



MODULIS 2 – Skaitmeniniai įgūdžiai dezinformacijos valdymui

Partneris: FORMA.Azione srl

Autoriai: Adina Curta, Sylvia Liuti



Co-funded by
the European Union



Santrauka

Įvadas	03
.....	
Įrankių rinkinio apžvalga	04
.....	
Nuotraukų ir vaizdo įrašų tikrinimas	07
.....	
Svetainės ir domeno analizė	17
.....	
Socialinės medijos ir paskyrų analizė	21
.....	

Įvadas

Kiekvieną dieną socialiniuose tinkluose, žinučių programėlėse ir interneto svetainėse – „TikTok“, „Instagram“, „YouTube“, „WhatsApp“ bei daugybėje tinklaraščių ir forumų – plinta patarimai sveikatos klausimais. Kai kurie iš šių turinio elementų yra tikslūs ir naudingi. Dauguma jų – ne. Problema ta, kad klaidinanti informacija apie sveikatą dažnai pateikiama taip, kad atrodytų įtikinama, o įgūdžiai, reikalingi jai atpažinti, retai mokomi aiškiai. Šis modulis pagrįstas penkiais nacionaliniais tyrimais, atliktais partnerių šalyse nuo 2025 m. birželio iki rugsėjo. Tyrimų rezultatai atskleidžia nuoseklią ir skubią padėtį: visose penkiose šalyse gebėjimas atpažinti dezinformaciją sveikatos klausimais yra kritiškai žemas. Problema nėra motyvacija ar nepasitikėjimas valdžios institucijomis – problema yra praktinių įrankių trūkumas.

Svarbiausi lyginamosios ataskaitos duomenys:

- **Italija:** 64 % respondentų nurodo klaidinančią internetinę informaciją kaip pagrindinę kliūtį gauti patikimą informaciją apie sveikatą; 42 % nėra tikri, ar kada nors yra dalijęsi klaidinga informacija apie sveikatą.
- **Lietuva:** 48 % respondentų teigia, kad pagrindinė kliūtis yra įgūdžių, reikalingų patikimumui įvertinti, trūkumas; tik maždaug 1 iš 3 nuolat tikrina faktus, nepaisant to, kad žino apie dezinformaciją.
- **Kroatija:** tik 5,6 % respondentų galėjo teisingai klasifikuoti klaidingą informaciją apie sveikatą. 80,4 % buvo susidūrę su suklastotais vaistais ar stebuklingais vaistais internete.
- **Bulgarija:** 83 % respondentų susidūrė su dezinformacija apie stebuklingus produktus; pagrindinės kliūtys yra nekalbos sudėtingumas, o neapibrėžtumas ir prieštaringa informacija.
- **Kipras:** 53,7 % respondentų nurodo, kad pagrindinė kliūtis priimti pagrįstus sprendimus sveikatos klausimais yra gausus klaidinantis turinys internete.

Šis modulis tiesiogiai skirtas šiai spragai užpildyti. Jis suteikia besimokantiejiems konkretų, pakartotinai pritaikomą priemonių rinkinį, kurį jie gali iš karto pritaikyti bet kuriam internete sutiktam teiginiui apie sveikatą. Nagrinėjamos trys kategorijos: vaizdų ir vaizdo įrašų tikrinimas, svetainių ir domenų analizė bei socialinių tinklų paskyrų vertinimas.

Mokymosi tikslai

Baigę šį modulį, jūs sugebėsite:

1. ➤ Naudoti atvirkštinę vaizdų paiešką bent dviejose platformose, siekiant patikrinti su sveikata susijusių vaizdų ir vaizdo įrašų kilmę bei autentiškumą;
2. naudoti vaizdo kadro išskyrimą ir metaduomenų analizę, siekiant nustatyti klaidingą kontekstą turinčius teiginius sveikatos vaizdo įrašuose;
3. Aptikti skaitmeninį vaizdų failų klastojimą naudojant klaidų lygio analizę;
4. Analizuoti URL adresą, siekiant nustatyti tikrąjį domeną, aptikti panašias suklastotas svetaines ir patikrinti domeno registracijos istoriją;
5. Taikyti šoninį skaitymą, kad per mažiau nei 60 sekundžių įvertintumėte bet kurios sveikatos svetainės patikimumą;
6. Nustatykite struktūrinius ir elgsenos požymius, rodančius, kad „Instagram“, „TikTok“ ir „YouTube“ paskyros, susijusios su sveikata, yra netikros;
7. Naudokite šias priemones nuosekliai kaip įprotį, kai susiduriate su sveikatos turiniu internete.

Toolkit Overview

Šiame modulyje aptariami devyni įrankiai ir metodai, suskirstyti į tris kategorijas. Kiekvienas įrankis pristatomas atskirame skyriuje, kuriame pateikiamos išsamios instrukcijos, pavyzdžiai, praktiniai uždaviniai ir svarbiausi patarimai. Toliau pateiktose lentelėse pateikiama trumpa informacija apie kiekvieną įrankį, prieš pradedant jį išsamiai aptarti.

