

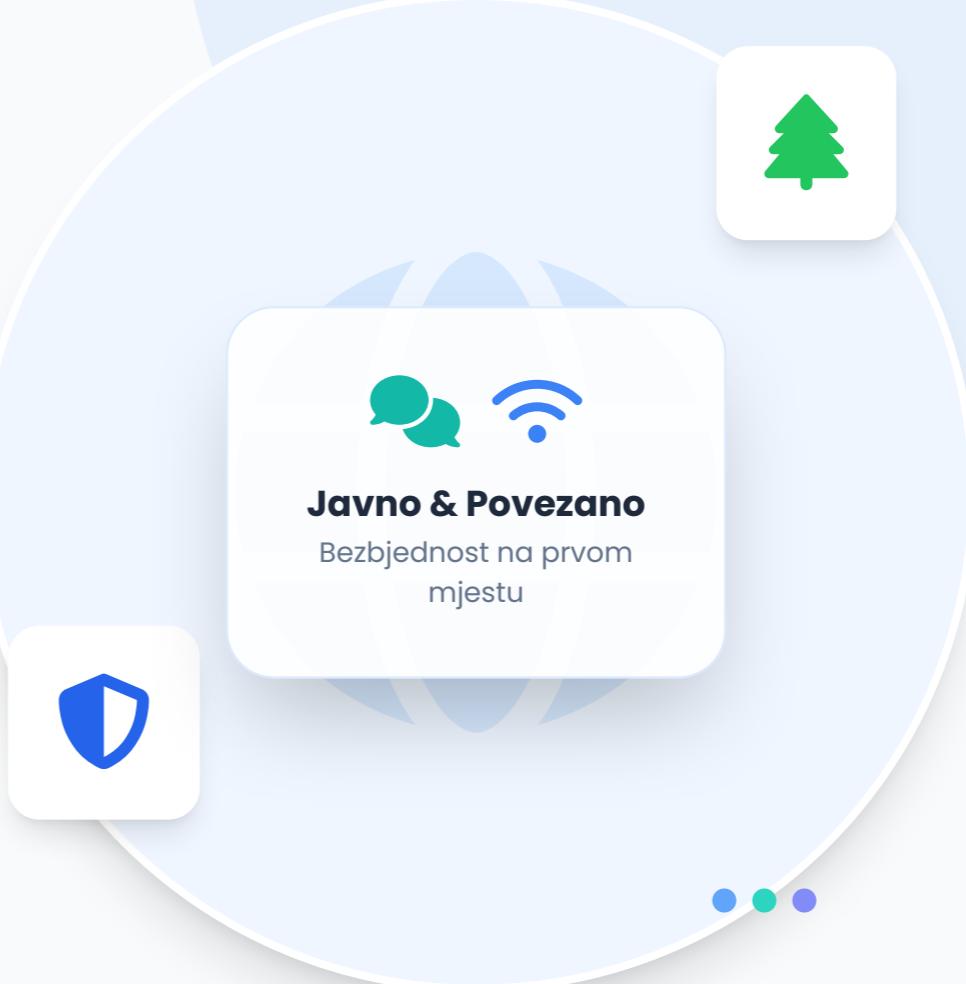
Internet kao Javni Prostor

Razumijevanje digitalnog svijeta kroz analogiju parka

Cilj radionice: Naučiti kako se ponašati odgovorno, prepoznati rizike i ostati bezbjedno u digitalnom okruženju.

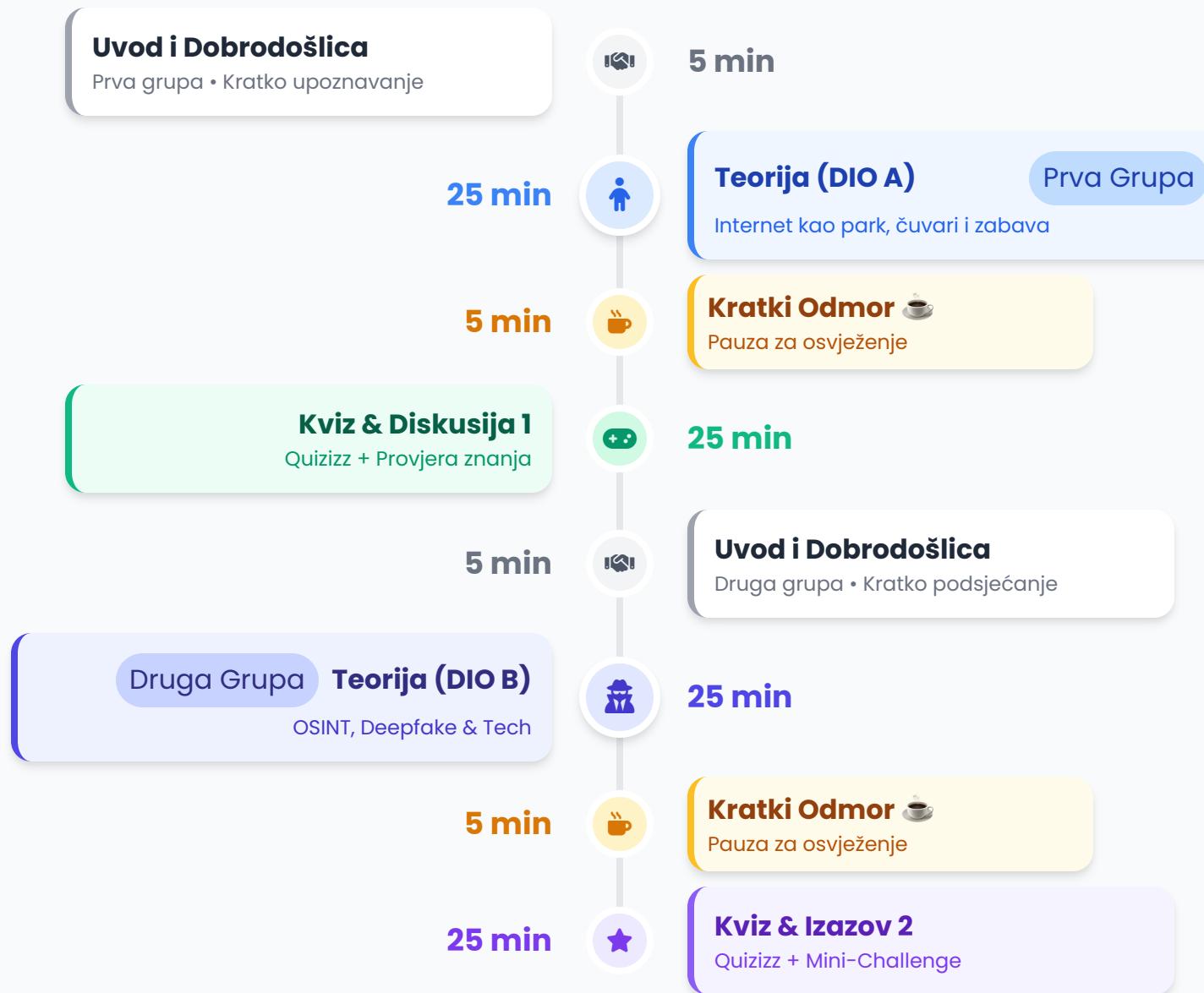
👤 Dio A: Mlađa grupa

👤 Dio B: Starija grupa



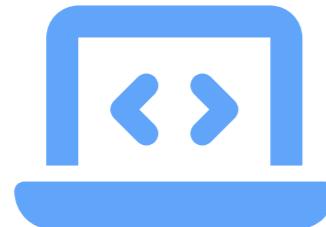
Agenda dana

Plan radionice digitalne bezbjednosti (120 minuta)



Dobrodošli! 🙌

Danas učimo kako biti pametni digitalni istraživači.



