PRETHODNO PRIOPĆENJE

UDK 001.103.2

KRUNOSLAV ANTOLIŠ*

DEZINFORMACIJE U DIGITALNOM DOBU

Sažetak[1]

U radu se istražuje pojavu dezinformacija i lažnih vijesti u suvremenom digitalnom okruženju. Naglašava se da dezinformatori koriste naprednu tehnologiju, uključujući botove, tvornice trolova i ciljano oglašavanje, kako bi manipulirali informacijama na društvenim mrežama. Dezinformacije predstavljaju ozbiljnu prijetnju demokraciji i zahtijevaju sustavan pristup njihovom suzbijanju.

Rad također ističe da čak i digitalno obrazovani ljudi ponekad teško prepoznaju manipulirane vijesti. Stoga se naglašava važnost prepoznavanja dezinformacija na individualnoj i institucionalnoj razini, te se preporučuje provjera sadržaja, autora, izvora, datuma i drugih elemenata prije dijeljenja informacija. U radu se nude brojni alati za analizu video materijala, slika i web stranica, uključujući alate za provjeru vjerodostojnosti, geolokaciju, detekciju plagijata, analizu sličnosti i druge tehnike analize informacija. Također se ističe važnost zaštite privatnosti i sigurnosti na internetu kroz korištenje virtualnih strojeva, VPN-ova i drugih alata. Nadalje, rad naglašava potrebu za sustavnim pristupom u borbi protiv dezinformacija kako bi se zaštitio integritet informacijske i komunikacijske infrastrukture, jer je očuvanje informacija ključno za povjerenje javnosti i zdravlje demokracije.

Rad također govori o proširenjima preglednika za blokiranje oglasa poput Adblock Plus-a, AdGuard-a i uBlock Origin-a, ističući njihove različite značajke. Također nudi napredne tehnike pretraživanja, uključujući operatore pretraživanja za precizno filtriranje rezultata pretraživanja. Osim toga, rad se bavi analizom e-pošte, sigurnosnim aspektima datoteka i alatima za prikupljanje i analizu informacija s društvenih medija (SOCMINT). Naglašava se važnost praćenja online aktivnosti i analize metapodataka društvenih medija. Kroz sve ove teme, rad pruža korisne informacije za online istraživanja, zaštitu privatnosti i analizu informacija s društvenih medija u digitalnom dobu.

Ključne riječi: *dezinformacije, digitalno doba, društvene mreže, metapodaci, obrazovanje*

---

* izv.prof.dr.sc. Krunoslav Antoliš, Veleučilište kriminalistike i javne sigurnosti, Policijska akademija "Prvi hrvatski redarstvenik", MUP Republika Hrvatska, Av. Gojka Šuška 1, Zagreb, kantolis@fkz.hr

[1] Rad je nastao temeljem istraživanja u projektu Erasmus + KA220-HED - Cooperation partnerships in higher education (2022./2025.)

UVOD

Lažne vijesti i dezinformacije, odnosno namjerno izmijenjene informacije s ciljem obmanjivanja ljudi, postaju sve raširenija globalni pojavni oblik. Primjerice Tynes, B. M., Stewart, A., Hamilton, M., & Willis, H. A. kažu kako internetske dezinformacije, dezinformacijske kampanje i propaganda danas postaju trajni problemi. Fenomen suvremenih dezinformacija, često nazivanih "lažnim vijestima", višestruk je izazov digitalnog doba. Dezinformatori danas ne samo da izmišljaju informacije i šire ih, podsjećajući na u povijesti već viđenu propagandu i dezinformacije, već također koriste naprednu informacijsko komunikacijsku tehnologiju za manipuliranje tekstom, slikama i video zapisima. Ovu manipulaciju društvenim aspektom društvenih medija orkestriraju različiti akteri, teko primjerice Howard, Neudert, Prakash, i Vosloo ističu da dezinformacije širene ljudskim djelovanjem, botovima i plaćenim organiziranim skupinama tzv. tvornicama trolova djeluju zlonamjerno kako bi se stekao politički utjecaj i financijska dobit, odobravanje ideja i popularnost. Richard Rogers , Sabine Niederer navode kako se u nizu empirijskih studija, koristeći se digitalnim metodama i podatkovnim novinarstvom, istražuje se u kojoj su mjeri društveni mediji omogućili prodor inozemnih operacijama dezinformiranja, rasprostranjeno objavljivanje i širenje sumnjivog sadržaja kao i ekstremne komentatore sa značajnim brojem sljedbenika koji napadaju mainstream mediji kao lažne."

Dezinformacije predstavljaju različite oblike obmanjujućeg ili neprikladnog sadržaja koji se koristi s ciljem manipulacije percepcijom ili uvjeravanja javnosti u nešto što nije istina. Evo nekoliko ključnih kategorija dezinformacija: fikcionalni sadržaj, koji je potpuno izmišljeni sadržaji koji nemaju veze s istinom; prerađeni sadržaj, koji koristi stvarne informacije ili slike, ali se izobličavaju senzacionalnim naslovima ili populističkim metodama kako bi privukli pažnju; lažni izvori, kod kojih se dezinformatori maskiraju kao ugledni izvori, često koristeći imena ili brendiranje poznatih agencija kako bi stekli povjerenje publike; varljive tvrdnje kod kojih dezinformatori plasiraju obmanjujuće informacije kao činjenice, često putem komentara ili tvrdnji koje nisu potkrijepljene dokazima; netočan kontekst, gdje se činjenice prezentiraju u ispravnom kontekstu, ali se kombiniraju s lažnim informacijama, često kroz naslove članaka koji ne odražavaju stvarni sadržaj; satira i parodija, kada se smiješne priče koje nisu istinite predstavljaju se kao stvarne, bez namjere nanijeti ozbiljnu štetu; neusklađenost informacija, gdje naslovi, slike ili opisi ne odgovaraju stvarnom sadržaju; sponzorirani sadržaj je kada se oglašavanje ili PR materijali prikazuju kao neovisni novinarski sadržaj; propaganda, kada se sadržaj koristi kako bi se oblikovali stavovi, vrijednosti i znanje publike; pogreške u izvješćima koje su napravile novinske agencije ili mediji.

Uspon umjetne inteligencije (AI) otvara vrata novim oblicima dezinformacija i dezinformacija. Sintetički mediji koriste AI za stvaranje, manipulaciju i izmjenu podataka i multimedije kako bi zavarali ili promijenili izvorno značenje. Postoji zabrinutost da

bi sintetički mediji mogli širiti lažne vijesti, dezinformacije i podrivati povjerenje u stvarnost te automatizirati kreativne procese.

Prepoznavanje dezinformacija kao dvostrukog problema koji uključuje manipulaciju sadržajem i njegovo pojačavanje, što je ključno, kako na individualnoj tako i na institucionalnoj razini. U tom kontekstu, bez obzira radi li se o novinarima, istražiteljima, agencijama za provođenje zakona, istraživačima, edukatorima ili običnim građanima, potreban je sustavni pristup u ispunjavanju sve veće potražnje za suzbijanjem svih vrsta dezinformacija, od izmišljenog i izmijenjenog sadržaja do web stranica koje prodaju lažne vijesti i dezinformacije na digitalnim platformama i društvenim mrežama.

Čak i digitalno obrazovanim mladim ljudima ponekad je teško prepoznati manipulirane vijesti. Važno je napomenuti da čak šest od deset vijesti koje se dijele na društvenim mrežama nisu ni pročitane od strane korisnika koji ih dijele. Otprilike 85 % Europljana smatra ‹lažne vijesti› problemom u svojoj zemlji, dok njih 83 % smatra da predstavljaju prijetnju demokraciji uopće.

Dezinformacije su posebno opasne jer su često organizirane, podržane resursima i tehnologijom, a stvaratelji dezinformacija pokušavaju iskoristiti ranjivosti informacijsko komunikacijskih sustava i potencijalne pristaše kako bi širili svoje poruke. Društvene mreže i njihove personalizacijske alatke olakšavaju širenje lažnih priča i dezinformacija. U mnogim slučajevima, ove vijesti manipuliraju emocijama kako bi privukle pažnju i stvorile što više klikova, bilo iz ekonomskih ili ideoloških motiva.