3.1 Nuotraukų ir vaizdo įrašų tikrinimas

Sveikatos dezinformacijoje dažnai naudojami tikri vaizdai ir vaizdo įrašai netinkamame kontekste arba skaitmeniniu būdu pakeisti vaizdai. Šios priemonės leidžia atsekti bet kokį vaizdą ar vaizdo įrašą iki jo pirminio šaltinio ir aptikti manipuliacijas.

Įrankis:	Ką daro?	Geriausiai tinka:
Google Images / Lens	Atvirkštinė vaizdų paieška: suranda visas vietas, kuriose vaizdas pasirodė internete, ir nustato, kada tai įvyko	Sveikatos produktų nuotraukų, prieš ir po nuotraukų, tariamų įrodymų nuotraukų tikrinimas
TinEye	Atvirkštinė vaizdų paieška, surūšiuota pagal senumo principą; parodo tikrąją bet kurio vaizdo kilmę	Išsiaiškinimas, kada ir kur pirmą kartą pasirodė populiari sveikatos tema susijusi nuotrauka
InVID / WeVerify	Naršyklės plėtinys: suskaido vaizdo įrašus į kadrus atvirkštinei paieškai; nuskaito vaizdo įrašo metaduomenis	Sveikatos patarimų vaizdo įrašų tikrinimas „TikTok“, „Instagram“ ir „YouTube“
FotoForensics	Klaidų lygio analizė (ELA) atskleidžia skaitmeninį manipuliavimą vaizdo failuose	Medicininės diagnostikos rezultatų ar statistikos duomenų klastojimo nustatymas

3.2 Svetainių ir duomenų analizė

Svetainė gali atrodyti visiškai profesionali, bet vis tiek būti dezinformacijos šaltiniu. Šie metodai leidžia įvertinti bet kurios sveikatos svetainės patikimumą per mažiau nei 60 sekundžių, neskaitant nė vieno straipsnio.

Įrankis:	Ką daro?	Geriausiai tinka:
URL structure reading	Tikrojo domeno nustatymas skaitant iš dešinės į kairę; panašių suklastotų domenų aptikimas	Bet kokiai sveikatos svetainės, prieš pasitikint jos turiniu
WHOIS / who.is	Rodo, kada domenas buvo užregistruotas, kam jis priklauso ir kur yra talpinamas	Svetainių, kurios teigia esą autoritetingos, bet buvo sukurtos praėjusį mėnesį, demaskavimas
Lateral reading	Atidaryti naujus langus, kad paieškotum informacijos apie šaltinį, o ne skaitytum jį	Greitas svetainės ar autoriaus patikimumo įvertinimas

3.3 Socialinių tinklų ir paskyrų analizė

Netikros paskyros ir koordinuoti tinklai naudojami tam, kad dezinformacija apie sveikatą atrodytų populiareesnė ir patikimesnė, nei yra iš tikrųjų. Šios priemonės padeda įvertinti autentiškumą „Instagram“, „TikTok“ ir „YouTube“.

Įrankis:	Ką daro?	Geriausiai tinka:
Profilio elgesio kontrolinis sąrašas	Rankinis vertinimas: paskyros amžius, sekėjų santykis, įrašų vienodumas, komentarų modeliai, sekėjų skaičiaus augimas	Botų paskyrų ir netikrų sveikatingumo įtakotojų identifikavimas „Instagram“, „TikTok“, „YouTube“
Social Blade	Stebi sekėjų skaičiaus augimo istoriją laikui bėgant; staigūs šuoliai rodo, kad sekėjai buvo nupirkti	Neteisėto augimo atskleidimas sveikatos papildų ir sveikatingumo paskyrose

Nuotraukų ir vaizdo įrašų tikrinimas

Toliau pateiktuose skyriuose aprašomi keturi įrankiai, skirti su sveikata susijusių vaizdų ir vaizdo įrašų autentiškumui ir kilmės vietai patikrinti. 3.1.1–3.1.4 langelius galima skaityti paeiliui arba atskirai, kai kyla konkreti patikrinimo užduotis.

3.1.1 Nepasitikėkite nuotrauka – Google Images / Lens

Kas yra atvirkštinė vaizdų paieška?

Atvirkštinė vaizdų paieška veikia priešinga kryptimi nei įprasta paieška. Vietoj to, kad įvestumėte žodžius norėdami rasti vaizdus, pateikiate vaizdą, o įrankis suranda visas vietas internete, kuriose jis pasirodė, ir nurodo, kada tai įvyko. Tai leidžia jums:

- surasti bet kurio vaizdo originalų šaltinį ir paskelbimo datą;
- sužinoti, ar vaizdas naudojamas visiškai kitame kontekste nei originalus;
- atpažinti nuotraukų banko nuotraukas, pateikiamas kaip autentiški sveikatos teiginių įrodymai;
- aptikti vaizdus, kurie buvo sukurti ar platinami gerokai anksčiau nei teiginys, kurį jie tariamai patvirtina.

Pradinis pavyzdys

„Mokslininkai atrado Amazonės žolę, kuri gydo diabetą – didžiosios farmacijos kompanijos nenori, kad jūs apie tai žinotumėte.“ Prie šio įrašo, kuris buvo pasidalintas 47 000 kartų, pridėta nuotrauka su ryškiai žalia augalu.

