



KAKO RAZGOVARATI S UČENICIMA O CYBERSIGURNOSTI?

**PRAKTIČNI SAVJETI ZA NASTAVNIKE
OSNOVNIH I SREDNJIH ŠKOLA**



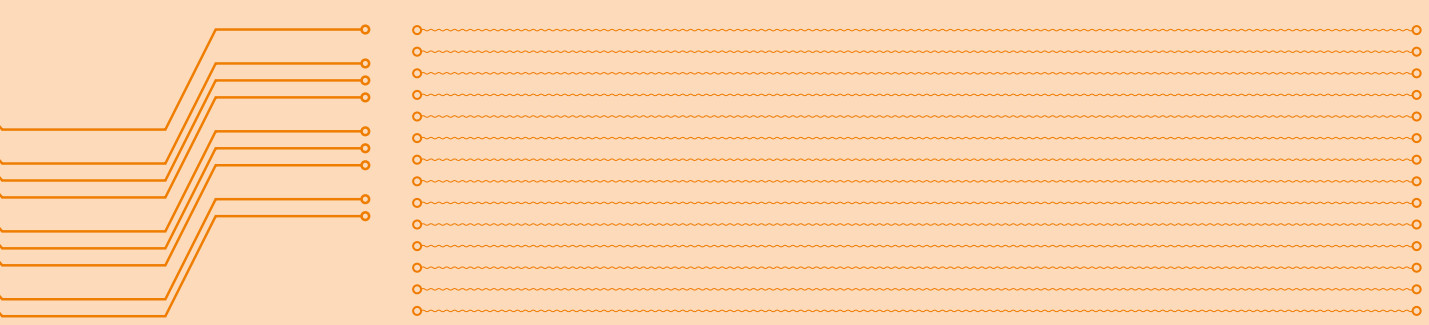
Udruženje

e-Transformacija

Sarajevo, 2025.

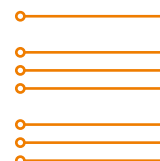
Sadržaj

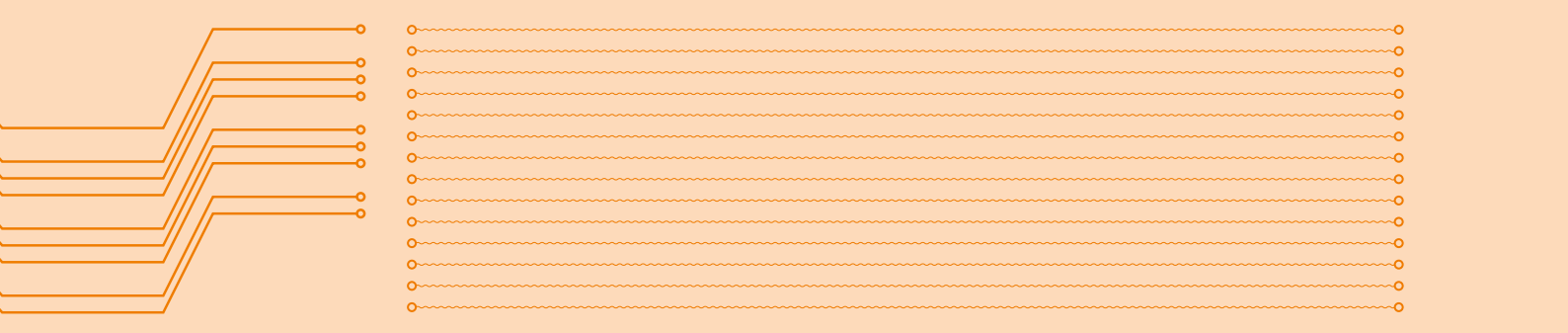
Predgovor	3
1. Zašto razgovarati o cyber sigurnosti?	4
2. Šta učenici (ne)znaju?	6
3. Kako razgovarati prema uzrastu?	8
4. Uloga nastavnika	10
5. Šta ako?	11
6. Preporučeni alati i izvori	13



