova) i analizu slučajeva u aktivnosti "Digitalni detektivi", te kroz završnu refleksiju na kraju časa.

Ideje za domaće zadaće (nastavak aktivnosti) i uključivanje roditelja

/

Savjeti za druge nastavnike/ce kod realizacije ove lekcije/teme

/

Metode i tehnike

Metoda razgovora

Collections

Mirovna pedagogija: kompendijum priprema za čas

Lesson plan - Elementary school