Paklauskite savęs: ar prieš dalindamiesi šiuo įrašu verta skirti 45 sekundes patikrinti, ar ta nuotrauka kada nors buvo padaryta Amazonėje?

Kaip naudoti „Google Images“ / „Lens“: žingsnis po žingsnio**Stalinio kompiuterio naršyklė (dešiniuoju pelės mygtuku)**

Atidarykite tinklalapį arba socialinės medijos įrašą, kuriame yra vaizdas. Dešiniuoju pelės mygtuku spustelėkite vaizdą ir pasirinkite „Ieškoti vaizdo“ arba „Ieškoti vaizdo su „Google““. Atsivers naujas langas su rezultatais, kuriuose bus rodomi visi žinomi to vaizdo pasirodymai. Pažiūrėkite, kur pasirodo vaizdas, kokios yra jo pasirodymo datos ir ar kuris nors šaltinis yra nuotraukų biblioteka.

Įkelkite arba įklijuokite URL (images.google.com)

Eikite į images.google.com. Spustelėkite fotoaparato piktogramą paieškos juostoje. Pasirinkite „Įkelti failą“, jei esate išsaugoję vaizdą, arba įklijuokite tiesioginį vaizdo URL. Spustelėkite „Ieškoti pagal vaizdą“ ir peržiūrėkite rezultatus kaip 1 metode.

Mobilusis telefonas (išmanusis telefonas)

Mobiliojoje naršyklėje ilgai spauskite (palaikykite) ant vaizdo ir pasirinkite „Ieškoti vaizdo“ arba „Ieškoti su „Google Lens““. „TikTok“ ar „Instagram“ programose, kuriose ilgai spausdami neatidarote meniu: padarykite vaizdo ekrano kopiją, tada eikite į images.google.com ir įkelkite ekrano kopiją naudodami B metodą.

Rezultatų skaitymas: ko ieškoti

Ką rasite?	Ką tai reiškia?
Vaizdas rastas nuotraukų banke	Vaizdas yra bendro pobūdžio, o ne autentiškas konkretaus teiginio įrodymas. Tai aiškus pavojaus signalas.
Tas pats vaizdas dešimtyse svetainių per 24–48 valandas	Turinys tapo populiarus dar prieš patikrinimą. Populiarumas nėra tiesos įrodymas.
Nuotrauka yra kelių mėnesių ar metų senumo	Nuotrauka naudojama netinkamame kontekste. Tvirtinimas pagrįstas pakartotinai panaudota arba pavogta medžiaga.
Vaizdas pasirodo tik originalioje žinutėje	Neįtikinama. Tęskite su „TinEye“ ir kitomis priemonėmis.
Nuotrauka susieta su patikima naujienų agentūra ar organizacija	Gali būti autentiškas. Patikrinkite originalų straipsnį, kad įsitikintumėte dėl viso konteksto.

Išbandykite dabar:

- Raskite bet kokią su sveikata susijusį vaizdą iš socialinių tinklų įrašo ar straipsnio, kurį matėte neseniai.
- Naudokite „Google Images“ (A arba B metodą), kad atliktumėte atvirkštinę paiešką.
- Užsirašykite: iš kur kilęs vaizdas? Ar šis šaltinis atitinka įrašė pateiktą informaciją?

Svarbus priminimas:

- Atvirkštinė vaizdo paieška trunka 45 sekundes. Pradėkite tai daryti prieš dalindamiesi bet koku su sveikata susijusiu vaizdu.
- Virusinis platinimas nėra tiesos įrodymas. Vaizdas, pasirodęs 50 svetainių per 24 valandas, reikalauja daugiau, o ne mažiau kruopštaus tikrinimo.
- Visada ieškokite originalaus šaltinio ir originalaus datos – ne tik to, ar vaizdas yra plačiai naudojamas.

3.1.2 Tikrosios kilmės paieška – „TinEye“

„TinEye“ specializuojasi vienoje funkcijoje, kuriai „Google“ neskiria pirmenybės: rezultatų rūšiavime pagal datą, pradedant seniausiais. Dėl to tai yra patikimiausias įrankis, padedantis atsakyti į pagrindinį klausimą apie bet kokį su sveikata susijusį vaizdą:

“Kada ši nuotrauka pasirodė pirmą kartą, ir kam ji iš pradžių buvo skirta?”

„TinEye“ atlieka paiešką savo pačios vaizdų indekse, kuris yra didelis, bet ne išsamus. Jei paieška pagal vaizdą neranda jokių rezultatų, tai nereiškia, kad vaizdas yra autentiškas – tai reiškia, kad „TinEye“ jo neįtraukė į indeksą. Tokiu atveju taip pat naudokitės „Google Images“ ir „InVID“ (3.1.3 skyrius).

Kaip naudoti „TinEye“: žingsnis po žingsnio**1**

Atidarykite tineye.com savo naršyklėje. Nereikia turėti paskyros ar prisijungti.

2

Spustelėkite „Įkelti“ ir pasirinkite vaizdo failą iš savo įrenginio, ARBA tiesiog perkelkite vaizdą tiesiai į puslapį, ARBA įklijuokite tiesioginį vaizdo URL adresą į paieškos juostą. Spustelėkite paieškos piktogramą.

