



MODUL 2 – Digitalne vještine za upravljanje dezinformacijama

Partner: FORMA.Azione srl

Autori: Adina Curta, Sylvia Liuti



Co-funded by
the European Union



Summary

Uvod	03
Pregled alata	04
Provjera autentičnosti slika i videozapisa	07
Analiza internetskih stranica i domena	17
Analiza društvenih mreža i korisničkih računa	21

Uvod

Svakodnevno se zdravstveni savjeti dijele putem društvenih mreža, aplikacija za razmjenu poruka i internetskih stranica – na TikToku, Instagramu, YouTubeu, WhatsAppu te na brojnim blogovima i forumima. Dio tih sadržaja je točan i koristan, no velik dio nije. Problem je u tome što su obmanjujuće zdravstvene informacije često osmišljene tako da djeluju uvjerljivo, dok se vještine potrebne za njihovo prepoznavanje rijetko sustavno poučavaju.

Ovaj modul temelji se na pet nacionalnih istraživanja provedenih u partnerskim zemljama između lipnja i rujna 2025. godine. Rezultati pokazuju dosljednu i zabrinjavajuću sliku: sposobnost prepoznavanja zdravstvenih dezinformacija vrlo je niska u svih pet zemalja. Problem nije nedostatak motivacije niti nepovjerenje u institucije, već nedostatak praktičnih alata.

Najvažniji nalazi usporednog izvješća

- Italija: 64 % ispitanika navodi da su obmanjujući internetski sadržaji najveća prepreka pronalasku pouzdanih zdravstvenih informacija, dok 42 % nije sigurno jesu li ikada podijelili netočne zdravstvene informacije.
- Litva: 48 % ispitanika smatra da je nedostatak vještina za procjenu pouzdanosti informacija njihova najveća prepreka; iako su svjesni postojanja dezinformacija, samo otprilike jedna trećina redovito provjerava činjenice.
- Hrvatska: samo 5,6 % ispitanika uspjelo je ispravno prepoznati lažne zdravstvene informacije. Čak 80,4 % susrelo se na internetu s lažnim lijekovima ili „čudotvornim“ pripravcima.
- Bugarska: 83 % ispitanika susrelo se s dezinformacijama o „čudotvornim“ proizvodima. Najveće prepreke nisu složen jezik, nego nesigurnost i proturječne informacije.
- Cipar: 53,7 % ispitanika navodi da je velika količina obmanjujućih internetskih sadržaja glavna prepreka donošenju informiranih zdravstvenih odluka.

Ovaj modul izravno odgovara na taj problem. Polaznicima pruža konkretan i lako primjenjiv skup alata koje mogu odmah koristiti pri procjeni bilo koje zdravstvene tvrdnje na internetu. Modul obuhvaća tri područja:

- provjeru autentičnosti slika i videozapisa,
- analizu internetskih stranica i domena,
- procjenu vjerodostojnosti računa na društvenim mrežama.

Ishodi učenja

Nakon završetka ovog modula moći ćete:

- koristiti obrnuto pretraživanje slika na najmanje dvije platforme kako biste provjerili podrijetlo i autentičnost zdravstvenih fotografija i videozapisa;
- koristiti izdvajanje kadrova iz videozapisa i analizu metapodataka za prepoznavanje videozapisa koji su prikazani izvan izvornog konteksta;
- otkriti digitalne manipulacije slikama primjenom metode Error Level Analysis (ELA);
- analizirati URL kako biste utvrdili stvarnu domenu, prepoznali lažne domene koje oponašaju legitimne stranice te provjerili povijest registracije domene;
- primijeniti metodu lateralnog čitanja za procjenu vjerodostojnosti bilo koje zdravstvene internetske stranice u manje od 60 sekundi;
- prepoznati strukturne i ponašajne pokazatelje nevjerodostojnih zdravstvenih računa na Instagramu, TikToku i YouTubeu;
- redovito primjenjivati ove alate pri susretu sa zdravstvenim sadržajima na internetu.

Pregled alata

Ovaj modul obuhvaća devet alata i metoda, podijeljenih u tri kategorije. Svaki alat predstavljen je u zasebnom poglavlju koje sadrži upute korak po korak, uvodne primjere, praktične vježbe i ključne napomene. Tablice u nastavku pružaju kratak pregled svakog alata prije njegove detaljne obrade.

