

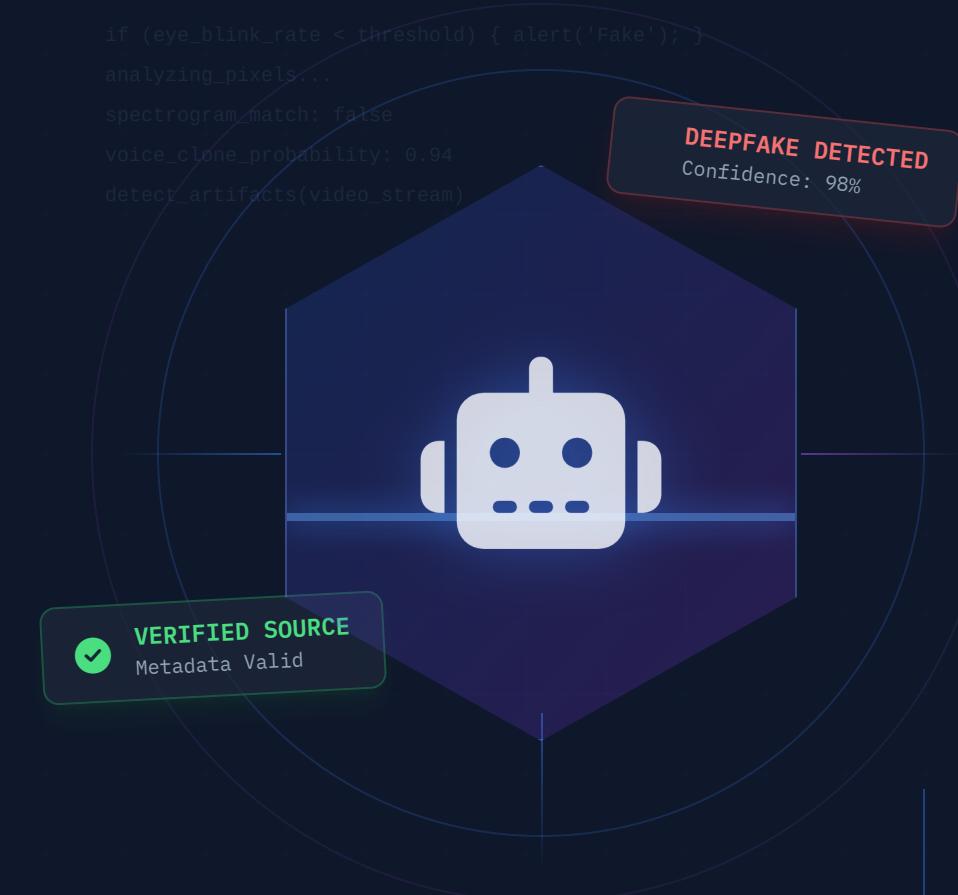
AI i Deepfake Tehnologija

> Otkrijte kako prepoznati lažne video i audio zapise u eri vještačke inteligencije.

Cilj radionice: Razumjeti AI tehnologije, naučiti detektovati deepfake sadržaj i zaštiti se od voice cloning prevara.

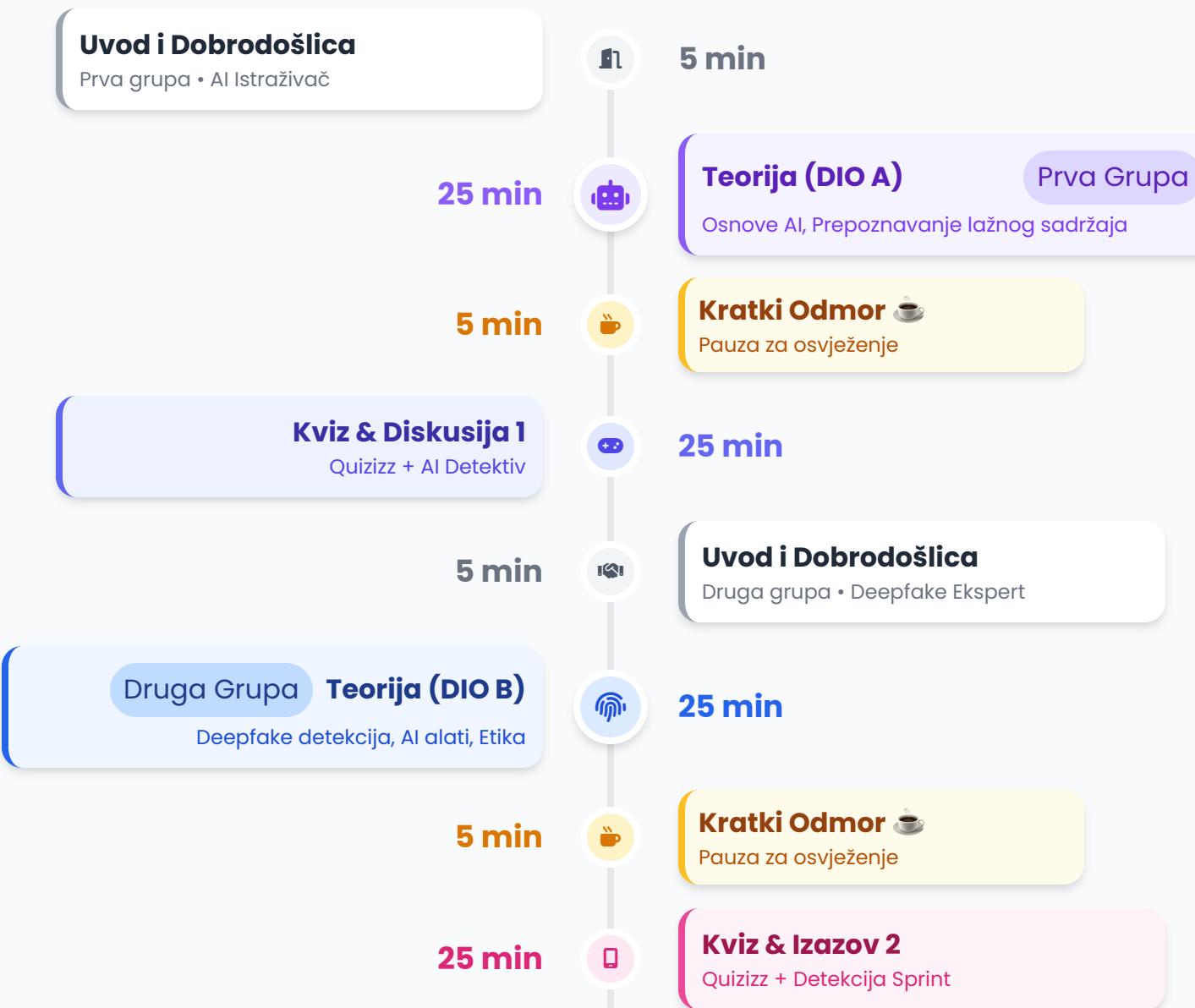
- Dio A: Osnove AI (9-11)

- Dio B: Napredna Detekcija (12-15)



Agenda dana

Plan radionice: AI i Deepfake Tehnologija (120 minuta)



Dobrodošli! 🤖🌟

Danas učimo o vještačkoj inteligenciji i sigurnosti.



Poštujemo jedni druge

Slušamo pažljivo i uvažavamo svačije mišljenje.



Postavljamo pitanja

Nema glupih pitanja! Pitaj sve što te zanima o AI.