Poštujemo jedni druge

Svi smo ovdje da naučimo nešto novo. Slušamo kada neko drugi govori.

Nema ismijavanja

Ovo je siguran prostor. Grijesiti je dio učenja!

Pitamo kad nije jasno

Nema glupih pitanja. Ako te nešto zbuni, podigni ruku.

Spremni? Idemo u avanturu! 🚀

Šta nas čeka danas?

Plan naše avanture kroz digitalni svijet



Internet kao Park

Razumjećemo kako internet liči na veliki javni park gdje se svi igraju, ali i paze.



Javno vs Privatno

Naučićemo šta smijemo dijeliti sa svima, a šta čuvamo samo za sebe i porodicu.



Ko nas vidi?

Otkrićemo ko sve može vidjeti naše slike i poruke čak i kad mislimo da su tajne.



Kviz & Zabava

Provjerićešmo znanje kroz zabavni Quizizz kviz i mini-izazove za sve!



Budite spremni/spremne da pitate i učestvujete!

MOTIVACIJA

Zašto učimo o bezbjednosti?

Internet nije odvojen svijet. To je mjesto gdje živiš, učiš i zabavljajaš se.



Dio svakodnevica

Kao što znaš pravila ponašanja u školi ili na ulici, tako su ti potrebna i ovdje. Internet je tvoj digitalni dom.



Male odluke, velika moć

Jedna jaka lozinka ili jedan klik na "Ne" mogu spriječiti velike probleme. Ti imaš kontrolu u svojim rukama.



Hrabrost i zaštita

Kada znaš kako da prepoznaš opasnost, ne moraš da se plašiš. Znanje ti daje samopouzdanje da istražuješ bezbjedno.



Znanje = Tvoja Supermoć

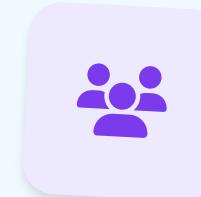
DIO A:

Internet kao Javni Prostor

Razumijevanje digitalnog svijeta kroz jednostavne priče,
analogije i primjere iz svakodnevnog života.



Park



Ljudi



Zaštita

Internet je kao Javni Park



Svako može uči

Baš kao u parku, na internetu srećemo prijatelje, ali i potpune strance.



Svi te mogu vidjeti

Tvoje riječi i slike su javne. Nema zidova koji te sakrivaju.



Postoje pravila

Da bi igra bila zabavna i sigurna za sve, moramo se lijepo ponašati.



• JAVNI PROSTOR



Zdravo svima! 🙌



Pravila Parka = Pravila Interneta

Ista logika važi i online i offline



U javnom parku

Fizički svijet

- Ne pričaš sa potpunim strancima o privatnim stvarima.
- Ako ti neko smeta ili te gura, skloniš se i kažeš odraslima.
- Ne ostavljaš svoj ranac otvoren nasred staze.
- Paziš kako se ponašaš jer te svi vide.



Na internetu

Digitalni svijet

- Ne dijeliš lične podatke sa osobama koje ne poznaješ.
- Ako te neko vrijeda (cyberbullying), blokiraš ga i prijaviš.
- Čuvaš svoje lozinke i ne ostavljaš otključan telefon.
- Paziš šta objavljuješ jer screenshot ostaje zauvijek.

VS



Zapamti: Ako nešto nije sigurno u parku, nije sigurno ni na internetu!

Šta je sve zabavno online?

Internet je kao ogromno igralište puno različitih aktivnosti. Evo šta najčešće radimo:



Igre i Takmičenja

Roblox, Minecraft, Brawl Stars... Timska igra i zabava sa drugarima.



Video i Muzika

YouTube, TikTok, crtači i omiljene pjesme. Gledanje smiješnih klipova.



Učenje i Otkrivanje

Tutorijali "kako napraviti", zanimljive činjenice, pomoć oko domaćeg.



Druženje i Chat

Dopisivanje sa prijateljima, video pozivi, dijeljenje fotografija.

Zabava + Odgovornost

Kako da uživamo online, a da ostanemo bezbjedni



Svijet zabave

Ono što volimo

- Gledanje smiješnih videoa i memova.
- Dopisivanje i video pozivi sa prijateljima.
- Igranje online igrica i takmičenja.
- Istraživanje hobija i učenje novih vještina.



Naša odgovornost

Ono što moramo

- Provjeri informaciju prije nego je podijeliš.
- Razmisli: "Da li bi ovo rekao/la nekome u lice?"
- Poštuj tuđu privatnost i ne objavljuj tuđe slike.
- Ako vidiš nasilje, nemoj čutati – prijav!



Balans je ključ: Možemo se zabavljati i biti sigurni u isto vrijeme!

Šta je Javno vs Šta je Privatno

Razlika između onoga što svi vide i onoga što čuvaš samo za sebe



Javno (Public)

Vide svi, čak i stranci

- Tvoji komentari na popularnim videima (YouTube, TikTok).
- Slike na otvorenim profilima koje svako može zapratiti.
- Tvoje korisničko ime i profilna slika u igricama.
- Sve što podijeliš u "Public" grupama ili chatovima.



Privatno (Private)

Samo za tebe i bliske osobe

- Poruke koje šalješ samo najboljim prijateljima ili porodicu.
- Tvoja kućna adresa, broj telefona i ime škole.
- Lozinke za tvoje naloge (to ne zna ni najbolji drug!).
- Slike iz kuće koje ne želiš da vidi cijeli svijet.

VS



Savjet: Uvijek provjeri podešavanja privatnosti na svojim profilima!

Šta nikada ne dijelimo?

Ovo su tvoji **privatni podaci**. Zamisli ih kao ključ od kuće – ne daješ ga bilo kome, zar ne?



Puno ime i škola

Tvoje prezime i ime škole su kao putokaz do tebe. Stranci ne trebaju znati u koju školu ideš.



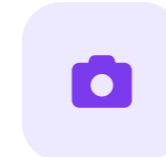
Adresa i telefon

Gdje stanuješ i tvoj broj telefona su samo za prave prijatelje koje poznaješ u stvarnom životu.