Predgovor

Ova publikacija je prvenstveno namijenjena nastavnicima osnovnih i srednjih škola, ali i stručnim saradnicima, pedagogima, psiholozima i svim edukatorima koji učenicima žele približiti teme iz oblasti cyber sigurnosti na primjeren, razumljiv i podsticajan način. U digitalnom dobu u kojem učenici od najranijeg uzrasta svakodnevno koriste internet, društvene mreže i različite digitalne alate, zadatak obrazovnog sistema jeste da ih tehnički opismeni, ali i da ih nauči kako da se ponašaju odgovorno, sigurno i etički u online okruženju. Cyber sigurnost nije tema koja pripada isključivo stručnjacima za informatiku ili IT sektoru, ona je međupredmetna, razvojno važna i duboko povezana sa svakodnevicom učenika koja podrazumijeva njihovu komunikaciju, identitet, emocionalno stanje i odnose s vršnjacima. Cilj ove publikacije je da podrži nastavnike u njihovoj ulozi vaspitača i vodiča u digitalnom prostoru. Kroz konkretne savjete, pitanja, metode i alate, nastavnici će moći lakše otvoriti dijalog s učenicima, razumjeti njihove potrebe i izazove, te razvijati njihovu digitalnu pismenost, kritičko mišljenje i osjećaj odgovornosti. Poseban fokus stavljen je na stvaranje sigurnog i povjerljivog okruženja u učionici, gdje učenici mogu slobodno iznositi svoja iskustva, postavljati pitanja i učiti jedni od drugih. Publikacija ne nudi gotove recepte, već fleksibilne pristupe koji nastavnicima omogućavaju da ovu temu prilagode svom stilu rada, uzrastu učenika i specifičnom kontekstu škole.





1. Zašto razgovarati o cyber sigurnost?

U današnjem digitalnom društvu, djeca i mladi sve ranije ulaze u online svijet, odnosno koriste mobilne telefone, tablete i računare za komunikaciju, igru, zabavu i učenje. Iako se često pretpostavlja da „digitalna generacija“ instinktivno zna koristiti tehnologiju, to ne znači da zna i kako da se zaštiti u digitalnom prostoru. Zbog toga, razgovor o cyber sigurnosti ne bi trebao biti dodatni zadatak u obrazovanju, već neophodan dio razvoja svakog učenika u 21. stoljeću.

U nastavku ću navesti i detaljnije obrazložiti 4 ključna razloga zbog kojih trebamo razgovarati o cyber sigurnosti:

1. Djeca sve ranije koriste internet

Djeca danas prvi pametni telefon dobijaju već u uzrastu od 7 do 10 godina, a mnogi već u prvom razredu osnovne škole koriste YouTube, aplikacije za dopisivanje, igrice i društvene mreže. Oni u digitalni svijet ulaze brzo i intenzivno, ali bez razvijenih mehanizama zaštite i bez jasne svijesti o mogućim rizicima. Bez razgovora i podrške odraslih, njihovo snalaženje u tom prostoru ostaje površno i često rizično jer dok znaju „kliknuti“, ne znaju uvijek zašto ne bi trebali kliknuti baš tu.

2. Online prijetnje nisu uvijek očigledne

Digitalne prijetnje danas nisu samo hakeri i virusi. Mnogo su suptilnije i često zamaskirane kao obične poruke, simpatični linkovi, izazovi na društvenim mrežama ili pozivi na „zabavne“ aplikacije.

Djeca i mladi nisu uvijek u stanju da prepoznaju:

- Phishing poruke (prevare koje izgledaju kao poruke prijatelja ili servisa poput „*vaš račun je blokiran*“),
- Lažne profile,
- Pozive na dijeljenje intimnih podataka ili fotografija,
- Govore mržnje i uvrede maskirane kao šale.

Zato je važno da učenici razviju vještine prepoznavanja opasnosti kroz diskusije, analize, realne primjere i razmjenu iskustava.

3. Prevencija je bolja od intervencije

Kao i u drugim oblicima nasilja, reakcija dolazi prekasno ako učenik već postane žrtva. Mnoga djeca i tinejdžeri se ne usude prijaviti digitalno nasilje jer se boje osude, kazne, ismijavanja ili ne vjeruju da će ih neko ozbiljno shvatiti.