Ne dijelimo lične priče

Čuvamo svoju privatnost i ne otkrivamo detalje o drugima.



Učestvujemo u kvizovima i izazovima

Zabavljamo se dok učimo kroz igru i detektivske zadatke!

Plan za Danas

AI i Deepfake Tehnologija: Detekcija i Zaštita



Dio A: Osnove AI

Uvod u vještačku inteligenciju.
Kako mašine uče i stvaraju
sadržaj? Razumijevanje
generativne tehnologije.



Dio A: Prepoznavanje

Učimo uočavati osnovne lažne
elemente. Crvene zastavice:
neprirodno treptanje, čudne
ruke i greške u pozadini.



Dio B: Deepfake

Napredne tehnike detekcije
manipulisanog videoa i zvuka.
Analiza sinhronizacije usana i
"voice cloning" prevara.



Dio B: Sigurnost

Korištenje AI sigurnosnih alata
i verifikacija izvora. Kako se
zaštititi od manipulacije i
ostati siguran online.



Ne vjeruj svemu što vidiš!

MOTIVACIJA

Zašto je ovo važno?

AI lažnjaci mogu prevariti, izmanipulisati i narušiti povjerenje. Tehnologija napreduje brže nego ikad, a 2026. godina donosi nove izazove.



Rizik od Prevare

AI lažnjaci mogu uvjerljivo oponašati stvarnost, navodeći nas da vjerujemo u neistine i postanemo žrtve manipulacije.



Porast Prevara

U 2026. godini očekujemo značajan **porast voice-clone prevara** i lažnih video. Tehnologija postaje sve dostupnija zlonamjernim akterima.

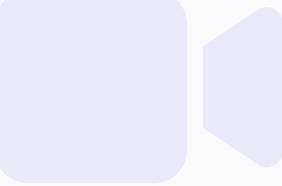


Znanje = Zaštita

Jedini način da se zaštитimo je da razumijemo kako AI radi. Znanje nam daje moć da prepoznamo laž i zaštитimo sebe i druge.



Ne dozvoli da te AI prevari. Nauči da gledaš pažljivije! 🕶️



PRVA GRUPA (9-11 GOD)

DIO A:

Upoznaj AI i prepoznaj lažnjake



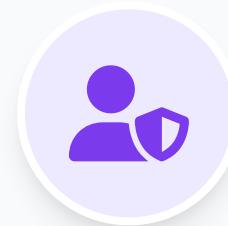
Fokus: jednostavne crvene zastavice, sigurne reakcije i kada pitati odraslu osobu.  



AI Osnove



Crvene Zastavice



Pitaj Odrasle



ANALOGIJA

Deepfake-ovi su kao Lutke na koncu



Pozajmljena lica

Kao što lutka nosi masku, deepfake koristi AI da "nalijepi" tuđe lice ili glas na drugu osobu.



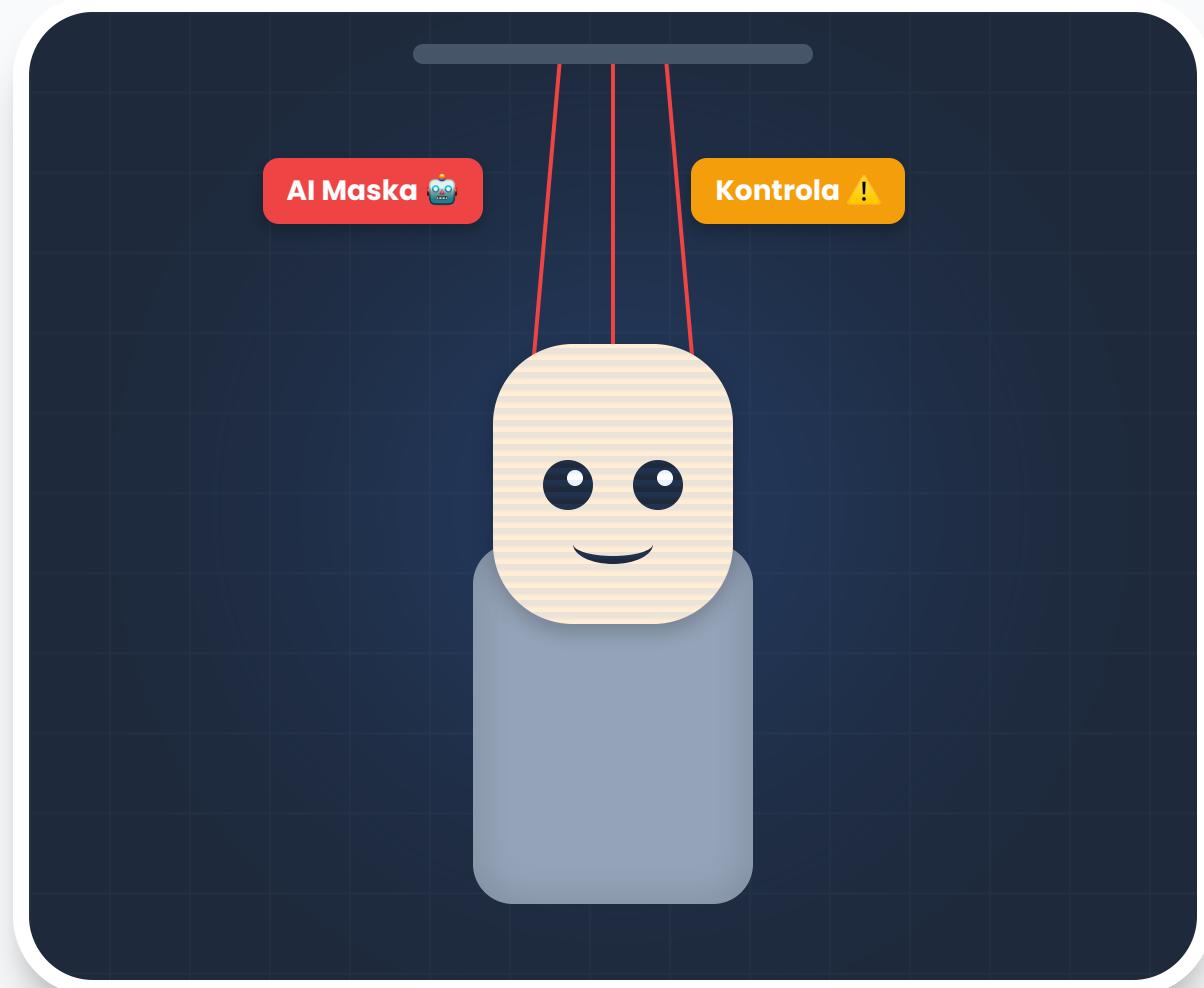
Nevidljivi konci

Neko drugi kontroliše pokrete i riječi. Moramo gledati pažljivo da uočimo te "konce" (greške).



Gledaj pažljivo

Potraži neprirodno trepćenje ili čudne ivice oko lica – to su znakovi da je u pitanju "lutka".



Šta je AI (Vještačka Inteligencija)?

AI je poput super-brzog računarskog mozga. Evo 4 ključne stvari koje trebaš znati:



Uči iz podataka

Čita milione slika i tekstova da bi prepoznao obrasce i naučio kako svijet izgleda.



Pravi nove stvari

Može nacrtati sliku ili napisati sastav koji nikada prije nije postojao.



Može imitirati ljude

Može kopirati nečiji glas ili lice toliko dobro da izgleda stvarno.



Nije uvijek pouzdan

Često griješi ili izmišlja činjenice, a da toga nije svjestan.