3.1. Provjera autentičnosti slika i videozapisa (Image and Video Verification)

Zdravstvene dezinformacije često koriste stvarne fotografije i videozapise izvan njihova izvornog konteksta ili medijske sadržaje koji su digitalno izmijenjeni. Alati predstavljeni u ovom poglavlju omogućuju vam da pratite podrijetlo bilo koje slike ili videozapisa, provjerite njihov izvor te otkrijete moguće digitalne manipulacije.

Alat	Što radi	Najkorisniji za
Google Images / Lens	Obrnuto pretraživanje slika – pronalazi sva mjesta na internetu na kojima se određena slika pojavila i kada.	Provjeru fotografija zdravstvenih proizvoda, fotografija „prije i poslije” te navodnih dokaznih fotografija.
TinEye	Obrnuto pretraživanje slika s mogućnošću sortiranja rezultata od najstarijih prema novijima; prikazuje pravo podrijetlo slike.	Utvrđivanje kada i gdje se neka viralna zdravstvena fotografija prvi put pojavi
InVID / WeVerify	Proširenje za preglednik koje razdvaja video na pojedinačne kadrove radi obrnutog pretraživanja te očitava metapodatke videozapisa.	Provjeru videozapisa sa zdravstvenim savjetima na TikTok, Instagramu i YouTubeu.
FotoForensics	Primjenjuje Error Level Analysis (ELA) za otkrivanje digitalnih manipulacija u slikama.	Otkrivanje izmijenjenih snimki zaslona medicinskih nalaza ili promijenjenih statističkih podataka.

3.2 Analiza internetskih stranica i domena

Internetska stranica može izgledati potpuno profesionalno, a ipak biti izvor dezinformacija. Ove metode omogućuju procjenu vjerodostojnosti bilo koje zdravstvene internetske stranice u manje od 60 sekundi, bez potrebe da pročitate ijedan članak.

Alat	Što radi	Najkorisniji za
Analiza strukture URL-a	Pomaže prepoznati stvarnu domenu čitanjem URL-a s desna na lijevo te otkriva domene koje oponašaju legitimne stranice.	Provjeru svake zdravstvene internetske stranice prije nego što joj povjerujete.
WHOIS / who.is	Prikazuje kada je domena registrirana, tko je vlasnik i gdje je smještena.	Otkrivanje stranica koje se predstavljaju kao autoriteti, a registrirane su tek nedavno.
Lateralno čitanje	Umjesto čitanja sadržaja na samoj stranici, otvaraju se nove kartice preglednika kako bi se istražio izvor informacija.	Brzu procjenu vjerodostojnosti internetske stranice ili autora.

3.3 Analiza društvenih mreža i korisničkih računa

Nevjerodostojni korisnički računi i koordinirane mreže često se koriste kako bi zdravstvene dezinformacije izgledale popularnije i vjerodostojnije nego što jesu. Ovi alati pomažu procijeniti autentičnost računa na Instagramu, TikToku i YouTubeu.

Alat	Što radi	Najkorisniji za
Kontrolni popis ponašanja profila	Ručna procjena starosti računa, omjera pratitelja i praćenih računa, ujednačenosti objava, obrazaca komentiranja i rasta broja pratitelja.	Prepoznavanje botova i lažnih zdravstvenih influencera na Instagramu, TikToku i YouTubeu.
Social Blade	Prati rast broja pratitelja kroz vrijeme; nagli skokovi mogu upućivati na kupljene pratitelje.	Otkrivanje neprirodnog rasta računa koji promoviraju dodatke prehrani i wellness proizvode.

Provjera autentičnosti slika i videozapisa

Tekst u nastavku predstavlja četiri alata za provjeru autentičnosti i podrijetla zdravstvenih fotografija i videozapisa. Poglavlja 3.1.1 do 3.1.4 mogu se čitati redoslijedom kojim su prikazana ili se mogu koristiti zasebno kada je potrebno provjeriti određenu fotografiju ili videozapis.

3.1.1 Don't Trust the Image — Google Images / Lens

Što je obrnuto pretraživanje slika?

Obrnuto pretraživanje slika funkcionira suprotno od klasičnog pretraživanja. Umjesto da upisujete ključne riječi kako biste pronašli slike, učitavate sliku, a alat pronalazi sva mjesta na internetu na kojima se ta slika pojavila te vrijeme njezine objave.

Na taj način možete:

- pronaći izvorni izvor i datum objave bilo koje slike;
- utvrditi koristi li se slika u potpuno drugačijem kontekstu od izvornoga;
- prepoznati fotografije iz baza fotografija (stock photos) koje se predstavljaju kao autentični dokaz neke zdravstvene tvrdnje;
- otkriti slike koje su nastale ili kružile internetom mnogo prije tvrdnje koju navodno potvrđuju.