Tvoje lozinke

Lozinka je kao četkica za zube – ne dijeliš je ni sa kim! (Osim sa roditeljima).



Slike ulice i kuće

Fotografije na kojima se vidi tvoja kuća, auto registracija ili ime ulice otkrivaju tvoju lokaciju.

Digitalni Otisak: Tvoj trag ostaje

Sve što radiš online ostavlja trag koji je teško izbrisati.



Širenje i kopiranje

Prijatelji mogu da sačuvaju (save), slikaju ekran (screenshot) ili podijele dalje. Čak i ako ti je profil privatан, neko može pokazati drugima.

Klikneš "objavi" ili pošalješ poruku. U tom trenutku tvoja slika, tekst ili video odlaze na servere (velike računare) koji ih čuvaju.



Brisanje nije kraj

Kada klikneš "obriši", ti to više ne vidiš. Ali kopije na tudem telefonima ili serverima mogu ostati dugo vremena. Internet ne zaboravlja lako!

Kako nastaje tvoj digitalni otisak?

Svaki klik ostavlja trag, baš kao stope u pijesku



Sve se sabira!

Čak i male stvari koje radiš svaki dan grade tvoju sliku na internetu.

-  **1. Objave i fotografije**
Selfiji, slike sa rođendana, snimci kućnih ljubimaca koje postaviš.
-  **2. Lajkovi i komentari**
Ono što ti se sviđa i šta pišeš drugima (čak i u šali) ostaje zapisano.
-  **3. Lokacija i pretrage**
Gdje si se "čekirao/la" i šta pretražuješ na Google-u ili YouTube-u.
-  **4. Čak i kad "obrišeš"**
Screenshot-ovi mogu sačuvati tvoju objavu zauvijek, iako si kliknuo/la delete.

Ko te sve može vidjeti online?

Nisi sam/a u digitalnom parku. Evo ko sve može gledati tvoj profil i objave:



Prijatelji i Porodica

Ljudi koje poznaješ i voliš. Oni vide tvoje slike jer si ih prihvatio/la za prijatelje.



Nepoznate Osobe

Ako ti je profil javan, BILO KO na svijetu može vidjeti tvoje objave. Baš kao prolaznici u parku.



Kompanije (Aplikacije)

TikTok, Instagram i YouTube prate šta lajkuješ da bi ti slali reklame i preporuke.



Nastavnici i Treneri

Škole i klubovi često pogledaju internet prije nego što te upoznaju ili prime u tim.

Šta vidiš **TI** vs Šta vide **ONI**

Kako funkcioniše prikupljanje podataka i algoritmi



Tvoj pogled

Korisničko iskustvo

- Besplatna zabava, igrice i dopisivanje sa prijateljima.
- Preporuke videoa "baš za tebe" (For You Page).
- Kul filteri za slike i zanimljivi kvizovi.
- Jednostavna prijava "samo jednim klikom".



Njihov pogled

Algoritmi i podaci

- Bilježe svaki tvoj klik, lajk i koliko sekundi gledaš sliku.
- Znaju tvoju tačnu lokaciju, model telefona i bateriju.
- Prave tvoj "profil" da bi ti prodali skuplje reklame.
- Cilj algoritma: Da ostaneš na aplikaciji što duže!

VS



Zapamti: Ako je aplikacija besplatna, proizvod si najčešće **TI** (i tvoji podaci)!

Stranci na internetu: Crvene Zastavice

Ako primijetiš bilo šta od ovoga, odmah se isključi i reci odrasloj osobi!



Pravilo broj 1:

"Ako ti je čudno u stomaku, nešto nije u redu!"



Traže tajne ili fotografije

Niko dobromjeran neće tražiti da mu šalješ slike koje ne bi pokazao/la roditeljima, niti će tražiti da čuvaš "naše male tajne".



Nagovaraju na brz odgovor ili susret

Stvaraju pritisak ("odgovori odmah ili se ljutim") ili te nagovaraju da se nadete u parku bez znanja roditelja.



Glume da su neko drugi

Mogu reći da su tvojih godina, da idu u tvoju školu ili da vole iste igrice samo da bi ti se približili. To se zove "Catfishing".



Nude poklone ili Robux-e

Obećavaju besplatne stvari u igricama, novac ili poklone u zamjenu za tvoje podatke ili slike.

Šta kad piše nepoznata osoba?

Ako dobiješ poruku od nekoga koga ne poznaješ u stvarnom životu, prati ova 4 pametna koraka:



1. NE Odgovoraj

Ne piši nazad. Ne šalji slike. Ne klikaj na linkove.
Samo stani.



2. Sačuvaj Dokaz

Napravi "screenshot" poruke. To je dokaz ako budeš morao/morala prijaviti.



3. Blokiraj

Pritisni dugme "Block" ili "Blokiraj". Tako ti više ne mogu pisati.



4. Reci Odraslima

Odmah pokaži roditeljima ili nastavniku. Nisi ti kriv/a i oni će pomoći.

Kako se zaštитiti online?

Četiri jednostavna koraka koja čine tvoj digitalni svijet mnogo sigurnijim.



Jaka Lozinka

Koristi dugačke lozinke sa mješavinom slova, brojeva i znakova. Zamisli ih kao ključ od kuće – ne daješ ga svakome!

#Bez123456

#Unikatno



Dvofaktorska Prijava (2FA)

Uključi "potvrdu u dva koraka". To je kao da imaš i ključ i alarm. Čak i ako neko sazna lozinku, ne može ući bez tvog telefona.

#DuplaZaštita



Privatni Profil

Drži svoje profile zaključanim (private). Tako ti biraš ko može da vidi tvoje slike i priče. Neka tvoj digitalni park ima ogradu.

#SamoPrijatelji



Oprezno sa Klikovima

Ne otvaraj sumnjive linkove u porukama ("osvojio si nagradu!"). To su često zamke. Ažuriraj telefon redovno.

#StopPhishing

#Update



Pro Savjet: Koristi Password Manager aplikaciju da ne moraš pamtitи sve te komplikovane lozinke!

Kako se zaštiti (dodatni savjeti)

Osim jakih lozinki, važno je i kako se ponašamo u digitalnom parku. Evo još nekoliko zlatnih pravila:



Razmisli pa objavi

Zapitaj se: "Da li bih ovo pokazalo svima u parku?" Ako je odgovor NE, nemoj objavljivati.



Oprezno sa linkovima

Ne klikaj na linkove koji nude "besplatne nagrade" ili izgledaju čudno. To su često zamke.



Blokiraj i Prijavi

Ako te neko uznemirava, odmah koristi opciju "Block" i "Report". To je tvoja supermoć!



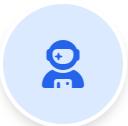
Uvijek se odjavi

Kada koristiš školski ili tudi uređaj, uvijek klikni "Log Out" kada završiš. A ako se pak moraš logovati s tuđeg uređaja, ne dozvoli opciju "zapamti me".