Pravo vs AI Generisano

Kako razlikovati stvarni sadržaj od vještačke inteligencije?



Pravo (Real)

Stvarni svijet i ljudi

- ❖ Dosljedni detalji

- 🛡 Pouzdan izvor

Karakteristike

- ✓ Sve izgleda prirodno i logično.
- ✓ Znaš ko je napravio (autor).
- ✓ Kontekst ima smisla.



AI Generisano

Napravio kompjuter

- ⌚ Čudni detalji (ruke, oči)

- ❓ Nepoznat izvor

VS

Znakovi upozorenja

- 🤖 "Wow" efekat i savršene boje.
- 🤖 Pozadina mutna ili nelogična.
- 🤖 Tekst na slici je besmislen.



Savjet: Ako slika izgleda previše savršeno ili čudno, zumbira detalje!

Priča: "Smiješna zamjena lica"

Kada tehnologija učini da video izgleda stvarno, a zapravo je samo AI trik.



Urnebesan video

Poznato lice?

Deepfake aplikacija

Pojavio se video gdje nastavnik fizičkog pleše kao profesionalac u spotu. Izgledalo je 100% stvarno i jako smiješno.

"Je li ovo stvarno naš nastavnik?!"



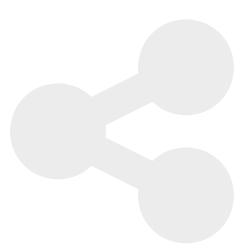
Prijatelji prevareni

Vjerovanje očima

Masovno dijeljenje

Cijeli razred je počeo dijeliti video u grupama. Svi su mislili da nastavnik ima tajni talent. Niko nije posumnjao.

- Hiljade pregleda
- Čudenje i smijeh
- Slijepo vjerovanje videu



Pauza i provjera

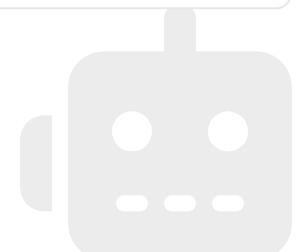
Učenje lekcije

Oštro oko

Maja je pauzirala video. Primjetila je da se lice "zamutilo" kad se okrenuo i da se ivice ne poklapaju. To je bio AI filter!

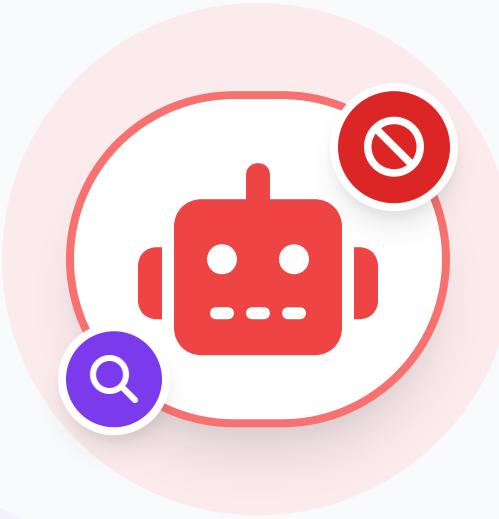


Rezultat: Naučili su prepoznati "glitch" i crvene zastavice AI-ja.



Kako prepoznati lažnjake? 🚨

AI tehnologija je napredna, ali često pravi greške u detaljima. Budi detektiv i potraži ove znakove.



Zlatno pravilo:

"Ako lice izgleda savršeno, ali prsti ili zubi izgledaju čudno - vjerovatno je AI."

Čudne ruke i zubi



AI se često muči sa prstima (ima ih 6 ili su spojeni) i zubima koji izgledaju kao jedna bijela traka.



Trepćenje izgleda neprirodno

U deepfake videima osoba trepće prebrzo, presporo ili nikako. Pogled može djelovati "prazno".



Neusklađeno osvjetljenje

Sjene na licu ne odgovaraju svjetlu u pozadini. Često postoji čudan sjaj oko ivica lica ili kose.



Previše savršen glas

AI klonirani glasovi često nemaju prirodne pauze za disanje, zvuče monotono ili previše "čisto".



Nema link izvora

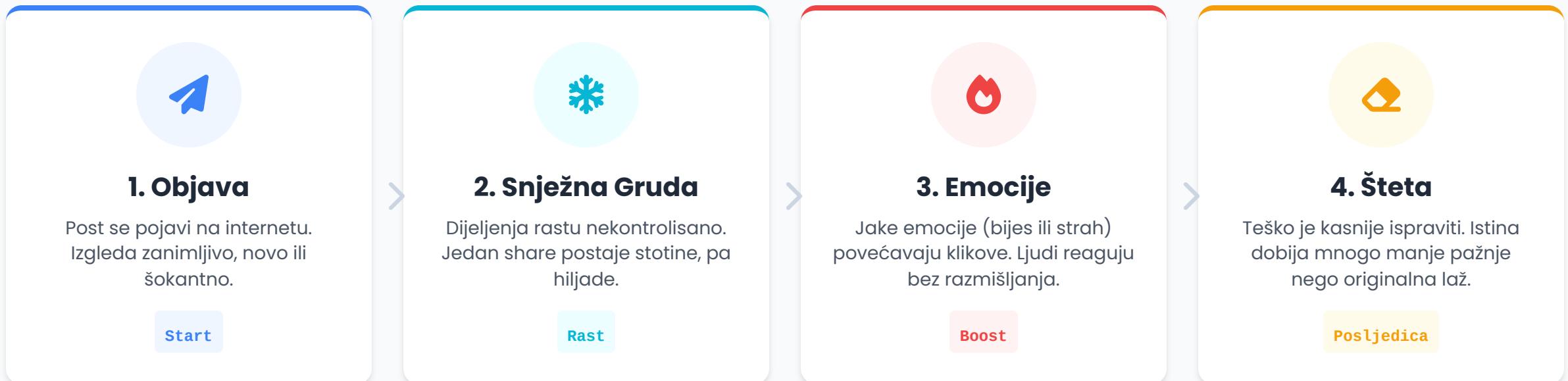
Šokantan video poznate osobe, ali ga nema na vijestima ili njihovom pravom profilu? Vjerovatno je lažnjak.

Kako se lažnjak širi?

4 faze viralnog ciklusa lažne vijesti



LANČANA REAKCIJA:



BRZINA ŠIRENJA

Viralne laži putuju internetom brže od istine.



Česti AI Lažnjaci

Tehnologija napreduje brzo. Evo 4 glavna načina kako AI može manipulisati onim što vidimo i čujemo:



Slike (Face Swaps)

Zamjena lica na fotografijama tako da izgleda kao da je osoba bila negdje gdje nikad nije bila.



Video (Lip-sync)

Manipulacija usana na videu da se savršeno poklapaju sa lažnim audio zapisom.



Audio (Voice Clone)

Kloniranje nečijeg glasa da zvuči potpuno identično, često se koristi za lažne pozive.



Tekst (Lažni Citati)

Generisanje lažnih vijesti ili izjava koje poznata osoba zapravo nikada nije rekla.

Jednostavni alati provjere

Kada vidiš nešto sumnjivo, koristi ove brze alate da otkriješ da li je u pitanju AI lažnjak ili prava stvar.



Pauza i ponovi reprodukciju

Zaustavi video i gledaj pažljivo detalje poput treptanja očiju ili pokreta usana. AI često pravi greške u sitnim pokretima.