3

Kai pasirodys rezultatai, raskite išskleidžiamąjį meniu „Rūšiuoti pagal“ rezultatų puslapio dešinėje viršutinėje dalyje. Pasirinkite „Senumo tvarka“. Pirmasis rezultatas dabar yra seniausias žinomas šio vaizdo pasirodymas internete.

4

Paspauskite ant seniausio rezultato. Tai greičiausiai yra vaizdo kilmės šaltinis. Apie ką jis iš pradžių buvo? Kas jį paskelbė? Ar jis turi kokį nors ryšį su dabar jį naudojančiu teiginiu apie naudą sveikatai?

5

Palyginkite seniausio rezultato datą su teiginio apie sveikatą data. Jei vaizdas yra keliais mėnesiais ar metais senesnis už teiginį, jis naudojamas klaidingame kontekste.

Realus pavyzdys:

Politikai ir aktyvistai taip pat perdirba senas nuotraukas, pridėdami naujus paaiškinimus, kad suklastotų įvykius. Sveikatos srities dezinformacijoje naudojama ta pati taktika: tikros ligoninės, tikro paciento ar tikros laboratorijos nuotraukai pridedamas visiškai naujas paaiškinimas, siekiant pagrįsti melagingą teiginį apie sveikatą. „TinEye“ atskleidžia šią manipuliaciją, parodydama originalų paaiškinimą ir kontekstą.

Išbandykite dabar:

1. Paimkite tą patį vaizdą, kurį ieškojote 3.1.1 skyriuje, arba raskite naują iš sveikatos srities įrašo.
2. Eikite į tineye.com ir įkelkite arba įklijuokite nuotraukos URL.
3. Rūšiuokite rezultatus pagal seniausius.
4. Užsirašykite: kokia yra seniausia data? Apie ką iš pradžių buvo tas vaizdas? Ar tai atitinka dabartinį teiginį apie sveikatą?

Svarbus priminimas:

- Visada rūšiuokite „TinEye“ rezultatus pagal seniausius – tai funkcija, dėl kurios ši paieškos sistema yra galingesnė už „Google“ nustatant vaizdo kilmę.
- Nulinis „TinEye“ rezultatų skaičius nereiškia, kad vaizdas yra autentiškas. Naudokite kelis įrankius.
- Svarbiausia rasti originalų paveikslėlio antraštę ir kontekstą.

3.1.3 Sveikatos vaizdo įrašų tikrinimas – InVID / WeVerify

Vaizdo įrašų dezinformaciją patikrinti sunkiau nei nuotraukų dezinformaciją, nes vaizdo įrašė yra daug kadro, o kiekvienas iš jų potencialiai yra nuotrauka, kurią galima paieškoti. Vaizdo įrašo negalima paspausti dešiniuoju pelės mygtuku taip, kaip galima paspausti ant nuotraukos. „InVID“ ir „WeVerify“ šią problemą sprendžia:

- suskirstydami vaizdo įrašą į atskirus kadrus, kuriuos vėliau galima vieną po kito ieškoti atvirkštine nuotraukų paieška;
- skaitydami vaizdo įrašė įterptus metaduomenis – nematomus duomenis, kurie gali atskleisti originalaus įrašo datą, įrenginio modelį, o kartais ir vietą;
- išskirdami miniatiūras, skirtas paieškai konkrečiose platformose.

Kaip įdiegti „InVID“ / „WeVerify“

- | | |
|---|--|
| 1 | „Chrome“ naršyklėje: atidarykite „Chrome“ internetinę parduotuvę (chrome.google.com/webstore). „Firefox“ naršyklėje: atidarykite „Firefox“ papildinių parduotuvę (addons.mozilla.org). |
| 2 | Paieškos juostoje įveskite „InVID WeVerify“. |
| 3 | Spustelėkite „Pridėti į „Chrome““ arba „Pridėti į „Firefox““. Įskiepis įdiegiamas per kelias sekundes. Naršyklės įrankių juostoje pasirodys nedidelė piktograma. |

Kaip naudoti „InVID“ / „WeVerify“: žingsnis po žingsnio

1	Nukopijuokite vaizdo įrašo URL „TikTok“, „Instagram“, „YouTube“ ar bet kurioje kitoje platformoje: raskite dalinimosi mygtuką ir nukopijuokite vaizdo įrašo nuorodą.
2	Atidarykite „InVID“ Spustelėkite „InVID/WeVerify“ piktogramą naršyklės įrankių juostoje. Atsivers įrankių skydelis.
3	Išskirkite pagrindinius kadrus Įklijuokite vaizdo įrašo URL adresą į įrankį. Pasirinkite „Pagrindiniai kadrai“ arba „Vaizdo įrašo analizė“. Įrankis iš vaizdo įrašo reguliariais intervalais išskiria seriją nejudančių kadrų.
4	Atlikite atvirkštinę kadrų paiešką Dešiniuoju pelės mygtuku spustelėkite bet kurį išgautą kadrą ir pasirinkite „Ieškoti vaizdo su „Google“ arba perkelti kadrą į „Google Images“ arba „TinEye“ – taip pat, kaip aprašyta 3.1.1 ir 3.1.2 skyriuose. Klausimas, į kurį reikia atsakyti: ar ši vieta yra ta, apie kurią kalbama vaizdo įrašė? Ar šis vaizdo įrašas anksčiau pasirodė kitame kontekste?
5	Vaizdo įrašo metaduomenų patikrinimas „InVID“ įrankyje ieškokite skirtuko „Metaduomenys“. Jame rodomi visi vaizdo įrašo faile įterpti duomenys, tarp kurių gali būti originalaus sukūrimo data, GPS koordinatės ir įrašymui naudotas įrenginys. Jei metaduomenyse nurodyta, kad vaizdo įrašas buvo sukurtas prieš dvejus metus, o įrašė teigiama, kad jis buvo nufilmuotas praeitą savaitę, tai reiškia, kad buvo nustatytas klaidingas kontekstas.