Priče iz stvarnog života

Učenje na tuđim greškama je pametno. Evo šta su ova djeca naučila na teži način.

✓ LEKCIJA: PRIVATNOST



Markova priča

11 godina

⚠ Šta se desilo?

Marko je imao otvoren profil i prihvatao je sve zahtjeve za prijateljstvo da bi imao više pratilaca. Jedan "prijatelj" je počeo da mu šalje ružne poruke i traži da mu Marko pošalje sliku iz svoje sobe.

💡 Šta je naučio?

"Sada je moj profil zaključan. Prihvatom samo ljudе koje stvarno poznajem iz škole ili treninga. Broj pratilaca nije važniji od moje sigurnosti."

✓ LEKCIJA: LOKACIJA



Anina priča

10 godina

⚠ Šta se desilo?

Ana je objavila sliku u parku i tagovala tačnu lokaciju dok je još bila tamo. Neko koga ne poznaje se pojavio u parku i počeo da je doziva po imenu, rekavši da je bio na internetu gdje se nalazi.

💡 Šta je naučila?

"Nikad više ne objavljujem lokaciju uživo. Slike iz parka ili sa putovanja objavljujem tek kad se vratim kući na sigurno."

Ti si Digitalni Čuvar!



Svako može biti digitalno hrabro i pametno dijete.



Internet je kao javni park

Ponašamo se pristojno i pazimo na nepoznate osobe, baš kao u parku.



Tvoje tajne su tvoje blago

Ne dijelimo adresu, školu ni lozinke sa strancima. Privatnost je moć!



Pomoć je uvijek dostupna

Ako vidiš nešto čudno ili se osjećaš nelagodno, odmah reci odrasloj osobi.



Male navike = Velika bezbjednost

Tvoje znanje te štiti. Svaki put kad razmisliš prije klika, ti si heroj interneta!

SLJEDEĆI KORAK

Vrijeme za Kviz!



Vrijeme je za Kratki Odmor

Napuni baterije za nastavak!

5

MINUTA



Hidratacija

Popij čašu vode



Pokret

Istegni se malo



Fokus

Spremi se za kviz



Vidimo se uskoro na Quizizz kvizu!

VRIJEME ZA IGRU!

Quizizz Kviz

Pokaži svoje znanje i osvoji poene!

1

Uzmi telefon ili tablet

Pripremi se za igru

2

Otvori quizizz.com/join

Ili skeniraj QR kod sa desne strane

3

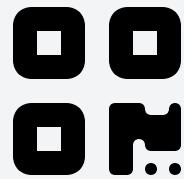
Unesi kod i svoje ime

Koristi nadimak ako želiš!



Skeniraj Kod

Otvori kameru na telefonu



GAME CODE

XXXXXX

Unesite ovaj kod na quizizz.com/join

Vrijeme za Razgovor



Šta mislite o onome što smo upravo naučili?



Iznenadjenje?

Šta vas je najviše iznenadilo u današnjoj priči o internet parku?



Moj Potez

Koji savjet o bezbjednosti ćete primijeniti već danas kada dođete kući?



Detektivi

Kako bismo sada prepoznali lažan profil ili sumnjivu osobu online?

👉 Podignite ruku ako imate ideju ili pitanje!

Šta smo naučili?

Ključne lekcije iz naše internet avanture



Internet je kao javni park

Ponašamo se pristojno jer nas svi vide. Ono što kažemo i uradimo ostaje zabilježeno.



Čuvamo svoje tajne

Lozinke, adresa i škola su privatni podaci. Ne dijelimo ih sa nepoznatima u igricama ili chat-u.



Stop, Blok, Prijavi

Ako se osjećaš nelagodno ili neko traži čudne stvari – odmah reci odrasloj osobi od povjerenja!



Bravo, Digitalni Čuvari!

Sada imate moć znanja. Koristite internet pametno i sigurno!

Slijedi: Veliki Kviz!



DRUGA GRUPA

DIO B

Realni slučajevi, **OSINT** tehnike, **AI** rizici i napredna zaštita
privatnosti u 2026. godini.



OSINT



AI & Deepfake



Cyber Zaštita



Dobrodošli nazad!



Sada prelazimo na napredne alate i stvarne rizike.



Cilj: Kritičko razmišljanje

Ne vjerujemo svemu što vidimo. Provjeravamo izvore i tragamo za dokazima.



Tema: Identitet i Privatnost

Kako zaštititi svoj pravi identitet dok istražujemo digitalni svijet.



Otvorena diskusija

Vaša iskustva su važna. Dijelimo priče bez osude i učimo iz grešaka.

Phishing napad: Marijin slučaj

Kada poruka od "priateljice" postane noćna mora. Kako prepoznati prevaru na vrijeme?

! INCIDENT

✓ RJEŠENJE



"Hitna" poruka

14 godina

⚡ Šta se desilo?

Marija je dobila DM na Instagramu od najbolje drugarice: "Hej!
Glasaj za mene na ovom linku, treba mi još 5 glasova da pobijedim! 🙌 Link: bit.ly/vote-contest"

Kada je kliknula, stranica je tražila da se uloguje sa Instagram podacima. Uradila je to bez razmišljanja. Dva sata kasnije, njen nalog je bio hakovan i slao je istu poruku svima.



Kako prepoznati?

Analiza

Q Crvene zastavice

- ✗ **Hitnost:** Poruka traži brzu reakciju ("još 5 glasova").
- ✗ **Čudan link:** Skraćeni linkovi (bit.ly) često kriju pravu adresu.
- ✗ **Ponovno logovanje:** Ako si već u aplikaciji, ona ti NIKAD neće tražiti password ponovo za "glasanje".

💡 Šta uraditi?

"Uvijek pozovi drugaricu ili pošalji SMS da provjeriš da li je ona stvarno poslala taj link. Ako traži lozinku = PREVARA."

Internet je park sa kamerama svuda



Sve se snima i čuva

Svaki klik, lajk, komentar i pretraga ostaju zabilježeni kao digitalni snimak.