#Pauziraj

#Detalji



Osnove reverse image search

Koristi Google Images da vidiš gdje se slika prvi put pojavila. Ako je nema nigdje drugdje, možda je generisana.

#PretragaSlika

#Izvor



Uporedi sa drugim postovima

Pogledaj druge objave iste osobe. Da li ovaj video izgleda drugačije? Da li glas zvuči čudno u poređenju sa ostalima?

#Uporedi

#Kontekst



Pitaj odraslu osobu

Ako nisi siguran/na da li je nešto stvarno, pokaži roditeljima ili nastavniku. Dvije glave su pametnije od jedne!

#Sigurnost

#Razgovor



AI Savjet: AI tehnologija napreduje, ali tvoje kritičko oko je i dalje najbolji alat za otkrivanje istine!

Podijeli Odmah vs Provjeri Prvo

Koja je tvoja reakcija na vijesti i slike online?



Podijeli Odmah

Reaguješ bez razmišljanja



Širiš štetu i laži



Žaljenje kasnije

POSLJEDICE

- ✗ Drugi ti manje vjeruju.
- ✗ Prijatelji se mogu uplašiti.
- ✗ Teško je povući laž nazad.

VS

Provjeri Prvo

Pauziraš i razmišljaš



Sigurnije za sve



Pomažeš prijateljima

PREDNOSTI

- ✓ Postaješ pouzdan izvor.
- ✓ Štitиш druge od prevara.
- ✓ Osjećaš se ponosno i pametno.



Savjet: Kad vidiš nešto šokantno, zamisli crveno svjetlo na semaforu – STANI!

Priča: "Lažni glas trenera"

Kada AI klonira glas poznate osobe da bi nas prevario u hitnoj situaciji.



Hitna poruka

Poznat glas



Glasovna poruka

Marko je dobio glasovnu poruku na WhatsApp-u. Zvučalo je **identično** kao njegov trener: "Hitno mi pošalji kod za pristup nalogu tima!"

"*Marko, brzo, nemamo vremena!*"



Čudan osjećaj

Zastani i razmisli

Crvene zastavice

Marku je bilo sumnjivo. Trener nikada ne traži takve stvari preko poruka. I zašto je tolika panika?

- Prevelik pritisak vremena
- Neuobičajen zahtjev
- Poziv sa nepoznatog broja (ili skriveno)



Poziv uživo

Otkrivanje istine



Siguran potez

Umjesto da pošalje kod, Marko je nazvao trenera na njegov **pravi broj**. Trener se javio i rekao da mu ništa nije slao!



Rezultat: Spriječena prevara. To je bio AI Voice Cloning.



Ako nisi siguran/na...

Ako ti nešto izgleda čudno, previše savršeno ili sumnjivo, prati ova 4 sigurnosna koraka:



Ne dijeli

Zaustavi se. Ako je lažno, dijeljenjem samo pomažeš da se prevara širi.



Sačuvaj link

Kopiraj adresu ili napravi screenshot da možeš kasnije pokazati nekome.



Pitaj odraslu osobu

Pokaži roditelju ili nastavniku. Oni ti mogu pomoći da provjeriš izvor.



Prijavi sumnjivo

Koristi opciju "Report" ili "Prijavi" na aplikaciji da upozoriš moderatora.

 influencer_max
Sponsored

...



1/1



12,459 likes

influencer_max Upravo sam sreо ovu nevjerovatnu osobu u centru grada! 🌟 #nofilter #real #meetup



DETETKIVSKI ZADATAK

Ova slika izgleda savršeno, možda *previše* savršeno. Radite u grupi i pronađite **2 ključna dokaza** (crvene zastavice) koji otkrivaju da je ovo AI generisano. Imate 3 minute!



Ruke i Prsti

Da li ima previše prstiju ili izgledaju kao da se tope?



Oči i Pogled

Da li su zjenice savršeno okrugle? Da li je odsjaj isti?



Tekstura Kože

Da li je lice previše glatko, "plastično" i bez pora?



Pozadina

Da li su objekti iza mutni, nelogični ili iskrivljeni?



AI PRO SAVJET

AI često griješi na detaljima: pogledajte nakit, zube, tekst na majici ili objekte u pozadini.

Šta bi ti uradio/la?

Podijeli svoje ideje o sigurnim reakcijama na sumnjivi AI sadržaj



Koga bi pitao/la?

Kada vidiš nešto sumnjivo ili te nešto uplaši na internetu, kome se prvo obraćaš za savjet?
Roditeljima, nastavniku ili nekome trećem?



Šta ti pomaže da pauziraš?

Šta te može podsjetiti da staneš i razmisliš prije nego što nešto podijeliš? Koja je tvoja "kočnica" u glavi?



Kako pomoći prijatelju?

Ako vidiš da prijatelj dijeli lažnu sliku ili video, šta bi mu rekao/la da ga upozoriš, a da ga ne uvrijediš?

Tvoj AI Sigurnosni Štit



4 jednostavna koraka za zaštitu od lažnog sadržaja.



1. Pauziraj

Kad vidiš nešto šokantno ili previše savršeno, stani. Ne reaguj odmah.



2. Provjeri

Potraži crvene zastavice: čudne oči, glas bez emocija, nepoznat izvor.



Ne Dijeli



3. Pitaj

Nisi siguran/na? Pokaži roditeljima, nastavniku ili drugoj odrasloj osobi.



Provjeri



PAUZIRAJ!



4. Ne Širi

Ako sumnjaš da je lažno, nemoj dijeliti. Prekini lanac dezinformacija.

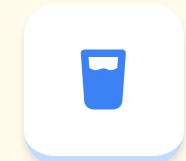


Kratki Odmor

Pauza za prvu grupu – Napuni baterije!

5

MINUTA



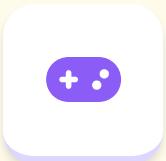
Hidratacija

Popij čašu vode



Istezanje

Protegni noge



Priprema

Spremi se za kviz



Slijedi: Quizizz kviz o lažnim vijestima!

PROVJERA ZNANJA DIO A

Quizizz Kviz

Pokaži šta znaš o AI osnovama, crvenim zastavicama i deepfake-ovima!

1

Prepremi uređaj

Uzmi svoj telefon ili tablet

2

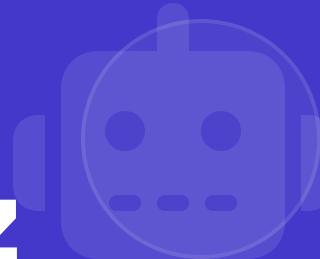
Otvori quizizz.com/join

Ili jednostavno skeniraj QR kod

3

Unesi kod i ime

Tvoja tajna šifra za ulaz u igru!



Skeniraj Kod

Otvori kameru na telefonu



GAME CODE

Unesite ovaj kod na quizizz.com/join

Šta smo Naučili?



Refleksija o AI tehnologiji i prepoznavanju lažnjaka



Nova Crvena Zastavica

Koja "crvena zastavica" (znak upozorenja) ti je bila potpuno nova danas? Da li su to čudne ruke, trepćenje ili nešto treće?



Večeras Probam...

Koji detektivski trik ćeš isprobati već večeras? Da li ćeš pauzirati video da nadeš greške ili provjeriti neki sumnjiv profil?



Širenje Znanja

Kome ćeš prvom ispričati o ovome što smo danas naučili? Kako možeš pomoći prijateljima da ne budu prevareni lažnim videima?



Znanje je najbolja odbrana od digitalnih prevara!