Rano uvođenje razgovora o cyber sigurnosti može pomoći da učenici:

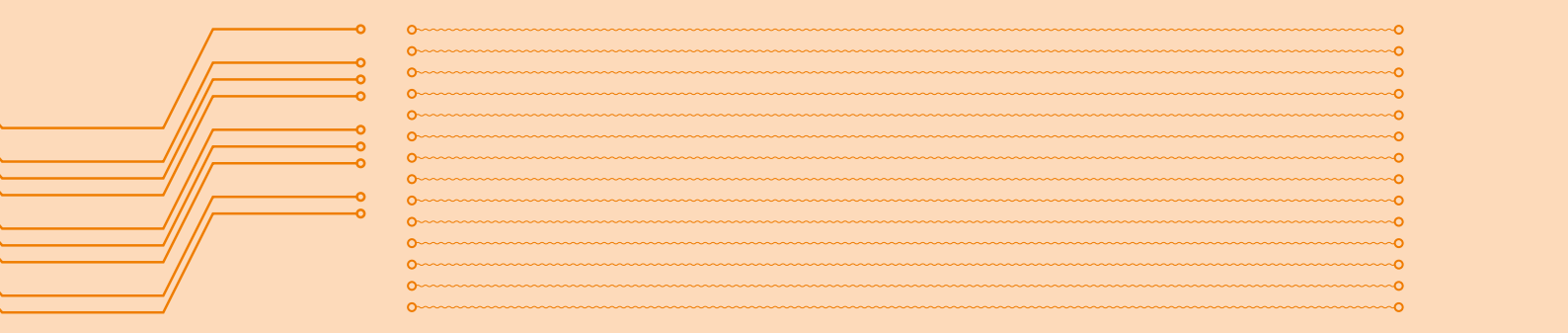
- znaju kome se i na koji način mogu obratiti
- ne osjećaju krivicu ako postanu žrtve prevare ili nasilja,
- razviju otpornost i samopouzdanje da se nose s digitalnim izazovima.
- Edukacija o digitalnoj sigurnosti je oblik psihološke i emocionalne zaštite.

4. Nastavnici su često prva linija zaštite

Iako se čini da roditelji imaju najveći uticaj, nastavnici su ti koji svakodnevno komuniciraju s učenicima, posmatraju njihovo ponašanje i mogu prvi primijetiti znakove problema poput povlačenja, promjene u komunikaciji, pada koncentracije, napetosti u razredu.

Zato su nastavnici ključni akteri u prepoznavanju i prevenciji problema vezanih za cyber nasilje, zloupotrebu interneta i digitalni stres. Njihova uloga nije da zamijene stručnjake, već da prepoznaju, osnaže i upute učenike prema rješenju. Prema tome, otvoren razgovor u učionici može biti prva i najvažnija tačka kontakta između učenika i svijeta sigurnog interneta.





2. Šta učenici (ne)znaju?

Jedna od ključnih prepreka u edukaciji o cyber sigurnosti je pogrešna pretpostavka da učenici sve znaju jer „odrastaju s tehnologijom“, „stalno su na telefonima“ i „znaju više od nas“. Iako učenici uistinu vješto koriste digitalne alate, aplikacije i društvene mreže, to ne znači da razumiju rizike, niti da su razvili sposobnost kritičkog mišljenja i samoodbrane u digitalnom prostoru. U stvarnosti, mnogi učenici:

Poznaju alate, ali ne razumiju posljedice

Znaju kreirati korisnički račun za potrebe društvenih mreža, koristiti filtere, objaviti slike ili igrati online igrice, ali ne znaju šta znači phishing, kako prepoznati prevaru, ili kako da se zaštite od krađe identiteta. Dakle, sama upotreba servisa i alata ne znači direktno i svijest o sigurnosti.

Smatraju da su „previše (digitalno) pametni da im se nešto desi“

Zbog digitalne samouvjerenosti ili uvjerenja da su „sve već čuli“, mnogi učenici odbacuju savjete odraslih. Ova iluzija nepovrjedivosti može ih učiniti lahkom metom za manipulaciju, ucjene i druge oblike digitalnog nasilja. „Meni se to ne može desiti“ možda jeste znak da se već nešto dešava.