Į ką atkreipti dėmesį tikrinant vaizdo įrašus apie sveikatą

- **Lokacijos tvirtinimas:** ar fonas iš tiesų rodo tai, ką teigia autorius? Asmuo, tvirtinantis, kad filmuoja ligoninėje, gali stovėti bet kuriame koridoriuje. Atlikite atvirkštinę paiešką pagal fono kadrą, kad patikrintumėte, ar ši vieta yra pasirodžiusi kitame kontekste.

- **Tapatybės tvirtinimas:** galima patikrinti asmenį, kuris teigia esąs gydytojas, mokslininkas ar sveikatos priežiūros institucijos atstovas. Nufotografuokite aiškų kadrą, kuriame matomas jo veidas arba bet koks matomas vardinė kortelė, tada naudokite vaizdų paiešką kartu su kontekstiniu vertinimu (3.2.3 skyrius), kad patikrintumėte jo vardą ir nurodytus kvalifikacijos duomenis.
- **Laiko teiginiai:** ar metaduomenų data sutampa su paskelbimo data? Ar aplinka atitinka nurodytą datą? Nesutapimas išduoda melagingą kontekstą turintį įrašą.

Svarbus priminimas

- „InVID/WeVerify“ yra profesionalus vaizdo įrašų tikrinimo standartas, kurį naudoja žurnalistai visame pasaulyje. Įdiekite jį kaip nuolatinį įrankį savo naršyklėje.
- Metaduomenys gali būti pašalinti arba pakeisti platformų, todėl metaduomenų nebuvimas nėra autentiškumo įrodymas.
- Paieška kadrų po kadro yra lėta, bet išsami. Sutelkite dėmesį į kadrus, kuriuose matoma vieta, kalbėtojo tapatybė ar bet koks matomas tekstas.

3.1.4 Vaizdo manipuliacijos nustatymas – FotoForensics

Kas yra klaidų lygio analizė?

Kiekvienas skaitmeninis vaizdo failas turi suspaudimo parašą – modelį, sukurtą išsaugant vaizdą. Kai dalis vaizdo redaguojama po jo sukūrimo – pavyzdžiui, pridamas tekstas, pakeičiamas skaičius arba pakeičiamas veidas – ta redaguota sritis išsaugoma su kitokiu suspaudimo lygiu. Likusi vaizdo dalis išlaiko savo pradinį suspaudimą.

Klaidų lygio analizė (Error Level Analysis – ELA) šį skirtumą parodo, suspaudimo lygius paverčiant spalvomis. Neseniai redaguotos vaizdo sritys atrodo žymiai šviesesnės arba kitokios spalvos nei neredaguotos aplinkinės sritys.

Kaip naudoti „FotoForensics“: žingsnis po žingsnio

1	Eikite į fotoforensics.com Atidarykite fotoforensics.com savo naršyklėje. Paskyros nereikia.
2	Pateikite vaizdą Spustelėkite „Įkelti“ ir pasirinkite vaizdo failą, ARBA įklijuokite tiesioginį vaizdo URL adresą į adresų juostą puslapio viršuje. Tada spustelėkite „Įkelti“.
3	Peržiūrėkite ELA rezultatą Įrankis rodo originalų vaizdą ir jo ELA versiją vieną šalia kito. Ieškokite vietų, kurios yra žymiai šviesesnės arba kitokios spalvos nei aplinkinės sritys.
4	Išaiškinkite rezultatą Vienodas ryškumas visame vaizde rodo, kad jis nebuvo neseniai redaguotas. Ryškūs plotai tam tikrose vietose, ypač virš teksto, skaičių, veidų ar statistikos, rodo, kad vaizdas buvo redaguotas po jo sukūrimo.
5	Įvertinkite reikšmę Ne visi ryškumo skirtumai rodo piktaivališką redagavimą – JPEG suspaudimo artefaktai ir ekrano kopijos gali sukelti tam tikrų skirtumų. Atkreipkite dėmesį į ryškias dėmes būtent virš reikšmingo turinio: skaičių, vardų, logotipų ar medicininių duomenų.

Dažniausiai naudojami sveikatos dezinformacijos nustatymo atvejai:

Suklastoti statistiniai duomenys medicininių tyrimų ekrano kopijose.