Tvoj AI Sigurnosni Štit



4 jednostavna koraka za zaštitu od lažnog sadržaja.

1. Pauziraj



Kad vidiš nešto šokantno ili previše savršeno, stani. Ne reaguj odmah na prvu loptu.

2. Provjeri



Potraži crvene zastavice: čudne oči, glas bez emocija, nepoznat izvor ili autor.

Odgovorno

3. Pitaj



Nisi siguran/na? Pokaži roditeljima, nastavniku ili drugoj odrasloj osobi od povjerenja.

Provjeri

4. Podijeli Odgovorno



Dijeli samo ono za što si 100% siguran/na. Budi filter, a ne pojačalo lažnih vijesti.

PAUZIRAJ!



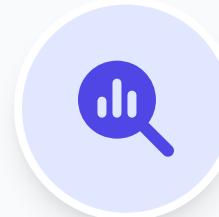
DRUGA GRUPA (12-15 GOD)

DIO B:

Detektuj i brani se



Fokus: napredne tehnike detekcije, AI alati, etika i odgovornost 🧠⚖️



Napredna Detekcija



AI Alati



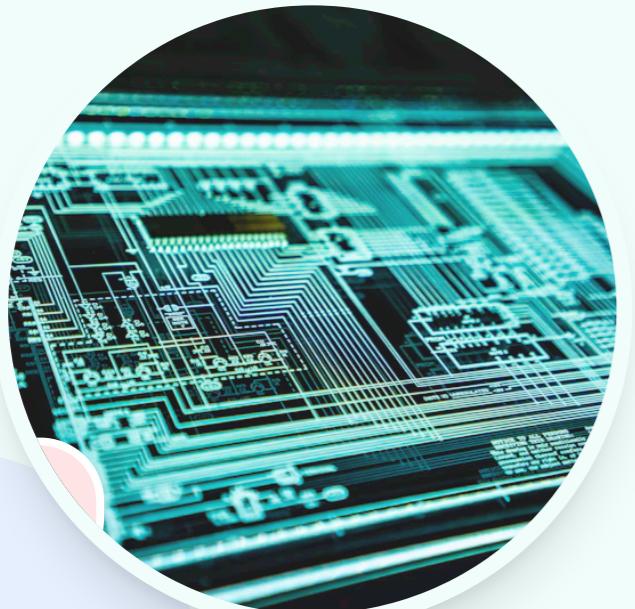
Etika



Detektuj i brani se



Napredne tehnike: Misliti kao istraživač u eri AI-a.



Misliti kao istraživač

Ne prihvataj informacije zdravo za gotovo. Uvijek traži izvor i kontekst.



Brze provjere

Nauči prepoznati deepfake markere u nekoliko sekundi.



Pravi alati

Koristimo napredne alate za verifikaciju videoa i zvuka.



Mirne odluke

Snažne emocije su često znak manipulacije. Ostani smiren/a.



AI Rizici:

Pregled Prijetnji

Zloupotreba generativne AI tehnologije stvara nove oblike digitalnih prijetnji.

Prepoznajte četiri glavna rizika:



Impersonacija

Krađa identiteta i "voice cloning" za prevare porodice ili zaposlenih.



Reputaciona Šteta

Kreiranje lažnog, kompromitujućeg sadržaja koji uništava ugled.



Dezinformacije

Masovno generisanje lažnih vijesti za manipulaciju izborima.

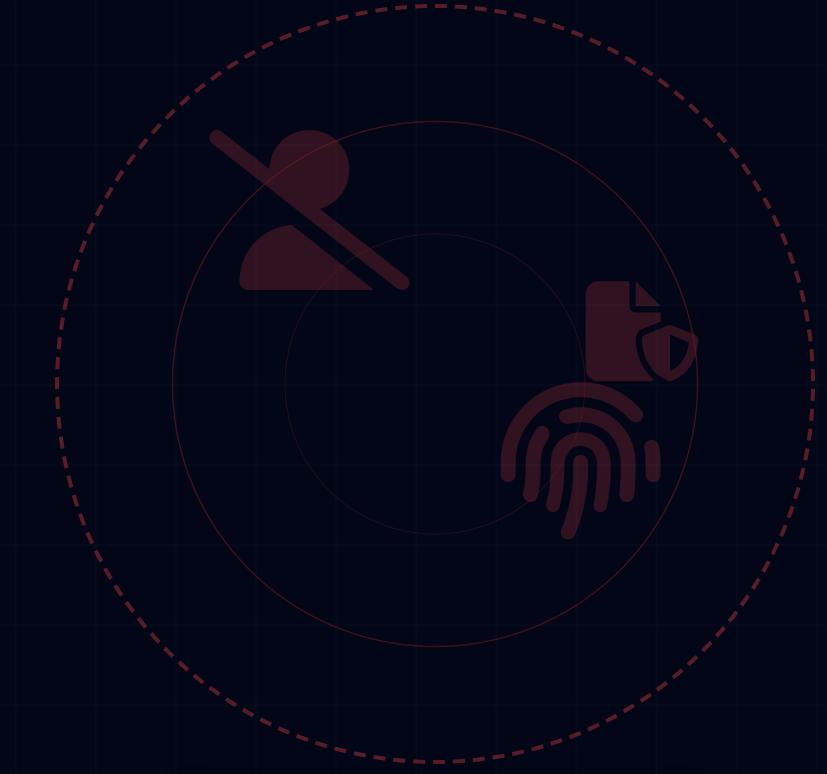


Pokušaji Ucjene

Sextortion i prijetnje objavom generisanog materijala.

PREVENCIJA

"Uvijek provjeri putem drugog kanala prije nego što reaguješ na hitan zahtjev."



SYSTEM ALERT

HIGH RISK DETECTED

AI Manipulation Probability: 98.4%

AI LAŽNJACI I DEEPFAKE ERA

Najnovije vijesti o regulaciji vještačke inteligencije, velikim deepfake incidentima i odgovoru obrazovnog sistema.

TRANSPARENTNOST

PLATFORME AUTOMATSKI OZNAČAVAJU SAV AI SADRŽAJ

Novi globalni standard obavezuje društvene mreže da koriste "Content Credentials" tehnologiju koja detektuje i vidljivo označava slike i videe generisane vještačkom inteligencijom.

DIGITAL STANDARDS AUTHORITY

OBRAZOVANJE

ŠKOLE UVODE OBAVEZAN PREDMET "AI PISMENOST"

Prepoznavanje deepfake-a, etika korištenja AI alata i zaštita biometrijskih podataka postaju dio redovnog nastavnog plana i programa za učenike starije od 10 godina.

EDUCATION WEEKLY

Global Update

INCIDENT

Breaking News

DEEPFAKE DIREKTORA IZAZVAO HAOS NA BERZI

Lažni video snimak u kojem CEO velike tehnološke kompanije najavljuje povlačenje proizvoda obrasio je milijarde dolara vrijednosti za samo 15 minuta prije nego što je prevara otkrivena.

FINANCIAL TIMES ALERT

ZAŠTITA

Sigurnost

ZABRANA NEOVLAŠTENOG KLONIRANJA GLASA

Novi zakon tretira neovlašteno AI kloniranje tuđeg glasa kao krađu identiteta. Razvijeni novi alati koji blokiraju pokušaje snimanja glasa tokom telefonskih poziva.

CYBER LAW UPDATE

Trendovi AI Dezinformacija



Ključni podaci o tome kako se AI tehnologija mijenja i utiče na nas u 2026.