Bitno je za uočiti kako društvene mreže i digitalne platforme igraju ključnu ulogu u širenju dezinformacija što posljedično otvara pravno pitanje regulacije tih platformi. Zbog toga su njihova samoregulacija i povećani pritisci na njih, usmjereni s ciljem poboljšanja kontrole i odgovornost u svezi sa sadržajem koji objavljuju.

Ovaj članak na osnovu istraživanja koje je provedeno na Policijskoj akademiji, MUP RH, nudi i preporuke vezane uz provjeru: sadržaja, vrste medija, autora, izvora, slike, uključujući provjere cirkulacije sadržaja, a predlaže također i korištenje web alata kao što su URL skeneri, ekstenzije preglednika, baze podataka crnih lista i alati za praćenje društvenih medija za platforme kao što su Facebook, TikTok, YouTube, kao i alati za analizu slika i videa.

Sustavni pristup je nužnost u ispravnom postavljanju borbe protiv dezinformacija u suvremenom dobu, unutar digitalnog okružja. On omogućuju dublje razumijevanje zamršenog odnosa između društvenih medija i dezinformacija, ističući kako se neprovjerene dezinformacije koje potječu s društvenih platformi mogu infiltrirati u glavne medije i utjecati na širi javni diskurs.

U konačnici, ovaj rad ima za cilj svojim spoznajama i prijedlozima, osnažiti stručnjake i institucije zadužene za očuvanje jedne od najvitalnijih vrijednosti u liberalnim društvima, a to je informacija. Točnosti i otpornosti informacija izravno utječu na povjerenje javnosti, kvalitetu javnog diskursa i cjelokupno zdravstveno stanje

demokracije. Rješavanje problema dezinformacija treba se promatrati kao stalnu bitku za zaštitu integriteta naše informacijske i komunikacijske infrastrukture.

Sustavni pristupa zaštiti od dezinformacija

Pérez-Escolar, Ordóñez-Olmedo i Alcaide-Pulido u svom radu Fact-Checking Skills And Project-Based Learning About Infodemic And Disinformation navode da obrazovanje predstavlja esencijalni temelj za zaštitu od dezinformacija, dok Van der Linden i sur. uz navedeno naglašavaju i važnost predlaganja rješenja koja se bave i ranjivošću učenika. Da biste se uspješno obranili od dezinformacija, ključno je imati sustavni pristup pripremi kontrolnog popisa za provjeru informacija. Antoliš K., Pačelat J.naglašavaju kako je razotkrivanje dezinformacija ključno za njihovo uspješno suzbijanje, a ovaj popis trebao bi obuhvaćati niz provjera kako bismo osigurali da su informacije koje konzumiramo vjerodostojne i točne.

Na popisu provjera trebali bismo uključiti sljedeće aspekte:

1. Vjerodostojnost Sadržaja: Prva provjera trebala bi se fokusirati na vjerodostojnost samog sadržaja. Trebali bismo procijeniti jesu li iznesene činjenice i statistike uvjerljive i podržane relevantnim izvorima.
2. Provjera Datuma: Važno je provjeriti točnost datuma kako bismo bili sigurni da je informacija aktualna i u korelaciji s trenutnim događajima.
3. Pouzdanost Izvora: Trebamo pažljivo provjeriti pouzdanost izvora informacija. To uključuje analizu URL-a, web stranice i/ili računa na društvenim medijima.
4. Provjera Autora: Autora članka trebali bismo procijeniti s obzirom na njihovu prepoznatljivost u struci, iskustvo i opus djelovanja. Ovo nam pomaže utvrditi autoritet autora.
5. Analiza Slika i Videozapisa: Slike i videozapise iz članka trebali bismo pažljivo analizirati kako bismo osigurali da nisu lažni ili manipulirani.
6. Provjera Referenci: Ukoliko su u članku navedene reference, trebali bismo provjeriti jesu li te reference pouzdane i podržavaju li iznesene tvrdnje.
7. Svijest o Vlastitoj Pritajenoj Pristranosti: Važno je biti svjestan vlastitih pristranosti i razmisliti o tome kako one mogu utjecati na našu prosudbu. Trebali bismo održavati skeptičan pristup.
8. Nakon što obavimo ovakvu pripremnu analizu, tek tada bismo trebali razmisliti o dijeljenju članka ili informacija.

Kako bismo osigurali sigurno radno okruženje, možemo poduzeti nekoliko preventivnih mjera:

1. Virtualni Stroj: Stvaranje virtualnog stroja kao emuliranog okruženja omogućuje nam izoliranje virtualnog računala od stvarnog, čime se povećava sigurnost.

2. Čišćenje Računala: Redovito čišćenje računala, uključujući brisanje povijesti pretraživanja i kolačića, pomaže očuvati privatnost i anonimnost pri pregledavanju interneta.
3. Virtualna Privatna Mreža (VPN): Korištenje VPN-a štiti internetski promet šifriranjem i skriva IP adresu, čime se osigurava anonimnost i zaštita online identiteta.
4. Proxy Poslužitelji: Proxy poslužitelji omogućuju skrivanje korisničkih IP adresa, čime se povećava sigurnost i privatnost pri pregledavanju interneta.
5. Sigurni Internet Preglednici: Odabir sigurnih internet preglednika kao što su Google Chrome, Mozilla Firefox, Microsoft Edge, Safari i Opera prvi je korak u osiguranju sigurnog pregledavanja interneta.
6. Proširenja Preglednika: Proširenja preglednika, kao što su dodaci za poboljšanje sigurnosti i privatnosti, mogu dodatno pojačati zaštitu računala.
7. Antivirusni Softver i Vatrozidi: Korištenje antivirusnih programa i vatrozida pomaže u zaštiti računala od kibernetičkih napada i zlonamjernog softvera.
8. Testiranje Veze: Važno je redovito provoditi testiranje veze kako bismo bili sigurni da ne dolazi do curenja važnih informacija s našeg računala.

Dodatno, možemo koristiti online alate poput https://ipleak.net/ i https://amiunique.org/ kako bismo provjerili informacije koje su dostupne o nama i zaštitili svoju privatnost. Neki autori Astuti, S. I., Giri, L., & Hidayah, N. preporučuju Video Web dramske serije za borbu protiv dezinformacija su inovacja u dopiranju do publike i njihovom poučavanju.

Alati za analizu video materijala i slika

Video materijali

U ovom poglavlju, istražujemo alate za analizu video materijala, uključujući inverznu pretragu video snimaka, pregled metapodataka, preuzimanje video sadržaja te alate za provjeru i uređivanje video materijala.

Inverzna pretraga video snimaka je moćna tehnika i alat za pronalaženje informacija o videozapisima i slikama na internetu. Ona uspoređuje sadržaj slika ili video isječaka s postojećim izvorima, omogućujući preciznije pretraživanje nego ikad prije. Za izvođenje inverzne pretrage videozapisa možete koristiti alate poput https://berify.com i https://www.google.com/imghp.

Analiza video sadržaja, također poznata kao analitika video sadržaja (VCA) ili video analiza (VA), predstavlja sposobnost automatske analize video materijala radi otkrivanja vremenskih i prostornih događaja. Ova tehnologija koristi video materijal za analizu i poboljšanje učinka timova ili pojedinaca. Analiza se može provoditi u stvarnom

vremenu, a rezultati su dragocjeni za sveobuhvatno razumijevanje učinka timova, bilo da se radi o vašem timu ili suparnicima.

Prilikom provođenja video analize, važno je postavljati relevantna pitanja, kao što su: Tko je autor ovog videa? Kome je namijenjen ovaj video? Kada je ovaj video snimljen? Koji je glavni koncept videa? Možete provesti analizu video zapisa putem alata kao što su http://lvcdn.net/gop i https://snapwonders.com/upload/analyse-video.