Kako koristiti Google Images / Google Lens – korak po korak



Otvorite internetsku stranicu ili objavu na društvenim mrežama koja sadrži sliku. Kliknite desnom tipkom miša na sliku i odaberite "Search image" ili "Search image with Google". Otvorit će se nova kartica s rezultatima koji prikazuju sva poznata pojavljivanja te slike. Obratite pozornost na: gdje se slika pojavljuje, datume njezinih objava, pojavljuje li se u bazama stock fotografija.



Otvorite images.google.com. Kliknite ikonu fotoaparata u traci za pretraživanje. Odaberite "Upload a file" ako ste spremili sliku ili zalijepite njezin izravni URL. Kliknite "Search by image" i analizirajte rezultate kao u Metodi A.



Na mobilnom pregledniku pritisnite i zadržite prst na slici te odaberite "Search image" ili "Search with Google Lens". Ako na TikToku ili Instagramu ta opcija nije dostupna napravite snimku zaslona (screenshot), otvorite images.google.com učitajte snimku zaslona koristeći Metodu B.

Tumačenje rezultata – na što obratiti pozornost

Što pronadete	Što to znači
Slika se nalazi na internetskoj stranici s fotografijama iz baze (stock photo website)	Slika je generička i ne predstavlja autentičan dokaz za konkretnu zdravstvenu tvrdnju. Ovo je ozbiljan znak upozorenja.
Ista se slika pojavljuje na desecima internetskih stranica unutar 24–48 sati.	Sadržaj se brzo proširio internetom prije nego što je provjeren. Velika popularnost ili viralnost nije dokaz da je informacija točna.
Slika je nastala mjesecima ili godinama prije zdravstvene tvrdnje koju navodno potvrđuje.	Slika se koristi izvan svojeg izvornog konteksta. Tvrdnja se temelji na ponovno iskorištenom ili preuzetom medijskom sadržaju.
Slika se pojavljuje samo u izvornoj objavi.	Rezultat nije dovoljan za zaključak. Nastavite provjeru pomoću alata TinEye i drugih dostupnih alata.
Slika se može povezati s vjerodostojnom novinskom organizacijom ili institucijom.	Moguće je da je autentična, ali svakako provjerite izvorni članak kako biste utvrdili puni kontekst u kojem je objavljena.

Isprobajte sami:

- Pronađite bilo koju fotografiju povezanu sa zdravljem iz objave na društvenim mrežama ili članka koji ste nedavno vidjeli.
- Pomoću Google Imagesa (Metoda A ili B) provedite obrnuto pretraživanje slike.
Zatim zapišite odgovore na sljedeća pitanja:
- Odakle slika izvorno potječe?
- Podudara li se izvor slike s onime što objava tvrdi?

Ključna napomena

- Obrnuto pretraživanje slike traje svega 45 sekundi. Neka vam postane navika provjeriti svaku fotografiju povezanu sa zdravljem prije nego što je podijelite.
- To što se neka slika brzo proširila internetom nije dokaz da je istinita. Ako se ista slika pojavila na 50 internetskih stranica u roku od 24 sata, potrebno ju je još pažljivije provjeriti, a ne automatski smatrati vjerodostojnom.
- Uvijek nastojte pronaći izvorni izvor i izvorni datum objave slike – nemojte procjenjivati njezinu vjerodostojnost samo prema tome koliko se često ili na koliko je mjesta objavljena

3.1.2 Pronalaženje izvornog podrijetla – TinEye

TinEye je specijaliziran za jednu značajku kojoj Google ne daje prednost: sortiranje rezultata prema datumu, od najstarijih prema najnovijima. Upravo zato predstavlja jedan od najpouzdanijih alata za odgovor na ključno pitanje vezano uz bilo koju zdravstvenu fotografiju:

„Kada se ova slika prvi put pojavila i za što je izvorno korištena?“

TinEye pretražuje vlastitu bazu slika koja je velika, ali nije potpuna. Ako za neku sliku ne pronađe rezultate, to ne znači da je slika autentična, već samo da nije uključena u TinEyeovu bazu. U tom slučaju potrebno je koristiti i Google Images te InVID (poglavlje 3.1.3).

Kako koristiti TinEye – korak po korak**1**

Otvorite tineye.com u svom internetskom pregledniku. Nije potrebno otvarati korisnički račun niti se prijavljivati.

2

Kliknite "Upload" i odaberite sliku sa svog uređaja, ili povucite sliku izravno na stranicu, ili zalijepite njezin izravni URL u traku za pretraživanje. Zatim kliknite na ikonu za pretraživanje.