Padaroma tikro tyrimo rezultato ekrano kopija ir pakeičiamas pagrindinis skaičius. ELA parodo pakeistą skaičių kaip šviesią dėmę ant vienodo fono.

Pakeistos produkto etiketės ar maistingumo informacija. Sudedamųjų dalių sąrašai, vartojimo instrukcijos ar įspėjamieji užrašai pakeisti, siekiant pašalinti saugos informaciją. Pakeistas tekstas atrodo ryškesnis nei originalioje etiketėje.

Suklastotos citatos, priskiriamos sveikatos institucijoms. Tikra sveikatos pareigūno nuotrauka su suklastotu tekstu, pridėtu kaip antraštė ar kalbos burbulas. Pridėto teksto suspaudimo profilis skiriasi nuo originalios nuotraukos.



- “FotoForensics” geriausiai veikia su vaizdais, kurie nebuvo smarkiai pakartotinai suspausti socialinių tinklų platformose. Kai vaizdas įkeliamas į „Instagram“ ar „TikTok“ ir vėliau vėl atsisiunčiama, pačios platformos suspaudimas gali sumažinti ELA veiksmingumą.
- Geriausiems rezultatams pasiekti: jei įmanoma, naudokite originalų vaizdo failą arba aukščiausios kokybės versiją, kurią galite rasti.
- ELA yra vienas iš kelių įrankių. Švarus ELA rezultatas negarantuoja, kad nuotrauka nėra suklastota. Derinkite su atvirkštine nuotraukų paieška ir konteksto analize.

Svarbus priminimas

- ELA savaime nėra manipuliacijos įrodymas – tai įrodymas, kurį reikia interpretuoti.
- ELA analizę sutelkite į reikšmingą turinį: skaičius, tekstą, veidus ir logotipus, o ne foną.
- Visada derinkite „FotoForensics“ su kitomis priemonėmis, kad gautumėte išsamų vaizdą.

Svetainių ir domenų analizė

Toliau pateikiamame skyriuje aprašomi trys metodai, kaip įvertinti sveikatos svetainių patikimumą. Juos galima taikyti paeiliui bet kuriai svetainei, dėl kurios kyla abejonių, arba naudoti atskirai, priklausomai nuo konkrečios problemos.

3.2.1 URL skaitymas kaip detektyvas – URL struktūra, WHOIS ir šoninis skaitymas

URL struktūros supratimas

Kiekvienas interneto adresas turi griežtą struktūrą. Teisingas jo perskaitymas užtrunka dešimt sekundžių ir leidžia nustatyti, ar svetainė yra ta, už kurią save laiko.

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

subdomain – Nustato savininkas. Gali būti bet koks žodis, įskaitant „nhs“, „who“, „government“.

realdomain – Tikrasis svetainės pavadinimas. Būtent jį turite atpažinti.

.extension (TLD) – Riboti plėtiniai (.gov, .int, .edu) rodo autoritetą. Atviri plėtiniai (.info, .biz, .net) yra prieinami bet kam.

Auksinė taisyklė: skaitykite iš dešinės į kairę nuo pirmojo įstrižinio brūkšnelio (/)

Tikrasis domenas yra tai, kas yra prieš pirmąjį /. Viskas, kas yra kairėje, yra subdomenas – kurį bet kas gali nustatyti kaip bet kokį žodį, įskaitant patikimos organizacijos pavadinimą.

- **who-healthalerts.net/vaccine-warning** → Tikrasis domenas: **who-healthalerts.net** (NE Pasaulio sveikatos organizacija)
- **health.nih-alerts.com/update** → Tikrasis domenas: **nih-alerts.com** (NE NIH)
- **who.int/news** → Tikrasis domenas: **who.int** ✓ Teisėta WHO

Lygis	Plėtiniai	Kas gali registruoti?
Apribotas	.gov .int .edu	Tik vyriausybės, tarptautinės organizacijos ir (plačioja prasme) švietimo įstaigos
Patikrinti	.org .nhs.uk .ac.uk	Iš pradžių ribotas; dabar atviresnis. Patikrinkite WHOIS
Visi	.com .net .info .biz	Atvira registracija. Sveikatos svetainė su .info domeno vardu, kuri teigia esanti autoritetinga, yra pavojaus signalas

Kaip naudotis WHOIS?

WHOIS yra vieša duomenų bazė, kurioje registruojama, kada buvo užregistruotas kiekvienas domenas, kas jį užregistravo ir kur jis talpinamas. Svetainė, kuri teigia turinti 20 metų patirtį sveikatos srityje, bet buvo užregistruota prieš tris mėnesius, nėra tokia, kokia save pristato.

1	Eikite į who.is Atidarykite who.is savo naršyklėje.
2	Įveskite domeną Įveskite domeno vardą (pvz., naturalhealthtruth.com) į paieškos juostą ir paspauskite „Enter“.
3	Raskite sukūrimo datą Ieškokite laukelio su pavadinimu „Sukurta“ arba „Registracijos data“.
4	Patikrinkite registruotoją Pažiūrėkite į „Registruotojas“ arba „Organizacija“. Paslėpti registruotojo duomenys, saugomi privatumo paslaugos, patys savaime yra svarbi informacija.
5	Įvertinkite Palyginkite registracijos datą ir registruotoją su institucija, kurią nurodo svetainė. Naujai užregistruota + paslėptas registruotojas + atviras TLD = aiškūs pavojaus ženklai.