Slično fotografijama, video snimci također sadrže metapodatke o mjestu na kojem su snimljeni. Osim toga, formate spremnika poput AVI i MP4 prate metainformacije o kodecima, video i audio tokovima te još mnogo toga. Preglednik metapodataka omogućuje otkrivanje informacija o video datotekama koje možda niste bili svjesni. Metapodatke video zapisa možete analizirati putem alata kao što su https://www.metadata2go.com i https://www.flexclip.com/tools/metadata-video.

Video Downloader je softver koji se koristi za preuzimanje video sadržaja s različitih platformi kao što su YouTube i Facebook. Ako želite preuzeti videozapise s interneta, možete koristiti dobro poznate platforme poput YouTubea i Vimea, budući da su obično sigurne od zlonamjernog softvera. Alati za preuzimanje videozapisa lokalno dostupni su na web stranicama kao što su https://catchvideo.net i https://smallseotools.com/online-video-downloader.

Video verifikacija je usluga koja se temelji na sveprisutnim računalnim kamerama, pametnim sigurnosnim kamerama i pametnim telefonima. Ova usluga koristi fotografije i video materijale kako bi potvrdila identitet osoba. Provjeru video materijala možete obaviti putem alata kao što je https://www.invid-project.eu/tools-and-services/invid-verification-plugin (proširenje).

Video uređivanje, odnosno montaža, predstavlja umjetnost manipulacije i kombiniranja video datoteka kako bi se stvorio konačni video projekt. Video uređivači mogu izrezivati filmske isječke, prilagođavati zvuk, dodavati digitalne efekte i provoditi druge tehničke izmjene video datoteka. Možete uređivati video datoteke koristeći alate poput https://clideo.com i https://www.kapwing.com/studio/editor."

Slika

Softver za analizu slika, također poznat kao softver za prepoznavanje slika ili računalni vid, koristi umjetnu inteligenciju za obradu slika i izdvajanje detalja. Algoritmi strojnog učenja često se primjenjuju za identifikaciju različitih objekata, pružajući mnoge korisne primjene za različite brendove.

Obrnuto pretraživanje slika, poznato i kao pretraživanje temeljeno na sadržaju slika (CBIR), uključuje uporabu uzorka slike kako bi se izvršila pretraga u CBIR sustavima. Ogledna slika igra ključnu ulogu u ovom postupku, jer sustav koristi njezinu strukturu za pretragu informacija. Možete izvršiti obrnuto pretraživanje slika putem https://tineye.com i https://www.google.com/imghp.

Analiza Slike Analiza slike ili analiza slika odnosi se na proces izvlačenja smislenih informacija iz digitalnih slika pomoću tehnika obrade digitalnih slika. Ovi zadaci mogu biti jednostavni, poput čitanja bar kodova, ili složeni, kao što je prepoznavanje lica. Računala su neizostavna za analizu velikih količina podataka i složene računske zadatke, dok ljudski vizualni korteks ostaje neprocjenjiv za analizu visoke razine informacija. To je posebno važno u medicini, sigurnosti i daljinskim istraživanjima. Mnogi alati za analizu slika inspirirani su modelima ljudske vizualne percepcije, uključujući rubne detektore i neuronske mreže. Možete izvršiti analizu slika putem https://www.aperisolve.com i https://snapwonders.com/upload/analyse-photo-or-image.

Slika Forenzika Forenzika slika primjenjuje znanost o slikama i ekspertno znanje za tumačenje slika u pravnim kontekstima. Ovo uključuje tumačenje sadržaja slika i samih slika u pravnom okruženju. Detekcija forenzike slika može se izvršiti putem https://29a.ch/photo-forensics i https://fotoforensics.com.

Preglednik Metapodataka Metapodatak je informacija o drugim podacima koja se često nalazi u datotekama, ali nije vidljiva na prvi pogled. Metapodaci se koriste za razne svrhe, uključujući informacije o autoru, datumu stvaranja i drugim relevantnim podacima. Preglednik metapodataka poput Metadata2Go.com omogućuje pristup tim skrivenim metapodacima u datotekama kao što su slike, dokumenti, videozapisi i audio zapisi. To je korisno za očuvanje privatnosti i pruža uvid u informacije koje se možda ne vide na prvi pogled. Možete provjeriti metapodatke slika putem https://exifdata.com i https://jimpl.com.

Pretvarač Slike u Tekst Alati za pretvaranje slike u tekst omogućuju kopiranje teksta s fotografija i drugih vizualnih sadržaja. Ovi alati koriste tehnologiju optičkog prepoznavanja znakova (OCR) kako bi izdvojili tekst iz slika i omogućili njegovo kopiranje. To je posebno korisno za izdvajanje teksta iz formata poput PNG. Možete koristiti alate poput https://www.onlineocr.net i https://ocr.space/copyfish (kao ekstenziju preglednika).

Prepoznavanje Lica Prepoznavanje lica koristi se za identifikaciju ljudskih lica na slikama i videozapisima, uključujući utvrđivanje identičnosti lica na različitim slikama ili pronalaženje određenih lica među velikim zbirkama slika. Ovo je posebno korisno u sigurnosnim i identifikacijskim aplikacijama. Možete izvršiti prepoznavanje lica putem https://pimeyes.com/en i https://betaface.com/demo.html.

Steganografska Detekcija Steganografija je tehnika skrivanja informacija unutar drugih podataka ili slika kako bi se izbjeglo otkrivanje. Steganografska detekcija pomaže u otkrivanju takvih skrivenih informacija u datotekama. To uključuje otkrivanje promjena u veličini datoteka, formatu, datumu zadnje izmjene i drugim karakteristikama koje ukazuju na prisutnost steganografije. Detekciju steganografije možete izvršiti putem https://mcafee.com/enterprise/en-us/downloads/free-tools/steganography.html.

Procjena Geolokacije Slike Procjena geolokacije slike omogućuje određivanje mjesta na kojem je slika snimljena putem kartografskog prikaza. Ovo se postiže povlačenjem

ili klikom na oznaku na karti svijeta na temelju slike. Također, ove alate možete koristiti za procjenu geolokacije slika koje ste prenijeli. Možete izvršiti procjenu geolokacije slika putem https://labs.tib.eu/geoestimation.

Alati zasnovani na Webu

Analiza Domena Proces analize domena uključuje stjecanje temeljnih informacija od strane softverskih inženjera. Njihova svrha je steći dovoljno znanja kako bi razumjeli kontekst problema i donijeli kvalitetne odluke tijekom analize zahtjeva i drugih faza procesa softverskog inženjeringa. Riječ "domena" ovdje se odnosi na opće područje poslovanja ili tehnologije gdje korisnici planiraju koristiti softver. Istraživanje Informacija o Domenama, vidi na: https://whois.domaintools.com i https://centralops.net/co.

Skener URL-ova s Malverom Koristite ovaj alat za skeniranje URL-ova kako biste otkrili zlonamjerni softver i potencijalne prijetnje identitetu. IPQS skener za zlonamjerne URL-ove pruža stvarnovremene rezultate s preciznom analizom putem strojnog učenja. Ovo vam omogućuje da provjerite URL-ove za moguće prijetnje kao što su krađa identiteta, zlonamjerni softver, virusi, zloupotreba ili problemi s reputacijom. Upotrijebite ovaj besplatan alat za skeniranje URL-ova kako biste se zaštitili od sumnjivih veza, prijevara ili opasnih web stranica. Možete pregledavati korisnički generirane sadržaje, e-poštanske poruke i poveznice, a sve s ciljem pouzdanog otkrivanja URL-ova koji predstavljaju prijetnju identitetu. IPQS upravlja najvećom mrežom prijetnji na internetu, omogućujući našim stručnjacima i algoritmima za strojno učenje da brže otkriju zlonamjerne URL-ove, sumnjive veze i lažno ponašanje nego bilo koji drugi servis. Imate izravan pristup izvorima podataka o prijetnjama i alatima za prevenciju prijevara, što vam omogućuje jednostavnu implementaciju ovih usluga u vlastito okruženje. To vam omogućuje provjeru vaših URL-ova kako biste bili sigurni da nisu zaraženi zlonamjernim softverom ili da se ne ponašaju sumnjivo.Otkrijte informacije o URL-ovima web mjesta: https://www.ipqualityscore.com/threat-feeds/malicious-url-scanner, https://urlscan.io, https://www.urlvoid.com