3

Kada se prikazu rezultati, pronađite padajući izbornik "Sort by" u gornjem desnom dijelu stranice s rezultatima. Odaberite opciju "Oldest". Prvi rezultat predstavlja najranije poznato pojavljivanje te slike na internetu.

4

Otvorite najstariji rezultat. To je najvjerojatnije izvorno mjesto objave slike. Zapitajte se: o čemu je izvorno bila riječ? Tko je objavio sliku? Ima li ikakve veze sa zdravstvenom tvrdnjom uz koju se danas koristi?

5

Usporedite datum najstarijeg rezultata s datumom zdravstvene tvrdnje. Ako je slika nastala mjesecima ili godinama prije te tvrdnje, koristi se izvan izvornog konteksta, odnosno za stvaranje pogrešnog dojma.

Primjer iz stvarnog života

Političari i aktivisti također koriste stare fotografije kojima dodaju nove opise kako bi prikazali događaje koji se zapravo nisu dogodili na način kako tvrde. Ista se taktika koristi i u zdravstvenim dezinformacijama: fotografiji stvarne bolnice, stvarnog pacijenta ili stvarnog laboratorija dodaje se potpuno novi opis kako bi poduprla lažnu zdravstvenu tvrdnju. TinEye omogućuje otkrivanje takvih manipulacija prikazujući izvorni opis fotografije i njezin izvorni kontekst

Ključna napomena

- Rezultate u TinEyeu uvijek sortirajte prema opciji "Oldest" – upravo ta značajka čini TinEye učinkovitijim od Googlea za utvrđivanje izvornog podrijetla slike.
- Ako TinEye ne pronađe rezultate, to ne znači da je slika autentična. Uvijek koristite više različitih alata za provjeru.
- Najvažnije informacije koje trebate pronaći su izvorni opis slike i njezin izvorni kontekst

3.1.3 Provjera zdravstvenih videozapisa – InVID / WeVerify

Dezinformacije u videozapisima teže je provjeriti nego dezinformacije u slikama jer videozapis sadrži velik broj kadrova, od kojih se svaki može zasebno pretraživati kao slika. Za razliku od fotografije, na videozapis nije moguće jednostavno kliknuti desnom tipkom miša i pokrenuti obrnuto pretraživanje.

Alati InVID i WeVerify rješavaju taj problem tako što:

- razdvajaju videozapis na pojedinačne kadrove koje je moguće pojedinačno pretraživati obrnutim pretraživanjem slika;
- očitavaju ugrađene metapodatke videozapisa – skrivene informacije koje mogu otkriti izvorni datum snimanja, model uređaja kojim je video snimljen te ponekad i lokaciju;
- izdvajaju sličice (thumbnails) koje se mogu koristiti za pretraživanje na različitim platformama.

1

U pregledniku Chrome otvorite Chrome Web Store (chrome.google.com/webstore). U pregledniku Firefox otvorite Firefox Add-ons (addons.mozilla.org)

2

U tražilicu upišite "InVID WeVerify"..

3

Kliknite "Add to Chrome" ili "Add to Firefox". Proširenje će se instalirati za nekoliko sekundi, a njegova će se ikona pojaviti na alatnoj traci vašeg preglednika.

Kako koristiti InVID / WeVerify – korak po korak

1	Na TikTok, Instagramu, YouTubeu ili bilo kojoj drugoj platformi pronađite gumb "Podijeli" (Share) i kopirajte poveznicu na videozapis.
2	Kliknite na ikonu InVID/WeVerify na alatnoj traci preglednika. Otvorit će se sučelje alata.
3	Zalijepite URL videozapisa u alat. Odaberite opciju "Keyframes" ili "Video Analysis". Alat će izdvojiti niz pojedinačnih kadrova iz videozapisa u pravilnim vremenskim razmacima.
4	Kliknite desnom tipkom miša na bilo koji izdvojeni kadar i odaberite "Search image with Google" ili ga povucite u Google Images ili TinEye, na isti način kako je opisano u poglavljima 3.1.1 i 3.1.2. Pritom odgovorite na sljedeća pitanja: prikazuje li kadar zaista lokaciju koju videozapis tvrdi da prikazuje? Je li se ta snimka već ranije pojavila u nekom drugom kontekstu?
5	U alatu InVID otvorite karticu "Metadata". Ona prikazuje ugrađene metapodatke videozapisa, koji mogu sadržavati izvorni datum nastanka, GPS koordinate i uređaj kojim je videozapis snimljen. Ako metapodaci pokazuju da je videozapis nastao prije dvije godine, a objava tvrdi da je snimljen prošlog tjedna, utvrđeno je da se radi o sadržaju prikazanom izvan izvornog konteksta

Na što obratiti pozornost pri provjeri zdravstvenih videozapisa

Tvrđenje o lokaciji: provjerite prikazuje li pozadina doista ono što autor tvrdi. Osoba koja kaže da snima u bolnici može se zapravo nalaziti u bilo kojem hodniku. Obrnutim pretraživanjem kadra koji prikazuje pozadinu možete provjeriti je li se ta lokacija već pojavljivala u nekom drugom kontekstu.