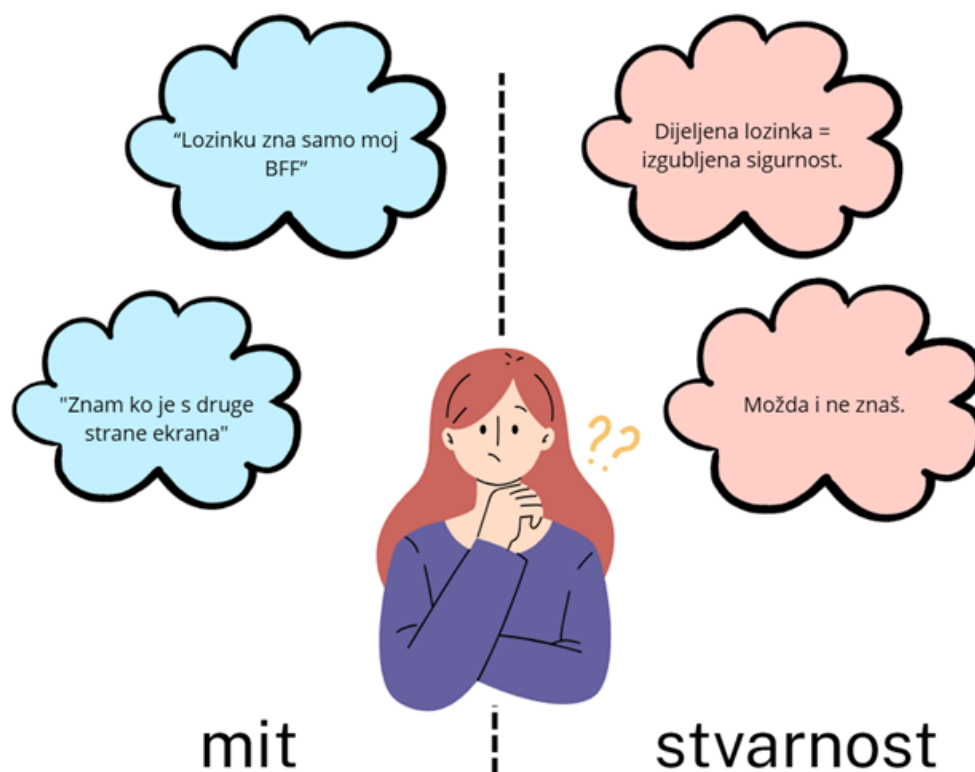
Ne razlikuju šalu, trolanje i nasilje

Mnogi tinejdžeri ne prepoznaju granicu između duhovite provokacije i ozbiljnog uznemiravanja. Komentari koji vrijeđaju, ponižavaju ili ismijavaju često se opravdavaju riječima „samo sam se šalio“, dok žrtva ostaje bez podrške. Nedostatak empatije i razumijevanja mogućih posljedica dodatno otežava reagovanje.

Ne razumiju vrijednost svojih podataka

Učenici često olahko daju svoje ime, prezime, broj telefona, adresu e-pošte ili lokaciju prilikom registracije na igre, aplikacije ili društvene mreže, a da pritom ne razumiju ko sve može doći do tih podataka i na koji način ih može zloupotrijebiti. Lične informacije su „digitalna valuta“¹ jer one mogu biti iskorištene za profilisanje, ciljani marketing, pa i prevare.

¹ Fraza „digitalna valuta“ je standardni izraz u obrazovnim i stručnim materijalima kad se govori o podacima, jer se njima „plaća“ pristup aplikacijama, igrama i sadržajima i to često nesvjesno.