DNS Pretraživanje Općenito, DNS pretraživanje je proces dobivanja DNS zapisa s DNS poslužitelja. To se može usporediti s traženjem telefonskog broja u telefonskom imeniku, pa se zato naziva "pretragom". Međusobno povezana računala, poslužitelji i pametni telefoni moraju znati kako prevesti adrese e-pošte i imena domena koje ljudi koriste u smislene numeričke adrese, a upravo to DNS pretraživanje omogućuje. Otkrijte informacije o sustavima naziva domena (DNS): https://dnschecker.org/all-dns-records-of-domain.php, https://viewdns.info

Provjerite na Crnoj Listi Provjerom na crnoj listi testira se IP adresa poslužitelja e-pošte na više od 100 crnih lista e-pošte temeljenih na DNS-u (često se nazivaju stvarnim vremenom, DNSBL ili RBL). Ako je vaš poslužitelj e-pošte na crnoj listi,

može se dogoditi da vaša e-pošta ne bude isporučena. Crne liste e-pošte često se koriste za smanjenje neželjene pošte. Ovaj alat provjerava je li domena uključena u bazu podataka neželjene pošte. Provjerite na crnoj listi na: https://www.blacklistalert.org, https://mxtoolbox.com/blacklists.aspx

Ekstraktor Slika Chrome proširenje "Image Extractor" omogućuje korisnicima izdvajanje slika i povezanih informacija sa sadržaja web stranice, uključujući nazive slika, alternativne tekstove i URL-ove. Korisnici također mogu preuzeti pojedinačne slike, kopirati URL-ove slika i preuzeti sve slike kao ZIP datoteku. Ovaj alat omogućuje ekstrakciju slika s web stranica. Ekstraktor slika dostupan na: https://extract.pics, https://download-all-images.mobilefirst.me (ekstenzija).

Detekcija Sličnosti Detekcija plagijata ili otkrivanje sličnosti sadržaja odnosi se na proces otkrivanja slučajeva plagijata ili kršenja autorskih prava unutar djela ili dokumenata. S porastom upotrebe računala i interneta, plagiranje tuđih radova postalo je češće. Ovaj alat pomaže u pronalaženju web stranica s sličnim sadržajem. Detekcija plagijata dostupna na: https://www.copyscape.com, https://www.similarweb.com

Arhiva Web Stranica Web arhiviranje je proces prikupljanja dijelova World Wide Weba kako bi se osiguralo da su informacije sačuvane u arhivu za buduće istraživače, povjesničare i javnost. Web arhivari koriste alate za indeksiranje weba kako bi automatski bilježili sadržaj zbog ogromne količine informacija dostupnih na webu. Najpoznatija organizacija za web arhiviranje je Wayback Machine, koja se trudi očuvati arhivu cijelog interneta. Pregledajte povijest web stranica na: https://archive.org/web, https://archive.ph

Analiza Malvera Analiza zlonamjernog softvera podrazumijeva razumijevanje ponašanja i svrhe sumnjivih datoteka ili URL-ova kako bi se otkrile potencijalne prijetnje. Rezultati analize pomažu u identifikaciji i suzbijanju tih prijetnji. Ovaj alat omogućuje analizu web stranica kako biste provjerili postoje li znakovi zlonamjernog softvera. Analizirajte web stranice na: https://www.virustotal.com/gui/home/url, https://sitecheck.sucuri.net

Proširenje preglednika

Proširenja preglednika s dodatnim funkcijama za zaštitu vaše radne okoline, uključujući blokiranje oglasa može igrati značajnu ulogu u borbi sa dezinformacijama.

Prema uglednim recenzijama, najbolji blokeri oglasa u 2023. godini uključuju Adblock Plus, AdGuard i uBlock Origin. Svako od ovih proširenja omogućuje blokiranje oglasa bez problema, ali nisu sva ista. Na primjer, uBlock Origin efikasno blokira različite vrste oglasa, dok Adblocker za YouTube blokira samo autoplay video oglase.

uBlock Origin, koje ne treba miješati s uBlock ili µBlock, je iznimno popularno proširenje koje je dostupno za brojne preglednike. Međutim, važno je paziti na točnu verziju koju instalirate, jer proširenja s sličnim nazivima nisu ista. Ovo proširenje je lagano i efikasno, ne opterećuje memoriju i procesor, čineći vaše surfanje bez frustracija.

Osim toga, uBlock Origin je svestrani blokator sadržaja s poboljšanom sigurnosnom funkcionalnošću koja ne ometa vaše online aktivnosti. Pruža vam i pristup različitim listama, uključujući Fanboyev poboljšani popis za praćenje, spam404, Domaćina Dana Pollocka itd. Sve u svemu, uBlock Origin je najbolji izbor za one koji žele blokirati oglase bez usporavanja svojih računala. Osim toga, uBlock Origin se nalazi među osam najboljih YouTube naprednih alternativa za gledanje YouTube videozapisa. Ako preferirate Chromium temeljen preglednik za gledanje YouTube videozapisa bez oglasa, Kiwi preglednik je dobar izbor. S podrškom za preglednička proširenja, možete instalirati proširenja poput uBlock Origin i SponsorBlock kako biste uživali u gledanju YouTube videozapisa bez prekida. Za razliku od nekih drugih alternativa poput YouTube Vanced, Kiwi preglednik vam omogućuje prijavu na svoj Google račun.

ScriptSafe je Chrome proširenje koje korisnicima pruža kontrolu nad webom i osigurava sigurno pregledavanje. Betonira siguran i šifriran HTTPS protokol koji se koristi za zaštićenu komunikaciju putem interneta ili mreže.

Dodatno, Proširenje za Promjenu Geolokacije (Location Guard) omogućuje vam jednostavno mijenjanje vaše geografske lokacije kako biste zaštitili svoju privatnost. Možete postaviti željenu geografsku širinu i dužinu prema vašim preferencijama, skrivajući tako vašu stvarnu lokaciju.

Canvas Fingerprint Defender je lagano proširenje koje omogućuje skrivanje stvarnog otiska platna putem upotrebe lažnih nasumičnih vrijednosti. Umjesto potpune blokade otiska platna, ova metoda dodaje nasumični šum kako bi spriječila praćenje.

InVID WeVerify proširenje je moćan alat koji pomaže novinarima i provjeriteljima činjenica u identificiranju dezinformacija na internetu, posebno kod provjere videozapisa i slika na društvenim mrežama.

Image Downloader - Image Search - Pic Finder je kompaktni alat za pretragu i preuzimanje slika s interneta.

SingleFile je Safari proširenje koje omogućuje spremanje cijelih web stranica kao jedne HTML datoteke, uključujući slike, stilove, okvire i fontove.

User Agent Switcher je alat koji omogućuje emulaciju različitih preglednika i operativnih sustava u Chrome pregledniku, što vam omogućuje pregledavanje interneta kao da koristite druge preglednike.

Napredne tehnike pretraživanja

Važno je odabrati tražilicu prema svojim specifičnim potrebama, a neke od najčešće korištenih tražilica uključuju Google, Bing, Yahoo!, DuckDuckGo i Carrot2.

U svrhu preciznog filtriranja rezultata pretraživanja, možete koristiti operatore pretraživanja, poznate i kao “dorks”, u većini tražilica. Ovdje su neki od često korištenih operatora pretraživanja koje je autor osmislio kao primjere koji pojašnjavaju njihovu uporabu:

Operator “”: Upotrijebite navodnike (“”) kako biste dobili rezultate koji sadrže riječi u istom redoslijedu kao u navodnicima.

Na primjer, “dezinformacija”.