Voice-Clone Prevare Rastu



Kloniranje glasa se sve više koristi za "vishing" napade. Prevaranti imitiraju glasove prijatelja ili porodice u lažnim hitnim situacijama.

Više AI Oznaka



Platforme uvode obavezne oznake za AI sadržaj. Korisnici sada češće viđaju "AI-Generated" bedževe na videima i slikama.

Tinejdžerska Konfuzija



Istraživanja pokazuju da mladi sve teže razlikuju satiru od pravih vijesti zbog hiper-realističnih deepfake sadržaja.

Deepfake Vizuelni Markeri

AI često pravi greške u detaljima. Nauči da prepoznaš ove "glitch" znakove koji otkrivaju lažni video.

Zubi i Oči



Ivice zuba su često mutne ili stopljene. Trepćenje može biti neprirodno rijetko, prebrzo ili ga uopšte nema.

Kosa i Uši



Pramenovi kose izgledaju zamrljano ili kao naljepnica. Uši mogu imati čudan oblik ili nedostajati detalji.

Osvjetljenje i Sjenke



Sjenke na licu ne odgovaraju smjeru svjetla u pozadini. Odsjaj u očima može nedostajati ili biti pogrešan.

Ruke i Prsti



Ruke često izgledaju gumenasto, kao rukavice. Prsti mogu biti stopljeni, predugi ili ih ima previše.

✓ ORIGINAL SOURCE

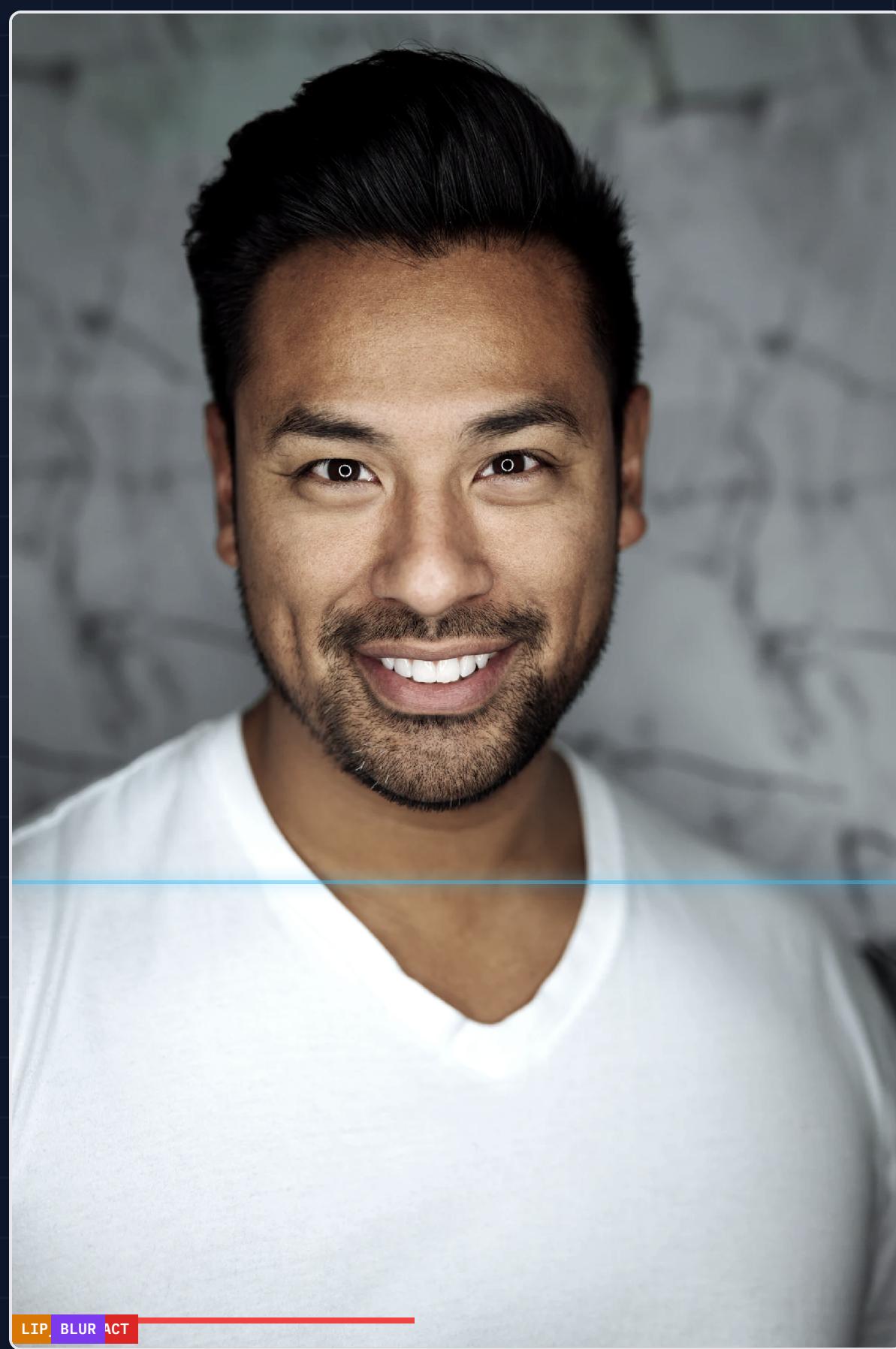
CONFIDENCE: 99.8%

! AI GENERATED / DEEPFAKE

DETECTED

CAM_A [RAW]

Natural Eye Micro-movements



LIGHTING CONSISTENCY

BLINK RATE

18 / min (Normal)

REAL-TIME ANALYSIS LOG

- > DETECTED: Irregular blinking pattern [Frame 2044]
- > WARNING: Audio/Video sync mismatch detected

Alati za detekciju i označavanje

Napredne tehnologije koje ti pomažu da identifikuješ sintetički sadržaj i provjeriš porijeklo informacija.



Platformske Oznake

Društvene mreže (TikTok, IG, YouTube) sada automatski označavaju sadržaj kreiran AI alatima. Potraži "AI generated" tag ispod videa.

#AILabel

#Transparency



Content Credentials (C2PA)

Digitalni "nutritivni sastav" fotografije. Klikom na "i" ikonu otkrivaš historiju izmjena i da li je korištena vještačka inteligencija.

#MetaData

#Porijeklo



Third-party Detektori

Alati poput "Hive Moderation" ili "Deepware" skeniraju video zapise tražeći anomalije u pikselima koje su nevidljive ljudskom oku.

#Deepware

#Analiza



Browser Ekstenzije

Dodaci poput InVID plugin-a pomažu da brzo analiziraš metapodatke videa i izvršiš obrnutu pretragu slika direktno iz preglednika.

#InVID

#Plugin



Pro Tip: Detektori daju vjerovatnoću, a ne apsolutnu istinu. Uvijek kombinuj alate sa vlastitim kritičkim razmišljanjem.

Kako radi voice-clone prevara?

4 koraka AI audio manipulacije



ANATOMIJA NAPADA:



1. Uzorak

Prevaranti pronalaze audio snimke vašeg glasa na društvenim mrežama (TikTok, IG story) ili govornoj pošti.

Prikupljanje



2. Kloniranje

AI softver analizira ton, naglasak i pauze, te kreira digitalnu kopiju koja može reći bilo šta.

Procesiranje



3. Hitan Poziv

Primate poziv od "člana porodice" koji zvuči uspaničeno. Pozadina je često bučna da prikrije greške.