Lateral Reading: Leave the Website Immediately

Stanfordo istorijos švietimo grupės tyrimas parodė, kad profesionalūs faktų tikrintojai įvertino svetainės patikimumą greičiau ir tiksliau nei ekspertai, atlikdami vieną dalyką: jie nedelsdami paliko svetainę ir paieškojo, ką apie ją sako kiti. Tai yra šoninis skaitymas.

Šoninio skaitymo procesas – 30 sekundžių

- 1** Atidarykite sveikatos svetainę, kurios nežinote.
- 2** Neskaitykite straipsnių. Nedelsdami atidarykite naują naršyklės skirtuką.
- 3** Paieška: [svetainės pavadinimas] + „faktų patikrinimas“ ARBA [svetainės pavadinimas] + „klaidinga informacija“ ARBA [svetainės pavadinimas] + „apžvalga“.
- 4** Ieškokite informacijos iš faktų tikrinimo organizacijų (Snopes, Full Fact, AFP Fact Check, Correctiv), medicinos institucijų (PSO, nacionalinių sveikatos ministerijų) arba akademinių vertinimų.
- 5** Vertinimas: patikima išorinė informacija = elkitės atsargiai; nėra išorinės informacijos = nėra pripažintos institucijos; faktų tikrintojas identifikuoja kaip dezinformacijos šaltinį = nenaudokite.

Svarbus priminimas:

- Tikrasis domenas = tai, kas yra prieš pirmąjį /. Patikimų prekės ženklų pavadinimai subdomeno pozicijoje yra klasikinė manipuliacijos taktika.
- WHOIS registracijos data yra vienas iš greičiausių patikimumo rodiklių.
- Šoninis skaitymas yra greitesnis ir tikslesnis nei gilus skaitymas vertinant šaltinio patikimumą.
- HTTPS = šifruotas ryšys. Tai nereiškia, kad turinys yra patikimas.



The HTTPS padlock does NOT mean a website is trustworthy. It only means the connection is encrypted. Disinformation websites routinely use HTTPS. The padlock says nothing about content accuracy.

Socialinių tinklų ir paskyrų analizė

Toliau pateikiamame skyriuje aptariami du įrankiai, skirti įvertinti, ar socialinių tinklų paskyra, skelbianti turinį apie sveikatą, yra autentiška. 6 punktų kontrolinis sąrašas pateikia vertinimo metodą; „Social Blade“ pateikia duomenimis pagrįstus įrodymus apie neautentišką sekėjų skaičiaus augimą.

3.3.1 Ar ši paskyra yra tikra? – Profilio kontrolinis sąrašas ir „Social Blade“

Kodėl netikri paskyros svarbios sveikatos srityje

Netikri paskyros – botai, nupirkti sekėjai ir koordinuoti netikri profiliai – naudojami sveikatos dezinformacijos kampanijose, kad melagingi teiginiai apie sveikatą atrodytų populiaresni ir plačiau priimami, nei yra iš tikrųjų. Visų penkių partnerių šalių apklausos duomenys parodė, kad iki 83 % respondentų buvo susidūrę su dezinformacija apie stebuklingus produktus. Daugelis tų produktų reklamuojami per netikrų paskyrų tinklus. Šio reiškinių mechanizmas yra tas pats, kuris visose penkiose nacionalinėse apklausose buvo nustatytas kaip pagrindinis rizikingos sveikatos elgsenos veiksnys: socialinis įrodymas. Jei atrodo, kad visi kažką rekomenduoja, impulsas sekti yra labai stiprus. Netikri paskyros dirbtinai sukuria tą socialinį įrodymą.

6 punktų paskyros autentiškumo patikrinimo sąrašas

Taikykite šiuos šešis patikrinimus bet kuriam paskyros, reklamuojančios teiginius apie sveikatą „Instagram“, „TikTok“ ar „YouTube“, atžvilgiu. Trys ar daugiau įspėjamųjų ženklų kartu yra tvirtas įrodymas, kad elgesys yra netikras.

1

Raskite paskyros sukūrimo datą (daugumoje platformų ji matoma skiltyje „Apie“ arba „Paskyros informacija“).

Palyginkite ją su sekėjų skaičiumi. Tikras sveikatos švietėjas, kuris per trejus metus susikūrė auditoriją, gali turėti 50 000 sekėjų. Paskyra, turinti 300 000 sekėjų po šešių mėnesių, verčia atidžiau ją patikrinti.

Įtartinas požymis: labai didelis sekėjų skaičius labai naujam paskyros.

2

Eikite į socialblade.com ir įveskite paskyros vartotojo vardą.

„Social Blade“ veikia „YouTube“, „Instagram“ ir „TikTok“ platformose. Natūralus augimas atrodo kaip laipsniškas nuolydis. Nusipirkti sekėjai atrodo kaip staigus šuolis – staigus tūkstančių sekėjų skaičiaus padidėjimas per vieną dieną.