Operator* : Zvjezdicu (*) možete koristiti da zamijenite riječi ili slova koja nedostaju.

Primjerice, “dezinformacija je * informacija”.

Operator -: Ako koristite znak minus (-) s riječi iza sebe, možete isključiti određene riječi iz rezultata. Na primjer, “dezinformacija” - propaganda.

Operator stranica: Koristite ovaj operator kako biste dobili rezultate s određenih stranica ili domena. Na primjer, stranica s “dezinformacijama”: enisa.europa.eu.

Operator link: Pronađite stranice koje povezuju na određenu stranicu koristeći operator veza.

Na primjer, link “dezinformacije”: youtube.com.

Operator filetype: Tražite određeni tip datoteke pomoću ovog operatora.

Primjerice, “dezinformacije” filetype:pdf.

Operator intitle: Pronađite stranice koje sadrže određene riječi u naslovu.

Na primjer, intitle:”dezinformacije”.

Operator inurl: Pronađite stranice koje sadrže određene riječi u URL-u.

Na primjer, inurl:”dezinformacije”.

Operator intext: Pronađite stranice koje sadrže određene riječi unutar teksta na stranici.

Na primjer, intext:”dezinforrmacije”.

Također, možete koristiti prevodilačke usluge za prevođenje teksta s jednog jezika na drugi. Neki od popularnih prevoditelja uključuju Google prevoditelja (https://translate.google.com), Bing prevoditelja (https://www.bing.com/translator) i DeepL (https://www.deepl.com/translator).

Ako želite istovremeno pretraživati na dva jezika, preporučuje se korištenje alata poput https://2lingual.com.

Alati za provjeru i analizu - temeljeni na E-pošti

Provjera Valjanosti E-pošte Provjera e-pošte je proces kojim se utvrđuje je li adresa e-pošte stvarna i može li se na nju dostaviti poruka. Ovo je važno kako bismo izbjegli neželjenu poštu i poboljšali reputaciju pošiljatelja. Možete provjeriti valjanost e-pošte na stranicama poput https://tools.emailhippo.com i https://centralops.net/co.

Reputacija E-pošte Reputacija pošiljatelja e-pošte ocjena je koju davatelj internetskih usluga (ISP) dodjeljuje organizaciji koja šalje e-poštu. To igra ključnu ulogu u isporuci e-pošte. Što je reputacija viša, to je veća vjerojatnost da će ISP isporučiti e-poštu u poštanske sandučiće primatelja. Možete analizirati reputaciju adrese e-pošte na stranicama poput https://emailrep.io i https://easydmarc.com/tools/ip-domain-reputation-check.

Provjera na Crnoj Listi Kada organizacija šalje e-poštu, ISP provjerava adresu e-pošte ili domenu na crnoj listi, što je popis domena i IP adresa označenih kao izvor neželjene pošte. Ako je adresa na crnoj listi, e-pošta se smatra neželjenom. Možete provjeriti status adrese e-pošte na crnoj listi putem stranica kao što su https://mxtoolbox.com/blacklists.aspx i https://dnschecker.org/ip-blacklist-checker.php.

Prikupljanje Zaglavlja E-pošte Zaglavlje e-pošte, ili internetsko zaglavlje, sadrži metapodatke o svakoj e-pošti, uključujući pošiljatelja, primatelja, rutu, vremensku oznaku i druge informacije. Davatelji e-pošte koriste zaglavlja za provjeru autentičnosti pošiljatelja i isporuku e-pošte. Možete pristupiti zaglavljima e-pošte putem svojih klijenata za e-poštu ili putem stranica kao što su https://mxtoolbox.com/Public/Content/EmailHeaders.

Analiza Zaglavlja E-pošte Zaglavlje e-pošte pruža detaljne informacije o pošiljatelju, uključujući autentičnost, IP adresu pošiljatelja i druge važne podatke. Analizom zaglavlja možete otkriti informacije o pošiljatelju. Možete analizirati zaglavlja e-pošte na stranicama kao što su https://toolbox.googleapps.com/apps/messageheader i https://www.iptrackeronline.com/email-header-analysis.php.

Proces analize IP adrese počinje s identifikacijom same adrese te pronalaskom vlasnika IP adrese. Tijekom istraživanja, traže se dodatne korisne informacije poput geolokacije, vrste mreže i povijesti problema s prijevarama povezanim s tom adresom. Više detalja o IP adresama možete pronaći na web stranicama kao što su https://www.ipaddress.com/reverse-ip-lookup i https://securitytrails.com (potrebna pretplata). Privitak e-pošte predstavlja računalnu datoteku koja se šalje zajedno s porukom e-pošte. Može se priložiti jedna ili više datoteka uz poruku kako bi se podijelili dokumenti i slike. Format datoteke EML, koji je skraćenica za elektroničku poštu ili e-poštu, koristi se za pohranu e-pošte u standardnom formatu. Stručnjaci za kibernetičku sigurnost razvili su Advanced Attachment Analysis kako bi razdvojili privitke na pojedinačne dijelove, analizirali ih neovisno, istražili njihove veze i dali ocjenu sigurnosti.

Vrste Datoteka i Sigurnost Postoje različite vrste datoteka, a neke su manje sigurne od drugih. Primjerice, tekstualne datoteke obično su bezopasne (.txt), dok slikovne datoteke (.jpg) mogu sadržavati viruse. Komprimirane datoteke (.zip/.rar) također su rizične jer virusi postaju aktivni prilikom izdvajanja datoteka iz njih. Postoje i audio (.mp3) i video datoteke (.mpg/.mpeg/.avi/.wmv/mov/.ram) koje mogu sadržavati prijetnje, kao i izvršne datoteke (.exe) koje su često rizične. Najsigurniji formati datoteka za privitke e-pošte uključuju fotografije (JPEG, JPG, GIF, PNG), dokumente (PDF, DOC, DOCX, HTML, HTM, XLS, XLSX, TXT), video zapise (MP4, MOV, WMV), prezentacije (PPT, PPTX) i audio datoteke (M4A, MP3, WAV). Možete provjeriti vrstu privitka na stranicama kao što su https://www.checkfiletype.com/ i https://filext.com/file-extension/CHECK.

Analiza Malware-a Analiza zlonamjernog softvera koristi se za otkrivanje prijetnji i identifikaciju indikatora ugroženosti (IoC) kod novih varijanti zlonamjernog softvera. Sigurnosni alati i analitičari koriste te IoC-ove za prepoznavanje infekcija

zlonamjernim softverom. Analiza zlonamjernog softvera uključuje proučavanje jedinstvenih karakteristika, ciljeva, izvora i potencijalnih učinaka zlonamjernog koda, kao što su spyware, virusi, zlonamjerno oglašavanje i ransomware. Možete provesti analizu zlonamjernog softvera putem sigurnosnih postavki sustava Windows, a postupak uključuje tri faze: forenziku ponašanja, analizu koda i analizu pamćenja. Razlika između analize zlonamjernog softvera i otkrivanja zlonamjernog softvera leži u tome što analiza pomaže identificirati vrstu i varijantu zlonamjernog softvera te razumjeti kako se razlikuje od drugih vrsta, dok se otkrivanjem samo utvrđuje prisutnost zlonamjernog softvera na sustavu ili mreži. Možete provjeriti datoteke za zlonamjerni softver na stranicama poput https://www.virustotal.com/gui/home/upload i https://www.hybrid-analysis.com.

SOCMINT Alati

Alati za prikupljanje i analizu informacija iz društvenih medija (SOCMINT) predstavljaju moćno sredstvo za stjecanje dragocjenih uvida i inteligencije iz javno dostupnih podataka društvenih medija. SOCMINT, putem analize sadržaja na društvenim mrežama, može biti koristan u identificiranju i praćenju ekstremističkih skupina, nadziranju javnog raspoloženja i mišljenja te podršci istraga organa za provođenje zakona. Jedan od popularnih alata za pretraživanje društvenih mreža je dostupan na web stranici https://www.social-searcher.com/google-social-search.