- **Tvrdnje o identitetu:** ako osoba tvrdi da je liječnik, znanstvenik ili zdravstveni stručnjak, njezin identitet moguće je provjeriti. Izdvojite jasan kadar na kojem se vidi lice ili službena identifikacijska oznaka s imenom te upotrijebite obrnuto pretraživanje slike zajedno s metodom lateralnog čitanja (poglavlje 3.2.3) kako biste provjerili njezino ime i kvalifikacije koje navodi.
- **Tvrdnje o vremenu nastanka:** provjerite podudara li se datum u metapodacima s datumom objave. Također provjerite odgovara li okruženje vremenu za koje se tvrdi da je videozapis snimljen. Nepodudarnosti mogu ukazivati na to da je videozapis iskorišten izvan izvornog konteksta.

Ključna napomena

- InVID/WeVerify profesionalni je standard za provjeru videozapisa koji koriste novinari diljem svijeta. Preporučuje se da ga trajno instalirate u svoj internetski preglednik.
- Platforme mogu ukloniti ili izmijeniti metapodatke videozapisa, stoga nedostatak metapodataka nije dokaz autentičnosti.
- Provjera videozapisa kadar po kadar zahtijeva više vremena, ali omogućuje temeljitiju analizu. Posebnu pozornost obratite na kadrove koji prikazuju lokaciju, identitet osobe koja govori ili bilo kakav vidljiv tekst

3.1.4 Otkrivanje manipulacija slikama – FotoForensics

Što je Error Level Analysis (ELA)?

Svaka digitalna slikovna datoteka ima svoj kompresijski zapis (compression signature) koji nastaje prilikom spremanja slike. Kada se dio slike naknadno izmijeni – primjerice dodavanjem teksta, promjenom broja ili zamjenom lica – taj se izmijenjeni dio ponovno sprema s drugačijom razinom kompresije, dok ostatak slike zadržava izvornu kompresiju.

Error Level Analysis (ELA) prikazuje te razlike tako da razine kompresije pretvara u različite boje. Dijelovi slike koji su naknadno uređivani obično se prikazuju znatno svjetliji ili drugačije obojeni u odnosu na okolne, neizmijenjene dijelove slike

1	Otvorite internetsku stranicu fotoforensics.com u svom pregledniku. Nije potrebno otvarati korisnički račun niti se prijavljivati.
2	Kliknite "Upload" i odaberite sliku sa svog uređaja ili zalijepite njezin izravni URL u polje na vrhu stranice. Zatim kliknite "Upload".
3	Alat će prikazati izvornu sliku i njezinu ELA (Error Level Analysis) verziju jednu pokraj druge. Obratite pozornost na područja koja su znatno svjetlija ili drugačije obojena od ostatka slike.
4	Ako je svjetlina ujednačena na cijeloj slici, to upućuje na to da slika vjerojatno nije nedavno uređivana. Svijetle mrlje koje se pojavljuju samo na određenim dijelovima slike – osobito preko teksta, brojeva, lica ili statističkih podataka – mogu upućivati na to da je sadržaj naknadno izmijenjen.
5	Imajte na umu da svaka razlika u svjetlini ne znači nužno zlonamjernu manipulaciju. JPEG kompresija i snimke zaslona (screenshots) također mogu uzrokovati određene razlike. Posebnu pozornost obratite na svijetle dijelove koji se nalaze preko važnih informacija poput brojeva, imena, logotipa ili medicinskih podataka.

Najčešće primjene u otkrivanju zdravstvenih dezinformacija

Manipulirane statistike u snimkama zaslona medicinskih istraživanja

Prikaz stvarnog rezultata istraživanja može biti snimljen, a zatim naknadno izmijenjen promjenom ključnog broja. ELA analiza prikazat će izmijenjeni broj kao znatno svjetlije područje u odnosu na ostatak slike.