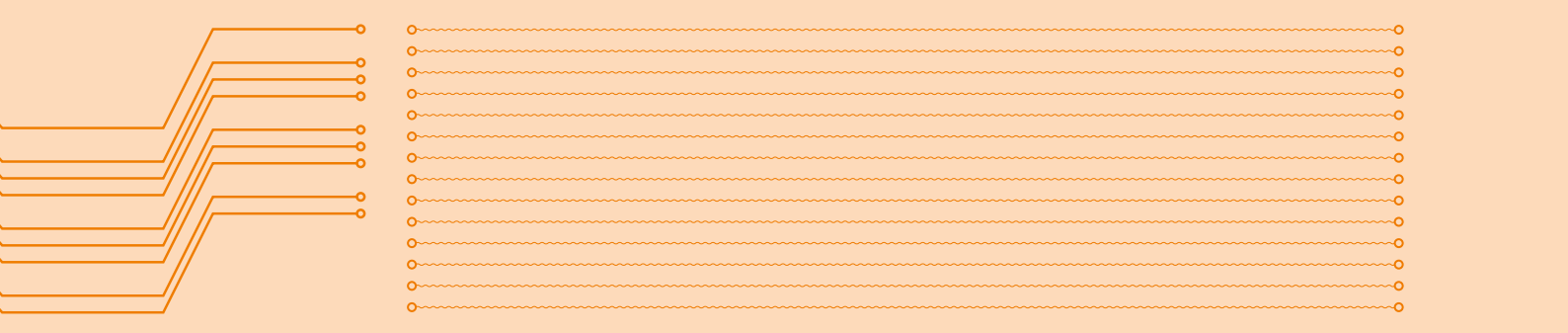


Podcjenjuju dugoročnost digitalnog sadržaja

Učenici često djeluju impulsivno i ne razmišljaju o digitalnom otisku kao trajnom zapisu njihovih aktivnosti na internetu. Vjeruju da se objava može obrisati, da „*story traje samo 24 sata*“, da screenshot neće niko napraviti, itd. U stvarnosti, sve što se jednom objavi, može se ponovo pojaviti i imati posljedice na reputaciju, odnose, pa čak i buduće zapošljavanje ili upis na fakultet.

Nisu naučeni kako da reaguju kad se nešto desi

Iako neki učenici i prepoznaju opasnu situaciju, ne znaju šta konkretno da urade: kome da prijave, kako da naprave screenshot kao dokaz, kako da blokiraju kontakt, kako da zaštite račun, gdje mogu dobiti podršku.



3. Razgovor prema uzrastu

Učenje o cyber sigurnosti nije „jedna veličina za sve“ jer pristupi koji motivišu mlađe učenike ne funkcionišu nužno sa starijima, i obrnuto. Kako bi poruke bile djelotvorne, potrebno je prilagoditi sadržaj, ton i metode razgovora uzrastu i stepenu digitalne zrelosti učenika. Ovdje su date smjernice za rad s dvije osnovne skupine: mlađim tinejdžerima (12–15) i starijim adolescentima (15–18) godina.

Učenici od 12 do 15 godina

U ovom uzrastu djeca počinju samostalnije koristiti internet, ali još uvijek nemaju razvijeno kritičko mišljenje o rizicima. Njihov digitalni život se često odvija na platformama koje naglašavaju zabavu, kreativnost i brzu komunikaciju. Imaju svoje profile, igraju online igre, prate omiljene YouTube kanale i TikTok trendove. Ipak, i dalje često ne vide sve opasnosti koje vrebaju. Zato je važno da im priđete sa razumijevanjem, bez da ih odmah zasipate „opasnostima“ i pravilima.

U nastavku se nalazi nekoliko savjeta i prijedloga razgovora:

Koristite jednostavan, prijateljski ton. Izbjegavajte stručne riječi ili preduga objašnjenja. Bolje je kratko i jasno, kako bi učenici brzo shvatili poruke.

Povežite teme s onim što oni svakodnevno rade online. Pitajte ih o aplikacijama i platformama koje koriste, ali bez osuđivanja! Tako ćete lakše ući u razgovor i time postepeno uvoditi priču o sigurnosti.

Postavljajte pitanja koja učenike potiču na razmišljanje, kao što su:

- „Šta bi ti uradio/la kad bi dobio/la poruku od nekog koga ne poznaješ?“
- „Kako možeš prepoznati da je nešto prevara?“
- „Zašto misliš da nije pametno dijeliti lozinku?“

Vrlo je važno da ih stvarno slušate i prihvatite njihove stavove i dileme. Djeca moraju osjetiti da ih razumijete i da ih ne osuđujete.

Ponavljajte im da je traženje pomoći od odraslih znak mudrosti, a ne slabosti. Ohrabrite ih da se obrate nekom kome vjeruju ako im je nešto nejasno ili ih nešto plaši.