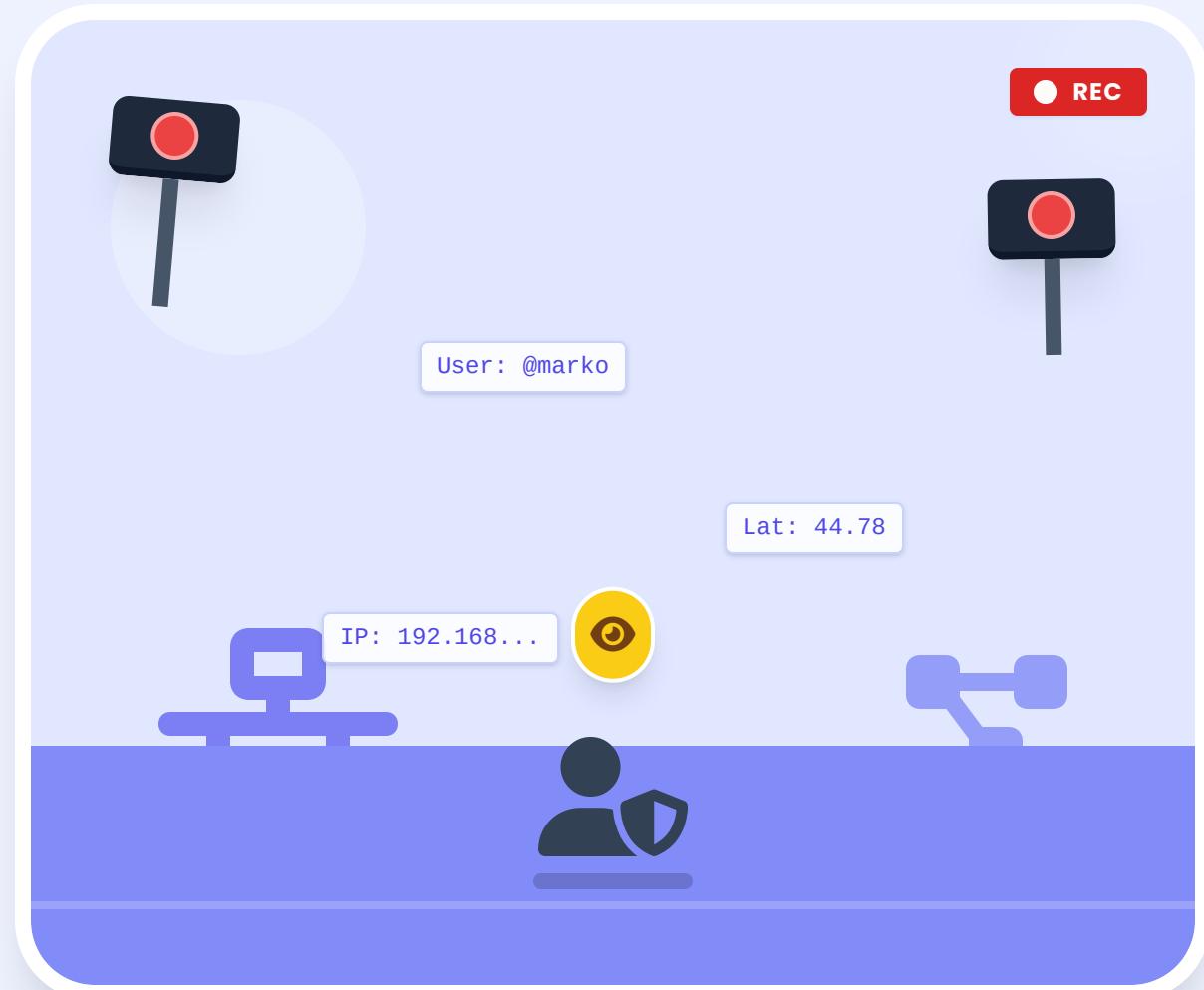
OSINT koristi te snimke

Open Source Intelligence je vještina pronalaženja tih javnih podataka o bilo kome.



Nema skrivanja u javnosti

Čak i "privatni" podaci mogu procuriti ili se otkriti kroz analizu tvojih navika.



Šta je OSINT?

Open Source Intelligence / Obavještajni rad iz otvorenih izvora

OSINT je prikupljanje i analiza informacija koje su **javno dostupne** svima na internetu.

Napadači ne moraju da "provaljuju" šifre – oni samo slažu slagalicu od onoga što smo sami objavili.

PROCES PRIKUPLJANJA PODATAKA:



1. Javni Izvori

Društvene mreže, forumi, novinski članci, mape, javni registri.



2. Prikupljanje

Pretraga korisničkih imena, starih komentara, tagovanih slika.



3. Povezivanje

Spajanje "nebitnih" detalja (npr. slika karte za koncert + check-in).



4. Tvoj Profil

Napadač sada zna gdje živiš, u koju školu ideš i šta voliš.

KLJUČNA POENTA

Tvoji "sitni" digitalni tragovi zajedno formiraju veliku sliku o tebi.





OSINT u Praksi: Alati Pretrage

1 Obrnuta Pretraga Slike (Reverse Image Search)

tool: Google Lens / TinEye

**Ulazni Podatak**

Tvoja profilna slika sa Instagrama

**Analiza**

Pretraživač skenira milijarde slika

**Rezultat**Ista slika na sajtu škole = **Lokacija otkrivena**

2 Pretraga Korisničkog Imena (Username Enumeration)

tool: Sherlock / Maigret

**Korisničko Ime**

@marko_gamer99

**Povezivanje**

Provjera imena na 500+ sajtova

**Digitalni Profil**Twitch + Reddit + Roblox = **Identitet složen**

OSINT u Praksi: Analiza Profila

Kako istraživači povezuju informacije iz biografije i prijatelja

> social_graph_analysis.exe

01

Datum Kreiranja

Novi profili su sumnjivi. Istraživači provjeravaju kada je nalog napravljen.

Target: Suspicious

Created: 2 days ago

02

Analiza Biografije

Nedosljednosti u školi, poslu ili lokaciji. "Živi u Parizu", a slike su iz lokalnog parka.

✗ Lokacija: New York

✓ IP: Local ISP

03

Mreža Prijatelja

Ko su prijatelji? Da li su to stvarni ljudi iz iste škole/grada ili nasumični profili?

BOT

04

Zaključak

Sve informacije zajedno daju sliku: **Pravi profil** ili **Lažnjak (Sockpuppet)**.

VERIFIKACIJA
★★★



19:42

DOKAZ #042

marko_cool_2011

...

128 sviđanja

marko_cool_2011 Napokon su stigle! 🎟 Jedva čekam koncert večeras u Areni! Vidimo se u prvom redu! 🎸🔥

#koncert #subota #party #arena #muzika

PRIJE 2 SATA

> TVOJA MISIJA

Ova osoba misli da je samo podijelila sreću sa prijateljima. **Tvoj zadatak:** Pronađi 3 skrivene informacije koje je slučajno otkrila javnosti.

PODATAK 1

1 Gdje se tačno nalazi?



PODATAK 2

2 Kada planira biti tamo?



PODATAK 3

3 Šta voli (potencijalna lozinka)?



UPOZORENJE: Ovi podaci mogu biti iskorišteni za "spear-phishing" napad.



AI Prijetnje: Deepfake Tehnologija

Video ili audio sadržaj koji je generisala vještačka inteligencija, a koji izgleda toliko stvarno da je teško razlikovati istinu od laži.



Face Swapping

Zamjena lica jedne osobe licem druge u videu u realnom vremenu.



Voice Cloning

AI može kopirati nečijii glas nakon samo 3 sekunde slušanja uzorka.