Izmijenjene deklaracije proizvoda ili podaci o nutritivnoj vrijednosti

Popisi sastojaka, upute za doziranje ili sigurnosna upozorenja mogu biti izmijenjeni kako bi se uklonile važne informacije o sigurnosti proizvoda. U ELA analizi izmijenjeni tekst obično se prikazuje svjetliji od izvornog teksta na deklaraciji.

Izmijenjene deklaracije proizvoda ili podaci o nutritivnoj vrijednosti.

IPopisi sastojaka, upute za doziranje ili sigurnosna upozorenja mogu biti izmijenjeni kako bi se uklonile važne informacije o sigurnosti proizvoda. U ELA analizi izmijenjeni tekst obično se prikazuje svjetliji od izvornog teksta na deklaraciji.

Izmišljeni citati koji se pripisuju zdravstvenim autoritetima. Autentična fotografija zdravstvenog djelatnika može biti naknadno uređena dodavanjem izmišljenog teksta u obliku opisa ili oblačića za govor. Dodani tekst ima drugačiji kompresijski profil od izvorne fotografije.



FotoForensics najbolje funkcioniра na slikama koje nisu bile višestruko komprimirane putem društvenih mreža. Kada se slika prenese na Instagram ili TikTok, a zatim ponovno preuzme, kompresija koju primjenjuje sama platforma može smanjiti učinkovitost ELA analize.

Za najbolje rezultate koristite izvornu slikovnu datoteku, ako je dostupna, ili verziju slike najviše moguće kvalitete.

ELA analiza sama po sebi predstavlja samo jedan alat za provjeru. Čak i uredan (čist) ELA rezultat ne jamči da slika nije bila manipulirana. ELA analizu uvijek kombinirajte s obrnutim pretraživanjem slike i analizom njezina konteksta.

Ključna napomena

- ELA nije dokaz manipulacije sama po sebi – ona predstavlja pokazatelj koji zahtijeva dodatnu interpretaciju.
- Pri ELA analizi usredotočite se na značajan sadržaj, poput brojeva, teksta, lica i logotipa, a ne na pozadinske dijelove slike.
- Za potpuniju procjenu vjerodostojnosti slike uvijek kombinirajte FotoForensics s drugim alatima za provjeru.

Analiza internetskih stranica i domena

Ovo poglavlje obuhvaća tri metode za procjenu vjerodostojnosti zdravstvenih internetskih stranica. Mogu se primjenjivati redom na bilo kojoj stranici u čiju vjerodostojnost niste sigurni ili se koristiti pojedinačno, ovisno o konkretnom pitanju koje želite provjeriti.

3.2.1 Čitajte URL kao detektiv – struktura URL-a, WHOIS i lateralno čitanje

Razumijevanje strukture URL-a

Svaka internetska adresa slijedi jasno definiranu strukturu. Za njezino pravilno čitanje potrebno je svega desetak sekundi, a ono može otkriti je li internetska stranica doista ono za što se predstavlja.

https://subdomain.realdomain.extension/path/page

subdomain (poddomena) – određuje je vlasnik stranice. Može biti bilo koja riječ, uključujući „nhs“, „who“ ili „government“.

realdomain (glavna domena) – stvarni naziv internetske stranice. Upravo je to dio na koji trebate obratiti najveću pozornost.

.extension (TLD – domena najviše razine) – ograničene domene poput .gov, .int i .edu upućuju na službene ili ovlaštene institucije. Otvorene domene poput .info, .biz i .net može registrirati bilo tko.

Zlatno pravilo: čitajte URL s desna na lijevo, počevši od prve kose crte (/)

Stvarna domena nalazi se neposredno prije prve kose crte (/).

Sve što se nalazi lijevo od nje predstavlja poddomenu, koju vlasnik stranice može nazvati kako god želi, uključujući i naziv poznate ili vjerodostojne organizacije.

- **who-healthalerts.net/vaccine-warning** → Stvarna domena je who-healthalerts.net (nije WHO).
- **health.nih-alerts.com/update** → Stvarna domena je nih-alerts.com (nije NIH).
- **who.int/news** → Stvarna domena je who.int ✓ Službena internetska stranica Svjetske zdravstvene organizacije (WHO).

Vrsta domene	Nastavci domena	Tko ih može registrirati
Ograničene domene	.gov .int .edu	Samo državna tijela, međunarodne organizacije i (uglavnom) obrazovne ustanove.
Provjerite dodatno	.org .nhs.uk .ac.uk	Nekada su bile ograničene, ali danas su otvorenije. Potrebno ih je dodatno provjeriti pomoću WHOIS-a.
Otvorene domene	.com .net .info .biz	Može ih registrirati bilo tko. Zdravstvena stranica koja koristi, primjerice, domenu .info, a pritom se predstavlja kao službeni autoritet, predstavlja znak upozorenja.