Twitter Analytics, s druge strane, predstavlja snažan alat koji tvrtke mogu koristiti za detaljno praćenje učinka svojih Twitter kampanja putem analitičke nadzorne ploče. Za analizu i praćenje aktivnosti na Twitteru, mogu se koristiti alati kao što su https://socialbearing.com i https://tweetbeaver.com. Također, za vizualizaciju širenja informacija na društvenim mrežama, korisna je platforma https://hoaxy.osome.iu.edu, dok za stvarno-vremensko praćenje Twitter aktivnosti možete koristiti https://tweetdeck.twitter.com. Za preuzimanje video sadržaja s Twittera, koristan je alat dostupan na https://www.downloadtwittervideo.com.

Facebook Facebook predstavlja popularnu društvenu mrežu koja omogućava povezivanje i dijeljenje s obitelji i prijateljima putem interneta. Alat za pretraživanje indeksira sve informacije na Facebooku, uključujući objavljene fotografije i "lajkane" stvari, filtrirajući ih na one koje dijele korisnici s vama ili su javno objavljene. Besplatan Facebook Video Downloader omogućuje korisnicima da spreme svoje omiljene Facebook videozapise kako bi ih mogli gledati izvan mreže. Ovaj alat možete pronaći na https://fdown.net. Za pretraživanje profila i alate za analizu na Facebooku možete koristiti resurse kao što su https://www.sowsearch.info i https://inteltechniques.com/tools/Facebook.html.

LinkedIn LinkedIn je najveća svjetska profesionalna mreža na internetu, koja služi za pronalaženje poslovnih prilika, izgradnju profesionalnih odnosa i stjecanje potrebnih vještina za uspjeh u karijeri. Profil na LinkedInu omogućava korisnicima da istaknu

svoje iskustvo, vještine i obrazovanje te se povežu s drugim profesionalcima. Osim toga, LinkedIn nudi mogućnost organizacije izvanmrežnih događanja, sudjelovanja u grupama, pisanja članaka i više. Za pretragu profila možete koristiti https://recruitin.net, za alate za analitiku https://www.inlytics.io, a za preuzimanje video sadržaja s LinkedIna https://www.expertsphp.com/linkedin-video-downloader.

Instagram Instagram je popularna besplatna aplikacija za dijeljenje fotografija i videa dostupna na mobilnim uređajima. Korisnici mogu dijeliti svoje sadržaje s pratiteljima i pregledavati, komentirati i "lajkati" objave svojih prijatelja. Platforma također omogućava kreativcima dodavanje efekata poput filtara, glazbe i naljepnica te suradnju na sadržaju, uključujući i video duetne sadržaje. Za analizu profila na Instagramu možete iskoristiti https://inflact.com/tools/profile-analyzer, dok za alate za analizu i praćenje aktivnosti na Instagramu možete koristiti https://analisa.io (uz pretplatu). Preuzimanje videozapisa s Instagrama moguće je putem https://instadp.io.

TikTok TikTok je popularna aplikacija za društvene medije koja omogućava stvaranje, pregledavanje i dijeljenje kratkih videozapisa. Korisnici mogu dodavati različite efekte i surađivati na sadržaju. Aplikacija je poznata po svojim zaraznim kratkim videima i personaliziranim feedovima. Za pretraživanje TikToka možete koristiti https://www.osintcombine.com/tiktok-quick-search, za analitiku kanala https://socialblade.com/tiktok, a za preuzimanje video sadržaja https://ttdown.org.

YouTube YouTube je popularna platforma za dijeljenje videozapisa na internetu, omogućavajući gledateljima da pregledavaju, dijele i izrađuju vlastite videozapise. Platforma nudi bogat sadržaj, a analizu kanala i metapodatke možete pronaći na https://mattw.io/youtube-metadata i https://studio.youtube.com. Preuzimanje video sadržaja s YouTubea možete obaviti putem https://snapsave.io/en2.

Obrazovanje i dezinformacije

Pružanje obrazovanja o dezinformacijama u suvremenom svijetu od presudnog je značaja za proces donošenja odluke. Potaknite druge da razvijaju sposobnost prepoznavanja dezinformacija pružanjem alata i izvora za kritičko razmišljanje i provjeru informacija. Obrazovanje o dezinformacijama može pomoći ljudima da budu bolje informirani i otporni na širenje lažnih informacija. Komunicirajte ljubazno i učinkovito, te ako se susretnete s osobom koja širi dezinformacije, budite ljubazni i učinkoviti u komunikaciji. Pružite im provjerene informacije i objasnite im zašto je važno oslanjati se na pouzdane izvore. Vaš pristup može imati veći utjecaj na promjenu njihovog mišljenja nego napad ili osuda. Pametno dijeljenje provjerenih informacija ključno je u borbi protiv dezinformacija i izgradnji pouzdane informacijske zajednice. Budimo odgovorni u našem pristupu informacijama i pomozimo drugima da budu bolje informirani.

Metodologija istraživanja

Istraživanje je provedeno tijekom svibnja i lipnja 2023. godine, a imalo je za cilj – ispitati stavove, vjerovanja te navike i ponašanja vezana za dezinformacije na internetu kod studenata Veleučilišta kriminalistike i javne sigurnosti, te ispitati potencijalne prediktore tih ponašanja. U istraživanju su ispitane navike korištenja metoda za provjeru istinitosti informacija kod studenata Veleučilišta kriminalistike i javne sigurnosti.

Sudionici i postupak

U istraživanju koje smo proveli, sudjelovalo je 278 sudionika (63.3% M, 36.7% Ž) prosječne dobi 29.29 godina (Sd= 6.36). Svi sudionici bili su studenti Veleučilišta kriminalistike i javne sigurnosti (69.9% - Stručni studij kriminalistike, 30.1% - Specijalistički diplomski studij) od kojih 74.8% čine zaposlenici Ministarstva unutarnjih poslova. Od svih policijskih službenika u uzorku, prosječnog radnog staža u od 6.23 godine (Sd= 5.37), njih 23.4% radi na poslovima temeljne policije, 18% na kriminalističkim poslovima, 15.1% na poslovima granice, 8.6% u prometu te 5.1% u interventnoj jedinici policije.

Detaljni socio-demografski podaci prikazani su u sljedećoj tablici.

Sociodemografski podaci sudionika

Varijabla	**M**	**Sd**
Dob	29.29	6.36
Radni staž u MUP-u	6.23	5.37
		%
Spol	**m**	63.3
	ž	36.7
Razina studija kriminalistike	**Stručni studij**	71.9
	Specijalistički studij	28.1
Zaposlenik MUP-a	**Da**	74.8
	Ne	25.2
Vrsta poslova u policiji	**temeljna**	23.4
	kriminalistička	18.0
	granična	15.1
	prometna	8.6
	Interventna/specijalna	5.1
	upravni poslovi	2.2
	UPPS	1.4
	drugi poslovi	25.9

Provjera istinitosti/autentičnosti informacija

Correlations

		godina_ studija	dob	staž_mup	poznavanje_ engleskog	mjesto_ stanovanja	prosjek_ ocjena	Provjera istinitosti informacije COMP
godina_studija	r	1	.132*	.206**	.019	-.008	.021	.004
	Sig.		.029	.001	.756	.898	.740	.947
	N	274	274	273	262	274	255	274
dob	r	.132*	1	.694**	-.208**	.014	-.032	-.055
	Sig.	.029		.000	.001	.815	.605	.359
	N	274	278	277	265	278	259	278
staž_mup	r	.206**	.694**	1	-.298**	.005	-.004	-.051
	Sig.	.001	.000		.000	.940	.952	.400
	N	273	277	277	264	277	258	277
poznavanje_	r	.019	-.208**	-.298**	1	.031	-.008	.028
engleskog	Sig.	.756	.001	.000		.618	.899	.649
	N	262	265	264	265	265	249	265
mjesto_stanovanja	r	-.008	.014	.005	.031	1	-.089	.080
	Sig.	.898	.815	.940	.618		.151	.183
	N	274	278	277	265	278	259	278
prosjek_ocjena	r	.021	-.032	-.004	-.008	-.089	1	.007
	Sig.	.740	.605	.952	.899	.151		.913
	N	255	259	258	249	259	259	259
Provjera istinitosti	r	.004	-.055	-.051	.028	.080	.007	1
informacije COMP	Sig.	.947	.359	.400	.649	.183	.913	
	N	274	278	277	265	278	259	278

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Nij Nijedna soc-dem varijabla ne korelira značajno sa varijablom Provjera istinitosti/ autentičnosti informacija.