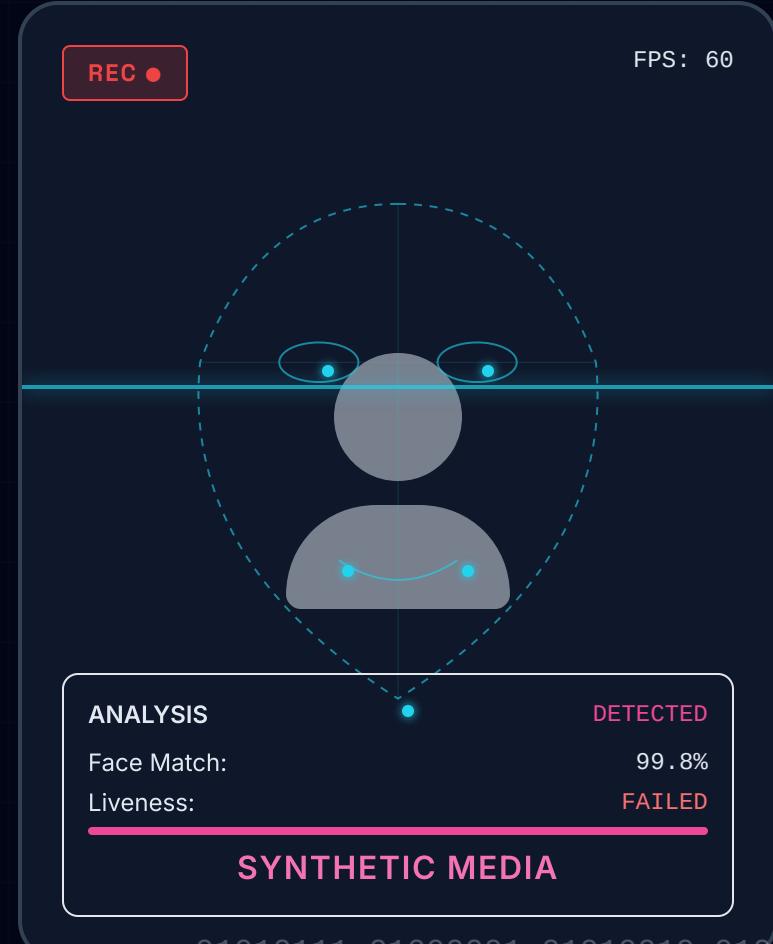


Lip Syncing

Manipulacija pokreta usana da izgleda kao da osoba govori riječi koje nikad nije rekla.

⚠ ZLATNO PRAVILO 2026

"Ne vjeruj svemu što vidiš ili čuješ na internetu. Uvijek provjeri izvor."



01010111 01000001 01010010 01001110
01001001 01001110 01000111 00111010
01000100 01000101 01000101 01010000
01000110 01000001 01001011 01000101

Kako Prepoznati Deepfake?

Iako je AI napredan, i dalje pravi greške. Tvoje oko može biti bolji detektor od softvera ako znaš gdje da gledaš.



Neprirodno Treptanje

Osoba trepće previše rijetko, previše često ili nikako. Oči mogu izgledati "prazno" ili staklasto.



Greške u Govoru (Lip-Sync)

Pokreti usana se ne poklapaju savršeno sa zvukom. Zubi mogu izgledati kao jedna ravna ploha.

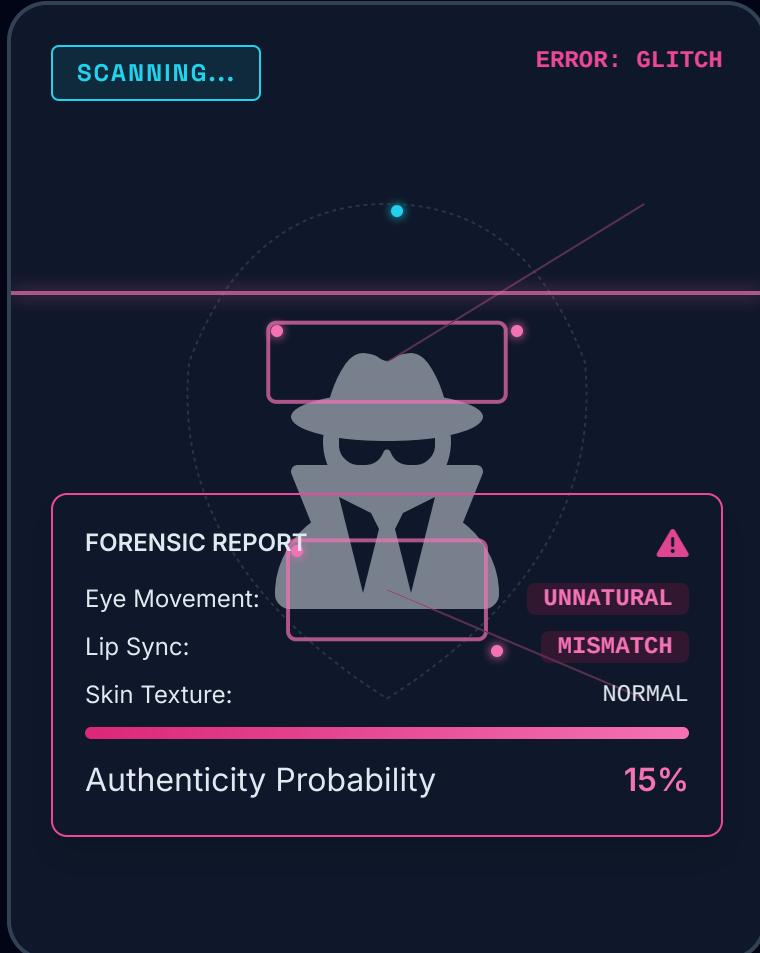


Mutni Rubovi i Glitchevi

Obrati pažnju na liniju kose, vrat i rubove lica. Tu se često vide mrlje ili digitalne smetnje.

PROVJERI IZVOR

"Ako ti video izaziva jake emocije (strah, bijes), stani i provjeri da li o tome pišu i drugi pouzdani mediji."



ERR_FRAME_DROP_224

SYNC_OFFSET_MS: 450

ARTITACT_DETECTED

AI AUDIO PRIJETNJA



Voice Cloning: Ukradeni Glas

AI sada može kopirati nečiji glas nakon samo 3 sekunde snimka.
Prevaranti koriste ovo za lažne pozive vašim roditeljima.



3 Sekunde je Dovoljno

Sa TikTok videa ili Instagram Story-ja mogu uzeti uzorak tvog glasa.



"Mama, u nevolji sam!"

Najčešća prevara: poziv roditeljima glasom djeteta koje traži hitan novac.

🛡 KAKO SE ZAŠTITITI?

"Dogovorite **porodičnu šifru** (tajnu riječ) koju znate samo vi. Ako neko zove i traži nešto hitno, traži šifru!"