Koristite praktične primjere i priče. Čak i male anegdote iz stvarnog života mogu im puno pomoći da shvate zašto su određene stvari opasne.

I ne zaboravite – sigurnost nije tema koju je dovoljno jednom spomenuti, to je ustvari proces. Zato budite dosljedni i često ponavljajte najvažnije poruke.

Učenici od 15 do 18 godina

Stariji srednjoškolci imaju veće digitalno iskustvo, ali često i više rizika, jer se upuštaju u kompleksnije online interakcije – od komentarisanja, stvaranja sadržaja i vođenja vlastitih profila do sudjelovanja u diskusijama, forumima i online vezama.

Za njih je ključno da se osjećaju uključeno i shvaćeno, da im se prizna važnost njihovog mišljenja i da imaju priliku sudjelovati u donošenju pravila koja ih se tiču. Kada im damo prostor da iznesu svoje stavove i da zajednički oblikujemo pravila ponašanja na internetu, osnažujemo ih da budu odgovorni korisnici digitalnog svijeta.

Praktični savjeti za nastavnike:

Počnite razgovor otvorenim pitanjima koja potiču kritičko razmišljanje, poput:

- „Šta mislite o granicama privatnosti na internetu?”
- „Kako procijeniti šta je prikladno za objavu, a šta nije?”

Koristite stvarne primjere i situacije koje su im bliske ili su već možda i doživjeli, kao što su lažni profili, online konflikti, ili manipulacije na društvenim mrežama.

Potaknite učenike da kreiraju vlastiti “kodeks ponašanja” u digitalnom prostoru. Neka definišu pravila koja bi svi trebali poštovati i razmotre posljedice neodgovornog ponašanja.

Razgovarajte o emocionalnim aspektima online iskustava – kako se učenici nose s cyber nasiljem, pritiskom vršnjaka ili stresom izazvanim internetom.

Istaknite važnost samopomoći i podrške. Podsjetite ih da nije slabost tražiti pomoć, bilo od nastavnika, školskog pedagoga, roditelja ili stručnjaka, te im ponudite informacije gdje mogu potražiti podršku.

Budite sagovornici u razgovoru, a ne sudije. Otvoren dijalog i međusobno poštovanje grade povjerenje i motivišu učenike na odgovorno ponašanje.

4. Uloga nastavnika

Učionica u kojoj se razgovara o cyber sigurnosti ne treba da izgleda kao predavanje iz informatike ili kao popis zabrana koje učenici treba da nauče napamet. Naprotiv, to treba da bude prostor u kojem se učenici osjećaju slobodno da postave pitanja, podijele sumnje i prepoznaju stvarne izazove digitalnog svijeta u kojem svakodnevno žive. U tom prostoru, nastavnik ne mora imati sve odgovore, ali ima ključnu ulogu: da bude vodič, oslonac i pokretač razmišljanja.



Nastavnik nije firewall (zaštitni zid),
ali može biti vodič.

Bez obzira da li predajete matematiku, književnost, biologiju ili likovno, svi imate priliku, i odgovornost, da kod učenika razvijate svijest o sigurnom i odgovornom ponašanju na internetu. Prema tome:

Budite facilitatori, ne kontrolori

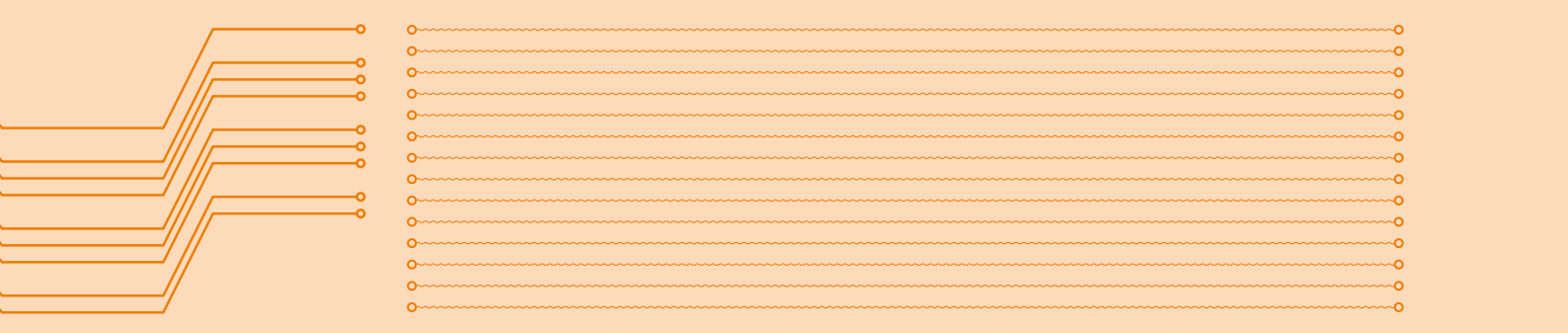
Vaša uloga ne bi trebala biti kontrola svakog digitalnog koraka učenika, već pomoć da razumiju posljedice svojih odluka. Umjesto da ih zastrašujemo, možemo ih osnažiti da donose bolje izbore kroz razgovor, primjere i povjerenje.