Iskustva sa sigurnošću i vjerojatnosti korištenja metoda za zaštitu sigurnosti

Correlations

		Žrtva/meta kibernetičkog napada COMP	Vjerojatnost korištenja metode za zaštitu sigurnosti COMP	Provjera istinitosti informacije COMP
Žrtva/meta kibernetičkog napada COMP	Pearson Correlation	1	-.199**	-.063
	Sig. (2-tailed)		.001	.294
	N	278	278	278
Vjerojatnost korištenja metode za zaštitu sigurnosti COMP	Pearson Correlation	-.199**	1	.410**
	Sig. (2-tailed)	.001		.000
	N	278	278	278
Provjera istinitosti informacije COMP	Pearson Correlation	-.063	.410**	1
	Sig. (2-tailed)	.294	.000	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Provjera istinitosti/autentičnosti informacija značajno pozitivno korelira sa vjerojatnošću korištenja metoda za zaštitu sigurnosti ($r=0.410$, $p<0.01$). Sudionici koji vjerojatnije koriste metode za provjera istinitosti/autentičnosti informacija također vjerojatnije koriste metode za zaštitu sigurnosti. Također, negativna iskustva sa sigurnošću na internetu negativno su značajno povezana sa vjerojatnošću korištenja metoda za zaštitu sigurnosti ($r=-0.199$, $p<0.01$), dakle osobe koje vjerojatnije koriste metode za zaštitu sigurnosti imaju manje negativnih iskustava sa sigurnošću na internetu. Negativna iskustva sa sigurnošću na internetu nisu povezana sa vjerojatnošću korištenja metoda za provjeru istinitosti/autentičnosti informacija**.**

Informiranost o dezinformacijama i percepcija informiranosti drugih ljudi o dezinformacijama

Correlations

		Informiran sam o dezinformacijama COMP	Ljudi su informirani o dezinformacijama COMP	Provjera istinitosti informacije COMP
Informiran sam o dezinformacijama COMP	Pearson Correlation	1	.035	.354**
	Sig. (2-tailed)		.562	.000
	N	278	278	278
Ljudi su informirani o dezinformacijama COMP	Pearson Correlation	.035	1	-.037
	Sig. (2-tailed)	.562		.535
	N	278	278	278
Provjera istinitosti informacije COMP	Pearson Correlation	.354**	-.037	1
	Sig. (2-tailed)	.000	.535	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Provjera istinitosti informacije pozitivno je značajno povezana sa informiranošću o dezinformacijama (r=0.354, p<0.01) – sudionici koji smatraju da su više informirani o dezinformacijama također vjerojatnije koriste metode provjere istinitosti informacije.

Percepcija učestalosti dezinformacija

Correlations

		Učestalost dezinformacija u medijima COMP	Učestalost dezinformacija na društvenim mrežama COMP	Provjera istinitosti informacije COMP
Učestalost dezinformacija u medijima COMP	Pearson Correlation	1	.547**	.181**
	Sig. (2-tailed)		.000	.002
	N	278	278	278
Učestalost dezinformacija na društvenim mrežama COMP	Pearson Correlation	.547**	1	.253**
	Sig. (2-tailed)	.000		.000
	N	278	278	278
Provjera istinitosti informacije COMP	Pearson Correlation	.181**	.253**	1
	Sig. (2-tailed)	.002	.000	
	N	278	278	278

**. Correlation is significant at the 0.01 level (2-tailed).

Provjera istinitosti informacije pozitivno je značajno povezana sa percepcijom učestalosti dezinformacija u medijima (r=0.181, p<0.01) te na društvenim mrežama (r=0.253, p<0.01). Sudionici koji smatraju da u medijima i na društvenim mrežama ima više dezinformacija također vjerojatnije koriste metode provjere istinitosti informacije. Očekivano, percepcija učestalosti dezinformacija u medijima i na društvenim mrežama pozitivno je značajno povezana (r=0.547, p<0.01).

Učestalost i količina korištenja društvenih mreža i internetski portala

Correlations

	23. Koliko često odlazite na društvene mreže?	24. Koliko vremena dnevno provodite na društvenim mrežama?	29. Koliko često posjećujete internetske portale?	30. Koliko vremena dnevno provodite na internetskim portalima?	31. Koliko često dijelite (share) sadržaj na društvenim mrežama?	32. Koliko često objavljujete vlastiti sadržaj na društvenim mrežama?	Provjera istinitosti informacije COMP
23. Koliko često odlazite na društvene mreže?	1	.955**	.138*	.121*	-.078	-.136*	.074
		.000	.021	.044	.196	.023	.217
	278	278	278	278	278	278	278
24. Koliko vremena dnevno provodite na društvenim mrežama?	.955**	1	.220**	.195**	-.073	-.133*	.071
	.000		.000	.001	.223	.027	.237
	278	278	278	278	278	278	278

29. Koliko često posjećujete internetske portale?	.138*	.220**	1	.913**	.174**	.137*	-.052
	0.21	.000		.000	.004	.022	.389
	278	278	278	278	278	278	278
30. Koliko vremena dnevno provodite na internetskim portalima?	.121*	.195**	.913**	1	.202**	.113	-.037
	.044	.001	.000		.001	.060	.542
	278	278	278	278	278	278	278
31. Koliko često dijelite (share) sadržaj na društvenim mrežama?	-0.78	-.073	.174**	.202**	1	.522**	-.040
	.196	.223	.004	.001		.000	.505
	278	278	278	278	278	278	278
32. Koliko često objavljujete vlastiti sadržaj na društvenim mrežama?	-.136*	-.133*	.137*	.113	.522**	1	-.081
	0.23	0.27	.022	.060	.000		.180
	278	278	278	278	278	278	278
Provjera istinitosti informacije COMP	-0.74	.071	-.052	-.037	-.040	-.081	1
	.217	.237	.389	.542	.505	.180	
	278	278	278	278	278	278	278

Nijedna varijabla učestalosti i količine korištenja društvenih mreža i internetskih portala ne korelira značajno sa varijablom provjere istinitosti informacije.

Diskusija

Rezultati provedenog istraživanja pokazuju da većina ispitanika (66.9%) smatra da je dovoljno informirana o opasnostima dezinformacija, te da lako raspoznaje dezinformacije od istine (55.4%) dok njih manje od polovice (48.9%) smatra da su dovoljno informirani o načinima raspoznavanja dezinformacija. Nadalje, muškarci značajno češće koriste metode za provjeru istinitosti informacija od žena ($t=2.674$, $df=276$, $p=0.008$), dok je regresijski model rezultirao sa dva najznačajnija prediktora: pojedinci koji vjerojatnije koriste metode za zaštitu vlastite privatnosti i sigurnosti na internetu ($\beta =0.7$, $p < .05$) te pojedinci koji smatraju da su bolje informirani o opasnostima i o načinima raspoznavanja dezinformacija ($\beta =0.106$, $p < .05$) češće koriste metode za provjeru istinitosti informacija ($R^2=0.551$, $F=168.821$, $p<0.001$). Daljnja analiza korelacija sugerira da oni pojedinci koji smatraju da dezinformacije imaju značajniji utjecaj na društvo te da su dezinformacije učestalije u medijima također češće koriste metode za provjeru istinitosti informacija.