The smartphone screen displays an AI analysis interface. At the top left is a red button labeled "AI DETECTED". To its right is a blue microphone icon with the text "Voice Match" and "Target: You 99.9%". Below this is a purple oval containing a white person icon. To the right of the icon is the name "Mama". Underneath the name is the text "Mobile • 00:14". On the left side of the screen, there is a box containing the text "AUDIO ANALYSIS" and "SYNTHETIC 98%". On the right side, there is a box containing the text "Frequency pattern matches AI generation model V4". At the bottom of the screen are two circular buttons: a red one with a white scissors icon and a green one with a white phone icon.

Obrana od Voice Cloning Prevara

Tvoj glas je jedinstven, ali AI ga može kopirati. Evo kako da se zaštitiš i prepoznaš lažni poziv.



Porodična "Sigurna Riječ"

Dogovorite tajnu riječ koju samo vi znate (npr. "ljubičasti dinosaurus"). Ako te neko nazove i traži novac glasom člana porodice, traži tu riječ!

#TajnaŠifra

#PorodičniKod



Prekini i Pozovi Nazad

Ako je poziv sumnjiv ili hitan ("izgubio sam telefon"), prekini vezu. Odmah pozovi tu osobu na njen pravi broj ili pozovi nekog drugog ko je s njom.

#ProvjeriIzvor



Nikad Ne Šalji Novac/Kodove

Prevaranti koriste AI glas da traže hitan transfer novca ili kodove za prijavu. Pravi prijatelji te to nikad neće tražiti na takav način.

#StopPrevari



Ograniči Javne Uzorke Glasa

AI treba samo 3 sekunde tvog glasa da ga klonira. Razmisli prije nego što objaviš javne videoe gdje puno pričaš, ili zaključaj profil.

#Privatnost



Zapamti: AI može imitirati glas, ali ne može znati vaše interne šale ili uspomene. Pitaj nešto lično!



Credential Stuffing

ATTACK_VECTOR: PASSWORD_REUSE

SEC_LEVEL: HIGH

Šta se dešava kada koristiš **istu lozinku** na više mesta?



Curenje podataka

Hakeri provale u slabiji sajt (npr. stari forum za igrice) i ukradu bazu korisnika i lozinki.



Automatizacija

Koriste botove (softver) da automatski isprobaju te iste email-ove i lozinke na hiljadama drugih sajtova.



Poklapanje

Ako koristiš **istu lozinku** za Instagram ili TikTok, botovi uspješno ulaze u tvoj nalog.



Preuzimanje

Napadač mijenja lozinku, krade podatke ili šalje prevare tvojim prijateljima.



CRITICAL_RISK: Jedna provajljena lozinka otključava sve tvoje naloge oko su isti.

SESSION_ID: SECURE_2026

Kako zaustaviti kradbu lozinki?

Alati koji zaključavaju tvoja vrata dok hakeri još traže ključ.



Password Manager

Ne moraš pamtitи 50 lozinki! Koristi "sef" koji ih pamti za tebe i automatski popunjava. Pamtiš samo jednu glavnu lozinku.

#Bitwarden

#1Password



Passkeys (Bez lozinke)

Budućnost bez kucanja! Prijavljuješ se otiskom prsta ili licem (FacID), baš kao što otključavaš telefon. Nemoguće za ukrasti.

#Budućnost

#Sigurno



Unikatne Lozinke

Nikad ne koristi istu lozinku na dva mesta. Ako hakeri probiju jedan sajt, tvoj email i banka ostaju sigurni.

#PraviloBroj1



MFA / 2FA Obavezno

Čak i ako imaju tvoju lozinku, ne mogu ući bez koda sa tvog telefona. Ovo zaustavlja 99% automatskih napada.

#AuthenticatorApp



Ekspert savjet: Provjeri da li je tvoja lozinka već ukradena na sajtu [haveibeenpwned.com](#)

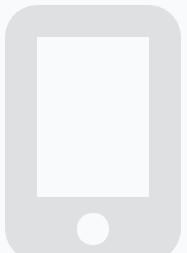


Algoritamska Zavisnost

Kako aplikacije koriste "dopaminski krug" da zadrže tvoju pažnju?



Rješenje: Prepoznaj okidač i isključi "autoplay" funkcije!



Kako vratiti balans?

Preuzmi kontrolu nad svojim vremenom i pažnjom

3 Koraka do slobode



Isključi notifikacije

Ostavi uključene samo one za poruke od stvarnih ljudi. Aplikacije ne moraju da te "cimaju".



Postavi limite

Koristi "Screen Time" ili "Digital Wellbeing" alate da ograničiš TikTok/Insta na 30 min dnevno.



Siva skala (Grayscale)

Probaj da prebacиш ekran na crno-bijelo. Telefon postaje dosadan alat umjesto šarene igračke.



Punjjenje baterija

"Tehnologija je odličan sluga, ali užasan gospodar."

TI BIRAŠ KADA JE KRAJ SKROLOVANJA!



Savjet: Ostavi telefon u drugoj sobi dok spavaš.

Napredna zaštita i alati

Alati i postavke koje te pretvaraju u digitalnog nindžu.



Anonimnost & Browseri

"Incognito" nije dovoljno. Koristi browsere kao što su Brave ili Firefox Focus koji automatski blokiraju trekere i reklame.

[#NoTrackers](#)[#Brave](#)

Kontrola Podataka

Redovno radi "Privacy Checkup". Isključi istoriju lokacije i personalizovane oglase u Google i Facebook podešavanjima.

[#Settings](#)[#Privacy](#)

Provjera Izvora

Ne vjeruj svemu! Koristi "Reverse Image Search" (Google Images, TinEye) da provjeriš da li je slika stvarna ili lažna.

[#FactCheck](#)[#StopFake](#)

Sigurnost Uredaja

Obavezno zaključavanje ekrana (FaceID/PIN). Ažuriraj telefon čim stigne notifikacija – to krpi sigurnosne rupe.

[#Update](#)[#LockScreen](#)

Pro Savjet: Instaliraj ekstenziju kao što je "uBlock Origin" da blokiraš dosadne reklame i skripte koje te prate!

REALNI SLUČAJEVI INCIDENATA

AI PREVARA

12. Mart 2026.

DIREKTOR "ZVAO" PREKO VIDEA: UKRADENO 2 MILIONA EURA

Kompanija u Hong Kongu izgubila milione nakon što je radnik prisustvovao video sastanku gdje su svi učesnici, uključujući direktora, bili **AI Deepfake** generisani likovi.

TECH GLOBAL NEWS

SCAM ALERT

22. Feb 2026.

LAŽNI INFLUENSERI DIJELE ZARAŽENE LINKOVE

Hiljade tinejdžera izgubilo pristup svojim profilima nakon klika na link za "ekskluzivni giveaway" koji je promovisao **lažni profil poznatog YouTubera**.