Kako koristiti WHOIS

WHOIS je javna baza podataka koja prikazuje:

- kada je domena registrirana,
- tko ju je registrirao,
- gdje se nalazi (na kojem je poslužitelju hostirana).

Ako internetska stranica tvrdi da je već 20 godina vodeći zdravstveni autoritet, a domena je registrirana prije samo tri mjeseca, očito nije ono za što se predstavlja.

1	Otvorite who.is u svom internetskom pregledniku.
2	U tražilicu upišite naziv domene (npr. naturalhealthtruth.com) i pritisnite Enter.
3	Pronađite polje "Created" ili "Registration Date" (datum registracije).
4	ogledajte polje "Registrant" ili "Organization". Ako su podaci o vlasniku skriveni iza usluge za zaštitu privatnosti, i to je važna informacija koju treba uzeti u obzir.
5	Usporedite datum registracije i podatke o vlasniku s autoritetom koji internetska stranica tvrdi da ima. Kombinacija: novoregistrirana domena, skriveni podaci o vlasniku, otvorena domena (.com, .info, .biz)

Lateralno čitanje: odmah napustite internetsku stranicu

Istraživanje Stanford History Education Groupa pokazalo je da su profesionalni provjeravatelji činjenica procjenjivali vjerodostojnost internetskih stranica brže i točnije od stručnjaka, zahvaljujući jednoj jednostavnoj navici: odmah bi napustili internetsku stranicu i provjerili što drugi izvori pišu o njoj. Ta se metoda naziva lateralno čitanje.

Postupak lateralnog čitanja – 30 sekundi

U tražilicu upišite:

[naziv internetske stranice] + "fact check" ILI [naziv internetske stranice] + "misinformation" ILI [naziv internetske stranice] + "review"

Nemojte čitati članke na samoj stranici. Umjesto toga, odmah otvorite novu karticu preglednika i potražite informacije o toj stranici iz drugih izvora. Ako ste otvorili zdravstvenu internetsku stranicu koju ne poznajete, upravo je to prvi korak koji biste trebali napraviti.

Ključna napomena

- Stvarna domena nalazi se neposredno prije prve kose crte (/).
- Nazivi poznatih organizacija u poddomeni predstavljaju jednu od najčešćih tehnika zavaravanja.
- Datum registracije domene u WHOIS-u jedan je od najbržih pokazatelja vjerodostojnosti internetske stranice.
- Lateralno čitanje brže je i pouzdanije od detaljnog čitanja same stranice kada procjenjujete vjerodostojnost izvora.
- HTTPS znači samo da je internetska veza šifrirana. To ne znači da je sadržaj internetske stranice pouzdan.



Ikona lokota uz HTTPS nije dokaz vjerodostojnosti. Ona samo označava sigurnu vezu. I internetske stranice koje šire dezinformacije redovito koriste HTTPS. Lokot ne govori ništa o točnosti sadržaja.

Analiza društvenih mreža i korisničkih računa

Ovo poglavlje predstavlja dva alata za procjenu vjerodostojnosti korisničkih računa na društvenim mrežama koji dijele zdravstvene informacije. Oba alata mogu se koristiti zajedno ili zasebno kako biste procijenili je li riječ o autentičnom računu ili računu koji umjetno stvara dojam vjerodostojnosti.

3.3.1 Kontrolni popis za procjenu korisničkih računa **Zašto su neautentični računi važni u području zdravlja**

Neautentični računi – botovi, kupljeni pratitelji i koordinirane mreže lažnih profila – koriste se u kampanjama zdravstvenih dezinformacija kako bi lažne zdravstvene tvrdnje izgledale popularnije i općeprihvaćenije nego što uistinu jesu.

Podaci prikupljeni u svih pet partnerskih zemalja pokazali su da je čak 83 % ispitanika bilo izloženo dezinformacijama o „čudotvornim proizvodima“. Mnoge od tih objava promovirane su upravo putem mreža neautentičnih korisničkih računa.

Isti obrazac prepoznat je u svih pet nacionalnih istraživanja kao jedan od glavnih pokretača rizičnih zdravstvenih ponašanja na internetu. Ako izgleda kao da svi preporučuju isti proizvod ili savjet, ljudi će ga lakše slijediti. Neautentični računi umjetno stvaraju upravo takav dojam društvene potvrde (social proof).