Ohrabrujte pitanja, i pri tome ne ismijavajte neznanje

Učenici se neće otvoriti ako osjećaju da će zbog svog neznanja biti ismijani ili ignorisani. Kada postave pitanje poput: „Šta ako mi neko prijete na mreži?“ ili „Da li je sigurno kliknuti na link u poruci?“ to je trenutak koji vrijedi više od cijelog školskog časa. Način na koji reagujemo može odlučiti hoće li nam se ikada više obratiti.

Priznajte kad nešto ne znate

Nije slabost reći „Nisam siguran/na, hajde da to zajedno istražimo“. Time šaljemo poruku da i odrasli uče, da nije sramota pitati i da sigurnost nije nešto što se uči jednom zauvijek, već stalno.



5. Šta ako...?

Nastavnici se u razgovorima o cyber sigurnosti često nađu u situacijama koje nisu uvijek predvidive niti jednostavne. Takvi razgovori mogu otvoriti teme koje su emocionalno teške, lične ili neugodne za učenike. Nisu svi spremni da slušaju, a još manje da se otvore. Ipak, način na koji nastavnik reaguje u tim trenucima presudan je za izgradnju povjerenja i sigurnog okruženja. Ova sekcija nudi smjernice kako reagovati u realnim i ponekad osjetljivim situacijama u učionici.

Šta ako učenik kaže: „To se meni ne može desiti“?

Učenici ponekad koriste ovu izjavu da sakriju osjećaj nesigurnosti, ranjivosti ili čak prethodno negativno iskustvo koje ne žele priznati pred drugima. Umjesto da osporite njihov stav, pokušajte postaviti pitanja koja ih vode ka razmišljanju:

- „Dobro, ali šta bi uradio da se desi nekom iz tvog razreda?“
- „Da li znaš nekoga kome se nešto slično desilo?“

Savjet nastavniku: Nekim učenicima je lakše govoriti „kao da se to dešava nekom drugom“. To je način da se zaštite, a istovremeno podijele stav ili iskustvo koje ih tišti. Umjesto da ih navodite da priznaju vlastitu ranjivost, dozvolite im da pričaju o „drugima“, i pažljivo slušajte između redova.

Šta ako učenik podijeli nešto uznemirujuće pred razredom?

Kada učenik podijeli lično ili osjetljivo iskustvo, to je pokazatelj da se osjeća dovoljno sigurno da se otvori, ali i da mu je možda hitno potrebna podrška. Takve izjave često dolaze nenajavljeno i mogu iznenaditi sve prisutne. U takvim situacijama zahvalite se na iskrenosti i priznanju i recite smireno: *„Hvala ti što si to podijelio/la. Znam da to nije lahko reći pred svima. Možemo o tome razgovarati i nasamo, ako želiš. Važno je da znaš da nisi sam/a.“*

Savjet nastavniku: Izbjegavajte dramatizaciju pred razredom. Održite sigurno ozračje za sve učenike, ali i odvojeno posvetite pažnju učeniku koji je nešto podijelio u saradnji s pedagogom ili drugim stručnim saradnicima, ako je potrebno.

Šta ako se drugi učenici počnu smijati ili omalovažavati pitanje?