SOCIAL TRENDS

VOICE CLONING

05. Jan 2026.

"MAMA, U NEVOLJI SAM": AI GLASOVNI VARAJU RODITELJE

Policija upozorava na porast poziva u kojima prevaranti koriste **klonirani glas djece** (uzorci uzeti sa TikToka) da traže hitan novac od roditelja.

CYBER SECURITY WEEKLY

GAMING & DATA

18. Dec 2025.

CURENJE LOZINKI NA POPULARNOJ GAMING PLATFORMI

Hakeri objavili bazu sa 500.000 korisničkih naloga. Korisnici koji su imali **istu lozinku** na drugim mrežama sada su pod napadom.

GAMER INSIDER

Šta učimo iz realnih slučajeva?

Greške se dešavaju, ali najvažnije je izvući pouku. Evo dva ključna zaključka iz 2025.

LEKCIJA: DETALJI



Sitni tragovi

Digitalna forenzika

Q Šta smo vidjeli?

Čak i slučajni detalji poput imena ulice na znaku u pozadini, specifične uniforme ili ulaznice na stolu mogu otkriti tvoju tačnu lokaciju ili identitet napadačima.

Pouka

"Provjeri pozadinu svake fotografije prije objave. Tvoj 'običan selfie' može sadržati previše informacija za nekoga ko zna da gleda."



Moć prijave

Odgovornost zajednice

⚠ Šta smo vidjeli?

Mnogi incidenti eskaliraju jer žrtve samo blokiraju nasilnika, ali ga ne prijave platformi. To omogućava napadaču da jednostavno pređe na sljedeću metu.

Pouka

"Prijavljivanje (Report) nije tužakanje, već čin digitalne građanske hrabrosti. Time štitiš ne samo sebe, već i cijelu zajednicu."

PAUZA

Kratki Odmor



Osvježi se i pripremi za kviz!

5
minuta



Popij vode



Prošetaj



Spremi fokus

Slijedi: Quizizz Izazov & OSINT Zadatak

PROVJERA ZNANJA

Quizizz Kviz

Testiramo tvoje znanje o OSINT-u i AI prijetnjama!

1 Pripremi uređaj

Telefon ili tablet su spremni?

2 Otvori quizizz.com/join

Skeniraj QR kod za brzi pristup

3 Unesi kod i nadimak

Pokaži koliko znaš o digitalnoj bezbjednosti!

Skeniraj Kod

Brzi pristup kvizu



GAME CODE

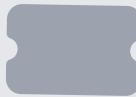
XXXXXX

Unesite kod na quizizz.com/join

🔍 TARGET_SOURCE: INSTAGRAM_PUBLIC

JS **jovan_skater_012**
Prije 14 minuta

...



📍 Central Park, BG

❤️ 💬 📲 

jovan_skater_012 Jedva čekam koncert večeras! Karta je tu, vidimo se u prvom redu! 🎸🔥
#koncert #subota #uzbudjenje #mojakarta

⚠️ UPOZORENJE: Slika sadrži barkod

DATA

'] opacity-30 pointer-events-none z-0">

TVOJA MISIJA

Analiziraj objavu i pronađi skrivene rizike.

1 Identifikuj Lokaciju

Gdje se tačno nalazi osoba u trenutku objave?

2 Pronađi Datum/Vrijeme

Kada se dešava događaj o kojem piše?

3 CRITIČNO: Krada Karte

Šta na slici omogućava nekome da ukrade kartu?

⌚ Vrijeme: 02:00

ZAPOČNI ANALIZU →

0101

 MISIJA ZAVRŠENA

ZNANJE = MOĆ

Internet je tvoj prostor. Koristi ga za učenje, zabavu i stvaranje, ali uvijek ostani korak ispred rizika.



Pametne Odluke

Svaki klik, svaka objava i svaki "Accept" je tvoja odluka. Zastani i razmisli prije nego što djeluješ.



Jake Postavke

Tvoji profili su tvoja kuća. Zaključaj vrata (privatnost) i ne puštaj nepoznate unutra.



Dijeli Znanje

Nauči prijatelje, roditelje ili brata/sestru ono što si danas saznao/la. Budi digitalni heroj za druge!



Tvoja sigurna avantura počinje SADA!

KORISNI LINKOVI

Resursi i Podrška

Nastavi da istražuješ i učiš. Evo nekoliko sigurnih mesta gdje možeš pronaći pomoć ili zabavu.



Quizizz Platforma

Kreiraj svoje kvizove, izazovi prijatelje i ponovi gradivo o bezbjednosti kroz igru.

 quizizz.com



Pomoć i Podrška

Ako se osjećaš nesigurno ili doživiš nasilje online, ovdje možeš potražiti anonimnu pomoć.

 [Lokalni Helpline / 116-111](tel:116111)



Centar za Bezbjednost

Vodiči, savjeti za podešavanje privatnosti na Instagramu, TikToku i Snapchatu.

 [kliknibezbedno.rs / .ba](http://kliknibezbedno.rs)



Predavač

Radionica Digitalne Bezbjednosti



kmail@kontakt.com



www.moj-sajt.com

Vodič za Predavača



Ključne napomene, struktura i savjeti za uspješnu radionicu

Ukupno trajanje: 120 min (2 × 60 min)



Jezik i Ton

- ✓ **Ijekavica:** "dio", "djeca", "bezbjednost".
- ✓ **Gender Neutral:** Koristi "dijete", "osoba", "neko" umjesto rodnih zamjenica.
- ✗ **Bez godina:** Ne pominji "9-11" ili "12-15". Koristi "Prva grupa" i "Druga grupa".



Struktura Radionice

GRUPA A (Prvih 60 min)

00:00 - 01:00

- 05 min: Uvod i zagrijavanje
- 25 min: Teorija (Park, Privatnost, Otisak)
- 05 min: Kratka pauza
- 25 min: Quizizz & Diskusija

GRUPA B (Drugih 60 min)

01:00 - 02:00

- 05 min: Uvod (Napredniji ton)
- 25 min: Teorija (OSINT, AI, Deepfake)
- 05 min: Kratka pauza
- 25 min: Quizizz & OSINT Izazov



Savjeti za Vođenje

Analogije su ključ: Za prvu grupu uvijek se vraćaj na analogiju parka. To im je poznato i sigurno.

Bez strašenja: Fokus na moći i kontroli ("ti odlučuješ"), a ne na strahu od interneta.

Pitanja: Koristi "Šta biste vi uradili?" umjesto suvoparnog predavanja.



Tehnička Provjera

- Projektor i zvuk rade?
- Internet konekcija stabilna?
- Quizizz kodovi spremni?
- QR kodovi na slajdovima (24, 47)?



Quizizz Savjeti

Priprema: Kreiraj dva zasebna kviza (lakši i teži) prije radionice na quizizz.com.

Pristup: Djeca mogu koristiti telefone. Ako nemaju svi, neka rade u parovima (bolje za diskusiju!).

Fokus: Nije bitno ko pobijedi, već objašnjenje tačnih odgovora nakon svakog pitanja.