Napad



4. Novac

Traže hitan transfer novca, kriptovalute ili gift kartice "da riješe problem" (zatvor, bolnica).

cilj

AI ČINJENICA

Za uvjerljivo kloniranje glasa ponekad je dovoljno samo **3 sekunde** audio snimka.



AUTHENTIC RECORDING

HUMAN SPEECH PATTERN DETECTED

98%

NATURAL SCORE

TURAL BREATH

SPECTROGRAM // 0Hz - 20kHz

 Consistent Background Noise

Human • AI Generated • Audio Artifact

SYNTHETIC / CLONED

AI GENERATED PATTERNS DETECTED

ROBOTIC MONOTONE

UNNATURAL SILENCE

99%

AI PROBABILITY

SPECTROGRAM // ARTIFACT DETECTION

METALLIC ARTIFACTS

Missing Background Noise

SYSTEM STATUS: ONLINE // ANALYZING STREAM...

AI Benefiti vs AI Rizici

Dvije strane medalje vještačke inteligencije



Benefiti

Kako nam AI pomaže

Pomoć i Asistencija

Kreativnost i Ideje

PREDNOSTI

- ✓ Brže rješavanje kompleksnih problema.
- ✓ Personalizovano učenje i dostupnost znanja.
- ✓ Automatizacija dosadnih zadataka.



Rizici

Tamna strana tehnologije

Prevara i Dezinformacije

Bias (Pristrasnost)

VS

OPASNOSTI

- ✗ Zloupotreba za deepfake i lažne vijesti.
- ✗ Diskriminacija zbog loših podataka (bias).
- ✗ Gubitak privatnosti i krađa identiteta.



Savjet: Koristi AI kao moćan alat, ali uvijek kritički provjeravaj rezultate!



AI_CONTENT_FILTER_SYS



Detektovan AI Sadržaj

Algoritam je 99.8% siguran da je ovaj video deepfake političara. Da li ga treba odmah obrisati?

Confidence Score

High Risk

BLOCK

ALLOW

? PITANJE ZA RASPRAVU

Treba li platforma (npr. TikTok, Instagram) **automatski blokirati i brisati** sav sadržaj koji AI detektori prepoznaju kao lažan, bez ljudske provjere?

OPCIJA A



ZA: Zaštita

Bolje sprječiti nego liječiti. Lažne vijesti se šire prebrzo. Ako čekamo ljudsku provjeru, šteta je već učinjena.

- ✓ Brza reakcija
- ✓ Manje prevara

OPCIJA B



PROTIV: Cenzura

Algoritmi često grijše. Mogu obrisati satiru, umjetnost ili dokaze o zločinima. Ko kontroliše istinu?

- ✗ Lažni pozitivi
- ✗ Gušenje govora



SIGURNIJI PRISTUP (NAJBOLJA PRAKSA)

Jasne Oznake (Label)

Frikcija (Uspori dijeljenje)

Pravo na Žalbu

Studija slučaja: Deepfake Političara

Analiza incidenta gdje je AI generisani video korišten za manipulaciju javnim mnjenjem i izazivanje panike.



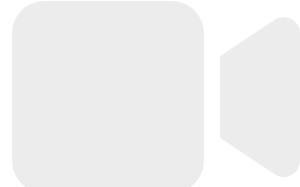
Viralni fake video

Šokantna izjava

TikTok & Twitter

Pojavio se video poznatog političara koji daje kontroverznu izjavu o ukidanju interneta. Video je izgledao hiperrealistično.

"Milion pregleda u samo 2 sata."



Korekcija izdata

Istina kasni

Emocionalna reakcija

PR tim je izdao demanti, ali bijesni komentari su već preplavili mreže. Ljudi su vjerovali videu jer je potvrđivao njihove strahove.

- Protesti online
- Širenje bez provjere
- Šteta reputaciji



Oznake i Pismenost

Sistem odbrane

Manipulated Media

Platforme su označile video kao "Manipulated Media". Novinari su koristili AI detektore da dokažu da je audio sintetizovan.



Pouka: Uvijek traži "Fact-Check" oznake na kontroverznim videima.



Provenance i Metadata

Kako provjeriti porijeklo digitalnog sadržaja i vidjeti šta se krije "ispod haube".



Content Credentials

Digitalni "pečat" koji pokazuje ko je i kada kreirao sadržaj, koristeći C2PA standard.



Istorija izmjena

Metadata podaci koji otkrivaju da li je slika editovana u Photoshopu ili generisana AI alatom.



Signalii izvornog uređaja

Informacije o modelu kamere, lokaciji i postavkama koje potvrđuju da je snimak autentičan.

Proces prijave i uklanjanja

4 koraka za efikasno prijavljivanje deepfake i štetnog sadržaja

TOK REAKCIJE:



ZLATNO PRAVILO

Prijavi, ali ne dijeli dalje – dijeljenje pomaže algoritmu da proširi lažnu vijest.



Detektuj i Reaguj



4 ključna koraka za borbu protiv naprednih deepfake prevara.

1. Prepoznaj Markere



Traži vizuelne greške: čudne ivice, neprirodno treptanje, "glatku" kožu ili artefakte.

2. Provjeri Audio



Slušaj pažljivo: robotizovan ton, neprirodne pauze ili neusklađenost s pozadinskom bukom.

Audio?

3. Koristi Alate



Traži "AI generated" oznake, koristi Content Credentials i alate za verifikaciju izvora.

Markeri?

4. Prijavi Sigurno



Ne dijeli sumnjiv sadržaj. Koristi opcije prijave (Report) da zaustaviš širenje.



Prijavi



Kratki Odmor

Pauza za drugu grupu – Odmori oči i mozak!

5

MINUTA



Disanje

Duboki udah i izdah



Hidratacija

Osvježi se vodom



Istezanje

Razgibaj vrat i ramena



Slijedi: Quizizz kviz o deepfake detekciji!

PROVJERA ZNANJA DIO B

Quizizz Kviz

Pokaži šta znaš o deepfake markerima, voice-clone prevarama, alatima i etici!

1

Prepreči kloniranje glasa

Uzmi svoj telefon ili tablet

2

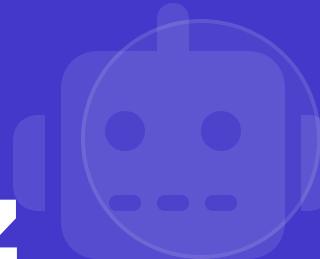
Otvori quizizz.com/join

Ili jednostavno skeniraj QR kod

3

Unesi kod i ime

Tvoja tajna šifra za ulaz u igru!



Skeniraj Kod

Otvori kameru na telefonu



GAME CODE

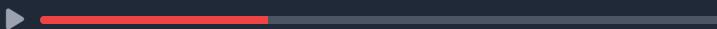
Unesite ovaj kod na quizizz.com/join



INCOMING FEED_

 **Portal_Vijesti_24** 1m ago
"ŠOKANTNO: EU zabranjuje sve video igre za mlađe od 18 godina! Klikni ovdje za listu zabranjenih igara..."
bit.ly/sokantno-igre

 **Celeb_Fan_Page** 15m ago
Ne mogu da vjerujem da je ovo obukao na dodjeli nagrada! 🤯 #fail
[Attachment: celeb_fail.jpg]

 **+387 61 ??? ???** Now
Audio poruka (0:14)
▶ 
"Hitno mi treba kod koji si dobio..."



ZADATAK TIMA

Pred vama su 3 sumnjiva posta. Brzo analizirajte sadržaj u grupi. Za svaki post odredite Nivo Rizika i Sljedeći Korak.