Kontrolni popis za procjenu autentičnosti korisničkog računa (6 koraka)

Primijenite ovih šest provjera na bilo koji račun koji na Instagramu, TikToku ili YouTubeu promovira zdravstvene tvrdnje. Ako uočite tri ili više znakova upozorenja, postoji snažan pokazatelj da račun nije autentičan.

1

Pronadite datum otvaranja računa (podatak se najčešće nalazi u odjeljku "About" ili "Account info".) Usporedite datum otvaranja s brojem pratitelja. Pravi zdravstveni edukator koji je tri godine gradio svoju publiku može imati, primjerice, 50.000 pratitelja. Račun sa 300.000 pratitelja nakon samo šest mjeseci zahtijeva dodatnu provjeru.

Znak upozorenja: vrlo velik broj pratitelja na vrlo novom računu.

2

Posjetite Social Blade i upišite korisničko ime računa Social Blade radi za YouTube, Instagram i TikTok.

Prirodan rast pratitelja izgleda kao postupan uzlazni trend. Kupljeni pratitelji često stvaraju nagli skok od nekoliko tisuća novih pratitelja u jednom danu.

Znak upozorenja: jedan izrazit dnevni skok od nekoliko tisuća pratitelja, nakon kojeg se rast ponovno usporava.

3

Pregledajte objave računa Autentični računi objavljuju raznolike sadržaje, koriste različite formate i obrađuju različite teme. Koordinirane mreže neautentičnih računa često objavljuju gotovo identične sadržaje – isti predložak, isti stil, isti raspored objava i gotovo nikakve varijacije.

Znak upozorenja: svaka objava koristi isti format, isti izgled i gotovo identičan tekst.

4

Pročitajte 10–15 komentara ispod najnovijih objava Na autentičnim računima komentari su raznoliki i konkretni. Na neautentičnim računima često se pojavljuju kratki, generički komentari koji se ponavljaju, primjerice: „Ovo mi je promijenilo život.“, „Tako je!“, „Nevjerojatan proizvod!“ bez ikakvih konkretnih detalja.

Znak upozorenja: većina komentara sastoji se od 3–5 općenitih riječi ili se ista rečenica doslovno ponavlja ispod više objava.

5
Velik autentičan račun obično prati relativno mali broj drugih računa .

Račun koji prati 12.000 osoba, a ima 14.000 pratitelja, može biti dio sustava međusobnog praćenja ("follow-for-follow"), što je česta praksa u promociji dodataka prehrani. Provjerite promoviraju li računi koje prati također zdravstvene proizvode.

Znak upozorenja: broj praćenih računa vrlo je blizu broju pratitelja ili ga čak premašuje.

6
Pretražite istu zdravstvenu tvrdnju ili korisničko ime na drugim platformama.

Koordinirane mreže često istovremeno objavljuju potpuno isti tekst i iste slike na Instagramu, Facebooku, TikToku i YouTubeu – riječ po riječ.

Znak upozorenja: potpuno isti tekst i iste slike istodobno se pojavljuju na više različitih platformi.

Kako koristiti Social Blade

- 1** Otvorite socialblade.com u svom internetskom pregledniku.
- 2** U tražilicu upišite korisničko ime s Instagrama, TikToka ili YouTubea te odaberite odgovarajuću platformu.
- 3** Glavni graf prikazuje dnevne promjene u broju pratitelja tijekom vremena. Postupan i ujednačen rast obično upućuje na prirodan razvoj računa. Velik okomiti skok u jednom danu može upućivati na kupljene pratitelje.
- 4** Ispod grafikona nalazi se tablica s točnim dnevnim promjenama broja pratitelja. Potražite dane s neuobičajeno velikim porastom. Ako je, primjerice, 20.000 novih pratitelja stiglo u jednom danu, a prije i poslije toga rast bio vrlo spor, postoji velika vjerojatnost da su ti pratitelji kupljeni.

Ključna napomena

- Nijedan pojedinačni znak upozorenja sam po sebi ne dokazuje da račun nije autentičan. Međutim, tri ili više znakova upozorenja zajedno snažan su pokazatelj neautentičnog ponašanja.
- Neautentični računi često pojačavaju (umjetno povećavaju) širenje dezinformacija koje su izvorno potekle iz stvarnog izvora – ne stvaraju ih nužno sami. Zato uvijek provjerite i izvornu tvrdnju koristeći alate za provjeru činjenica.
- Velik broj pratitelja ne znači ništa ako su pratitelji kupljeni. Social Blade može pomoći u prepoznavanju takvih obrazaca.