U učionici se često desi da reakcija grupe prikrije nesnalaženje, nelagodu ili strah. Smijeh može biti način da učenici odagnaju neprijatnost, ali i mehanizam distanciranja od problema.

Ipak, takve reakcije mogu obeshrabiliti one koji bi željeli da podijele svoje iskustvo. Reagujte tako što ćete zaustaviti reakciju mirnim, ali odlučnim tonom: „**Svako pitanje je važno. Ako se nečemu smijemo, to ne znači da je manje ozbiljno. Hajde da budemo podrška jer ovo se može desiti bilo kome.**“

Savjet nastavniku: Ne dozvolite da se učenici ismijavaju ili omalovažavaju jedni druge, ni u šali. To ne znači da ih morate odmah kazniti, već da jasno postavite granicu. Po potrebi, u narednim časovima podsjetite razred na pravila međusobnog poštovanja.

Šta ako ne znate tačan odgovor na neko pitanje?

Učenici sve češće postavljaju pitanja koja se odnose na konkretne situacije iz digitalnog života poput hakiranja računara, lažnih poruka, deepfake sadržaja, online prevara... I nije uvijek moguće imati spreman i tačan odgovor. Ali važno je kako na to reagujemo. Uvijek možete reći:

„Hajde da to zajedno istražimo. Važno je znati gdje i kako tražiti tačne informacije.“

Savjet nastavniku: U ovoj situaciji učite primjerom. Pokažite učenicima da je u redu ne znati sve, ali da je kritičko provjeravanje izvora i zajedničko istraživanje znak odgovornog digitalnog ponašanja.

Šta ako učenik negira sve rizike i ne želi učestvovati?

Otpor učenika da razgovaraju o cyber sigurnosti može biti znak nezainteresovanosti, ali i samoodbrane jer ne žele priznati da su nešto doživjeli, uradili ili ne razumiju. Kako reagovati:

„Razumijem da ti to možda ne izgleda važno sada. Ali dovoljno je da slušaš i vidiš prepoznaješ li nešto što može biti korisno. Ne moraš učestvovati, ali možeš razmisлити.“

Savjet nastavniku: Ne forsirajte dijalog s otporom. Uključite učenika indirektno kroz analizu slučaja, grupni rad ili primjer iz medija.

Svaka od ovih situacija je prilika da gradite povjerenje i stvarate učionicu u kojoj se učenici osjećaju sigurno, poštovano i spremno da uče jedni od drugih. Nastavnik u ovim razgovorima ne mora biti ekspert za IT, ali mora biti prisutan, empatičan i spreman da podrži.

6. Rječnik cyber pojmova

Razumijevanje osnovnih pojmova iz oblasti cyber sigurnosti pomaže nastavnicima da lakše komuniciraju s učenicima i odgovore na njihova pitanja. Ne gledajte na ovo kao na tehnički rječnik, već kao na alat za osnaživanje u svakodnevnom razgovoru.

Pojam	Objašnjenje
Cyber sigurnost	<i>Zaštita računara, interneta i digitalnih podataka od opasnosti kao što su hakeri, virusi i krađa, kako bi naši podaci i uređaji bili sigurni</i>
Lozinka	<i>Tajni niz znakova koji štiti pristup računu</i>
Digitalni otisak	<i>Sve što osoba objavi, pregleda ili klikne online, ostaje kao trag</i>
Cyber nasilje	<i>Namjerno uznemiravanje putem interneta (vrijeđanje, prijetnje, ismijavanje)</i>
Doxxing	<i>Objavljivanje tuđih ličnih podataka na internetu bez dozvole</i>
Spam	<i>Neželjene poruke, često promotivne ili sa sumnjivim linkovima</i>
Phishing	<i>Prevara putem e-maila ili poruke kojom se pokušava ukrasti lozinka ili podaci</i>
Scam	<i>Lažne ponude, nagradne igre, poruke ili pozivi kojima se pokušava prevariti osoba da da novac ili lične podatke</i>
Deepfake sadržaj	<i>Lažni ili manipulisani video, audio ili slika, kreiran pomoću vještačke inteligencije (AI), koji izgleda vrlo uvjerljivo i realistično, ali prikazuje nešto što se u stvarnosti nije dogodilo</i>

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.