IZVOR

NIVO RIZIKA

AKCIJA

Post 1: Vijesti

NISKO

SREDNJE

PROVJERI

Post 2: Foto

NISKO

VISOKO

ZOOM

Post 3: Audio

NISKO

SREDNJE

BLOKIRAJ

STRATEGIJA ZA GRUPE

1. **Identifikuj** izvor (poznat ili ne?).
2. **Analiziraj** sadržaj (emocionalni okidači?).
3. **Odluči** (klik, provjera ili ignore?).

Wrap-up: Tvoj Sljedeći Korak 🚀

Refleksija na naučeno o AI tehnologiji i plan za digitalnu odbranu



Najkorisnija Tehnika?

Od vizuelnih markera (zubi, ruke) do audio analize – koja metoda ti se čini najmoćnijom za otkrivanje deepfake sadržaja?



Podrška Vršnjacima

Kako možeš pomoći vršnjacima da prepoznaju AI lažnjake i prevare, a da im pristupiš na prijateljski način?



Šta ćeš prvo primjeniti?

Koju konkretnu naviku ili alat ćeš početi koristiti već danas kada otvoriš društvene mreže?



Kritičko razmišljanje je tvoj najjači alat protiv deepfake-a!

 AKCIONI PLAN

TVOJ PLAN VERIFIKACIJE

Kada naideš na sumnjiv sadržaj, ne reaguj impulsivno. Aktiviraj ovaj sigurnosni protokol u 4 koraka.



PAUZIRAJ

Ne vjeruj odmah. Emocije su često okidač za prevaru. Stani, udahni i uspori prije nego klikneš.

1



IZVOR

Ko je ovo kreirao? Da li je profil verifikovan? Provjeri datum nastanka profila i prethodne objave.

2



CROSS-CHECK

Traži potvrdu. Koristi Google, Snopes ili druge fact-checking sajtove. Da li drugi izvori to potvrđuju?

3



PRIJAVI

Ako je lažno ili štetno, ne dijeli dalje. Prijavi sadržaj platformi i upozori prijatelje.

4



Postani bedem istine na internetu!

TRENDovi i BUDUĆNOST AI TEHNOLOGIJE

TRANSPARENTNOST

SVAKI PIKSEL IMA POTPIS: OBAVEZNE 'C2PA' OZNAKE

U 2026. godini, "Content Credentials" postaju standard. Svaka slika generisana AI alatima nosi neizbrisiv digitalni potpis porijekla (provenance), vidljiv na svim većim platformama.

DIGITAL TRUST ALLIANCE

Novi Standardi

UPOZORENJE

PREVARE EVOLUIRAJU: GLASOVNE PORUKE SU NOVA META

Dok se vizuelni deepfake lakše otkriva, audio prevare postaju sofisticirane. Napadači sve češće koriste klonirane glasove u privatnim porukama (WhatsApp, Viber) za brze prevare.

CYBER SECURITY WATCH

TEHNOLOGIJA

AI vs AI

DETEKTORI POSTAJU PAMETNIJI I BRŽI

Nova generacija odbrambenih algoritama sada prepoznaće deepfake video u realnom vremenu sa visokom tačnošću, integrisana direktno u vaše browser-e i aplikacije za kameru.

TECH RADAR DAILY

BUDNOST

Ljudski Faktor

OSTANI BUDAN/NA: TVOJ UM JE NAJBOLJI FILTER

Stručnjaci su saglasni: Nijedan softverski alat nije savršen. Vaša sposobnost kritičkog razmišljanja, provjere izvora i smirene reakcije ostaje najvažnija linija odbrane.

EDUCATION FUTURE



Resursi i Podrška

Verifikacija sadržaja, sigurnosne postavke platformi i kanali za hitnu pomoć.



Verifikacija i Alati

Content Credentials (C2PA)

Otvoreni standard koji ti omogućava da vidiš porijeklo i istoriju izmjena digitalnog sadržaja.

AI Detector Tools

Alati poput Hive Moderation ili Deepware za analizu sumnjivih videa i audio zapisa.

contentcredentials.org



Sigurnost na Platformama

Meta Safety Center

Alati za upravljanje privatnošću i prijavu lažnih profila na Instagramu i Facebooku.

TikTok Safety Center

Vodiči za prepoznavanje prevara i upravljanje digitalnim blagostanjem.

Google Safety

Upravljanje podacima i sigurnosne provjere za Google nalog.

safety.google



Pomoć i Podrška

Scam Helpline

Linija za hitnu pomoć i savjete u slučaju online prevare ili krađe identiteta.

Nacionalni CERT

Prijava incidenata računarske sigurnosti i edukativni resursi.

StopNasilju.net

Anonimna prijava digitalnog nasilja i podrška za mlade.

[192 / CERT](https://192.cert)



Vodič za Predavača: AI i Deepfake Tehnologija



Ključne napomene za Temu 9: Detekcija, Etika i Sigurnost

Ukupno trajanje: 120 min (2 x 60 min)



Jezik i Ton

- ✓ **Ijekavica:** "vještačka inteligencija", "činjenica", "provjera", "sigurnost".
- ✓ **Inkluzivnost:** Koristi rodno neutralne termine (istraživač/ica, učenik/ca).
- ⚠ **Sigurnost (Bez stida):** Naglasi da AI može prevariti svakoga. Nema krivice ako nasjedneš.



Struktura Radionice

DIO A (Mlađi 9-11)

Prvih 60 min

- **Uvod (5')**: Šta je AI? Analogija lutke.
- **Teorija (25')**: Prepoznavanje osnovnih lažnjaka.
- **Pauza (5')**: Odmor.
- **Kviz (25')**: Quizizz + Mini izazov "Nađi grešku".
- **Kraj (5')**: Rekapitulacija i sigurni koraci.

DIO B (Stariji 12-15)

Drugih 60 min

- **Uvod (5')**: Deepfake rizici & Voice Cloning.
- **Teorija (25')**: Napredna detekcija, Metadata, Alati.
- **Pauza (5')**: Odmor.
- **Kviz (25')**: Quizizz + Detection Sprint (Grupni rad).
- **Kraj (5')**: Diskusija i plan verifikacije.



Ključni Koncepti

- ⚠ **"Pauza i Provjera" (Dio A):** Djeca trebaju naučiti da ne reaguju na prvu emociju. AI cilja na "wow" efekat.
- ⚠ **Detektivski rad (Dio B):** Fokus na detalje - zubi, oči, trepćenje, pozadinska buka (audio).

Etika AI-ja: Nije sav AI loš. Fokus je na odgovornoj upotrebi i zaštiti od zloupotrebe.



Priprema i Materijali

- Quizizz:** Kodovi spremni za Dio A i Dio B.
- Sample Media:** Pripremi 1 dobar deepfake video i 1 audio klon primjer.
- Prompti:** Pitanja za diskusiju o etici (slajd 36).



Interakcija & Podrška



Empatija: Ako je neko prevaren, to je lekcija, ne greška. Stvorи sigurnu atmosferу за dijeljenje iskustava.



Gamification: Koristi "Detection Sprint" da podigneš energiju. Neka se takmiče ko će naći više "glitcheva".



Diskusija: "Kako bi se osjećao/la da neko klonira tvoj glas?" (Podsticanje empatije).