Įtartinas požymis: bet koks vienos dienos šuolis, kai sekėjų skaičius padidėja tūkstančiais, po kurio vėl grįžtama prie lėto augimo.

3

Pereikite per paskyros įrašus. Autentiškos paskyros derina turinio tipus, formatus ir temas. Suderintos neautentiškos paskyros skelbia įrašus su mechaniniu reguliarumu: tas pats šablonas, tas pats stilius, tas pats tvarkaraštis, kasdien be jokių nukrypimų.

Įtartinas požymis: kiekvienas įrašas yra to paties formato, išdėstymo ir antraštės struktūros.

4**Perskaitykite 10–15 komentarų prie naujausių įrašų.**

Autentiškas bendravimas apima konkrečius, įvairius atsakymus. Neautentiški komentarų tinklai generuoja trypas, bendro pobūdžio, pasikartojančias frazes – „Tai pakeitė mano gyvenimą!“, „Tiesa!“, „Nuostabus produktas!“ – be jokių asmeninių detalių.

Įtartinas požymis: *dauguma komentarų susideda iš 3–5 bendrų žodžių arba tos pačios frazės, kuri pažodžiui kartojasi keliuose įrašuose..*

5**Didelis autentiškas paskyros savininkas paprastai seka palyginti nedaugelį kitų paskyrų.**

Paskyra, kuri seka 12 000 žmonių, o turi 14 000 sekėjų, gali būti dalis „sek-už-sekimą“ schemos, paplitusios papildų reklamos tinkluose. Patikrinkite, ar paskyros, kurias seka, taip pat yra sveikatos produktų reklamuotojai.

Įtartinas požymis: *sekamų paskyrų skaičius artimas arba viršija sekėjų skaičių.*

6**Ieškokite to paties teiginio apie sveikatą arba paskyros vardo kitose platformose.**

Koordinuoti tinklai dažnai vienu metu skelbia identiškų tekstus ir vaizdus „Instagram“, „Facebook“, „TikTok“ ir „YouTube“ – žodis į žodį.

Įtartinas požymis: *visiškai tas pats tekstas ir vaizdai, pasirodantys vienu metu keliose platformose.*

Kaip naudoti „Social Blade“

1 Eikite į **socialblade.com**

Atidarykite socialblade.com savo naršyklėje.

2 Įveskite vartotojo vardą

Į paieškos juostą įveskite „Instagram“, „TikTok“ arba „YouTube“ vartotojo vardą. Išskleidžiamajame meniu pasirinkite reikiamą platformą.

3 Peržiūrėkite grafiką

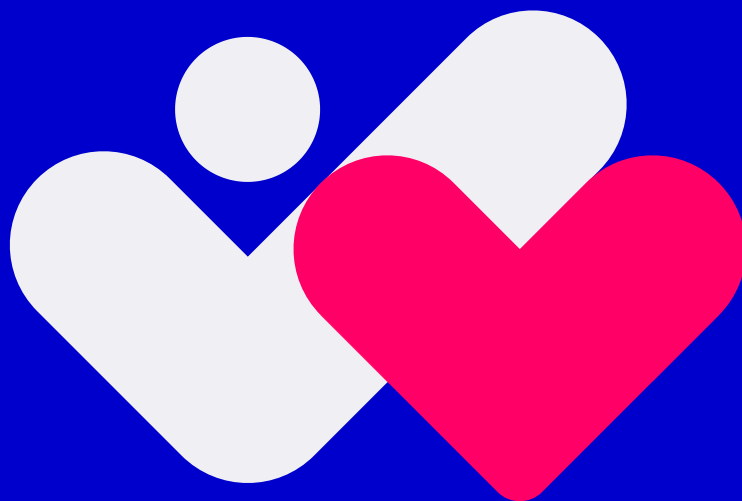
Pagrindiniame grafike matomi kasdieniniai sekėjų skaičiaus pokyčiai laikui bėgant. Lygus, laipsniškas nuolydis = natūralus augimas. Staigus vertikalus šuolis vieną dieną = nupirkti sekėjai.

4 Patikrinkite duomenų lentelę

Po grafiku esančioje kasdienėje duomenų lentelėje pateikiami tikslūs sekėjų skaičiai kiekvienai dienai. Ieškokite dienos, kurią sekėjų skaičius padidėjo neįprastai smarkiai. Jei vieną dieną atsirado 200 000 sekėjų, o augimas kitomis dienomis buvo lėtas, tie sekėjai buvo nupirkti.

Svarbus priminimas:

- Nė vienas įspėjamasis ženklas savaime neįrodo netikrumo. Trys ar daugiau kartu yra tvirtas įrodymas.
- Netikros paskyros sustiprina dezinformaciją iš tikro šaltinio – jos ne visada ją kuria. Taip pat patikrinkite pirminį teiginį naudodami platesnį faktų tikrinimo įrankių rinkinį.
- Didelis sekėjų skaičius nieko nereiškia, jei sekėjai buvo nupirkti. „Social Blade“ leidžia pamatyti nupirktus sekėjus.



Centar za mir, nenasilje i ljudska prava - Osijek
30 godina aktivno gradimo mir



**future
needs**



FORMA.Azione



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.