Ishodi učenja

Na osnovu u radu prezentiranog pristupa, te provedenih istraživanja, mogli bi smo predložiti ishode učenja za kolegij koji bi u fokusu imao informacijsko komunikacijske tehnologije i njihovu zlouporabu putem stvaranja i širenja dezinformacija. Ishodi

učenja su ključni za stvaranje svijesti i kompetencija potrebnih za suočavanje s problemom dezinformacija u digitalnom dobu te zaštite kvalitete informacija i javnog diskursa. Razumijevanje pojma dezinformacije, gdje bi ishod učenja bio da polaznici razumiju što su dezinformacije i lažne vijesti, te kako se razlikuju od istinitih informacija. Prepoznavanje globalnog širenja dezinformacija, s ciljem da bi polaznici trebali biti osviješteni da su dezinformacije globalni problem koji utječe na društva diljem svijeta. Razumijevanje uloge digitalne tehnologije, gdje bi ishod učenja bio obuhvatiti razumijevanje kako digitalna tehnologija, uključujući društvene medije, olakšava širenje dezinformacija. Identifikacija aktera dezinformacija, gdje bi polaznici trebali prepoznati različite aktere koji šire dezinformacije, kao što su botovi, tvornice trolova i drugi. Razumijevanje društvenih aspekata dezinformacija, gdje bi ishod učenja uključivao razumijevanje kako dezinformacije utječu na društveni diskurs i demokraciju. Prepoznavanje potrebe za sustavnim pristupom, gdje bi polaznici trebali razumjeti potrebu za sustavnim pristupom suzbijanju dezinformacija na individualnoj i institucionalnoj razini. Razumijevanje teškoća u prepoznavanju dezinformacija, gdje bi ishod učenja obuhvatio osvješćivanje o tome koliko je teško ponekad prepoznati manipulirane vijesti, čak i za digitalno obrazovane osobe. Studija nad djecom u Finskoj, koju su proveli Vartiainen, Kahila, Tedre, Sointu i Valtonen, osim potrebe za dubljim razumijevanjem problematike dezinformacija kao zadaće obrazovnoga sustava sa nužnostima navedenima od strane većine ovdje navedenih autora, naglašava i potrebu izučavanja dezinformacija kroz kolegije koji se bave informacijsko komunikacijskim sadržajima i mehanizmima strojnog učenja, uključujući praćenje i profiliranje, podatkovni inženjering i oglašavanje temeljeno na psihometriji. S druge strane, neki autori, poput Farmera (Farmer, 2019) smatraju da bi ključnu ulogu u suočavanju s dezinformacijama trebali imati školski knjižničari. Svijest o pravnoj regulaciji digitalnih platformi također je važno uključiti kao očekivani ishod učenja, gdje bi polaznici trebali biti svjesni pitanja regulacije digitalnih platformi i njihovih napora za suzbijanje dezinformacija. Poznavanje alata za provjeru informacija, gdje bi ishod učenja uključivao poznavanje alata i tehnika za provjeru informacija, kao što su provjera izvora, analiza slika i video materijala te analiza metapodataka. Razumijevanje važnosti borbe protiv dezinformacija, gdje bi polaznici trebali razumjeti da rješavanje problema dezinformacija ima ključnu ulogu u zaštiti integriteta informacijske i komunikacijske infrastrukture te demokracije. Razumijevanje važnosti proširenja preglednika u zaštiti online rada. Prepoznavanje uloge proširenja preglednika u poboljšanju sigurnosti i funkcionalnosti preglednika. Shvaćanje kako proširenja preglednika mogu pomoći u borbi protiv dezinformacija i blokiranju oglasa. Poznavanje popularnih proširenja preglednika i njihovih značajki. Da mladi preferiraju informirati se putem društvenih mreža u odnosu na tradicionalne medije, potvrdilo je i najnovije istraživanje nad mladom meksičkom populacijom, koje je proveo Galarza-Molina i istraživanje nad mladom afričkom populacijom koje su proveli Camara, Banu i Abeck.

Prepoznavanje proširenja kao što su Adblock Plus, AdGuard i uBlock Origin. Razumijevanje različitih značajki tih proširenja, uključujući blokiranje oglasa i poboljšanu sigurnosnu funkcionalnost. Sposobnost odabira odgovarajućeg proširenja preglednika. Razumijevanje važnosti odabira pravog proširenja za svoje potrebe. Poznavanje kriterija za odabir proširenja, uključujući učinkovitost, lakoću korištenja i sigurnost. Poznavanje naprednih tehnika pretraživanja i operatera pretraživanja. Razumijevanje kako koristiti operatore pretraživanja za precizno filtriranje rezultata pretraživanja. Poznavanje operatora kao što su "", *, -, stranica, link, filetype, intitle, inurl i intext. Upotreba alata za provjeru i analizu e-pošte. Razumijevanje procesa provjere valjanosti e-pošte i njezine reputacije. Poznavanje alata za provjeru e-pošte na crnoj listi, prikupljanje zaglavlja e-pošte i analizu zaglavlja. Analiza sigurnosnih aspekata datoteka i zlonamjernog softvera. Razumijevanje različitih vrsta datoteka i njihove razine sigurnosti. Poznavanje postupka analize zlonamjernog softvera i kako identificirati potencijalne prijetnje. Upotreba SOCMINT alata za prikupljanje i analizu informacija s društvenih medija. Razumijevanje važnosti SOCMINT alata u analizi društvenih medija. Sposobnost korištenja alata za pretraživanje, analizu i preuzimanje sadržaja s društvenih medija kao što su Twitter, Facebook, LinkedIn, Instagram, TikTok i YouTube. Razumijevanje važnosti praćenja i analize online aktivnosti. Prepoznavanje svrhe praćenja online aktivnosti, uključujući praćenje performansi kampanja na društvenim mrežama. Sposobnost analize metapodataka i statistike društvenih medija. Ovi ishodi učenja pomažu stvoriti temeljno razumijevanje proširenja preglednika, tehnika pretraživanja, analize e-pošte, sigurnosnih aspekata datoteka, SOCMINT alata i praćenja online aktivnosti, što može biti korisno u online istraživanjima, zaštiti privatnosti i analizi informacija s društvenih medija.

Zaključak

Zaključno ovaj rad naglašava ozbiljnost problema dezinformacija u digitalnom dobu i potrebu za djelovanjem na različitim razinama kako bismo se suočili s ovim izazovom. Lažne vijesti i manipulacija informacijama su sveprisutni, a digitalne tehnologije i društvene mreže olakšavaju njihovo širenje. Različiti akteri, uključujući botove i tvornice trolova, koriste različite strategije za širenje dezinformacija, često ciljajući na emocionalne reakcije kako bi privukli pažnju.

Prepoznavanje problema dezinformacija treba biti prioritet na individualnoj i institucionalnoj razini. Sustavan pristup za suzbijanje dezinformacija uključuje provjeru vjerodostojnosti informacija, analizu izvora i autora te svijest o vlastitim pristranostima. Društvene mreže i digitalne platforme također treba staviti pod povećani nadzor i regulaciju kako bi se smanjilo širenje dezinformacija.

Također, u radu se ističe važnost primjene sustavnog pristupa provjeri informacija uz korištenje različitih online alata i tehnika, uključujući analizu slika, analizu e-pošte

i analizu zlonamjernog softvera. Socijalni medijski alati za prikupljanje informacija također su istaknuti kao moćno sredstvo za analizu društvenih medija.

Uz to, proširenja preglednika igraju ključnu ulogu u zaštiti online okoline i borbi protiv dezinformacija, a neka od njih su prepoznata kao posebno učinkovita u blokiranju oglasa i zaštiti od različitih prijetnji.

Sve navedeno, a posebice provedenog istraživanja ukazuje na potrebu za obrazovanjem i osvješćivanjem javnosti o dezinformacijama te razvojem i primjenom alata i tehnika koje će pomoći u zaštiti informacijske i komunikacijske infrastrukture te promicanju zdravog javnog diskursa i demokracije u digitalnom dobu.

LITERATURA

1. Antoliš K., Pačelat J. (2023). *Razotkrivanje dezinformacija*, Medijska istraživanja, 2023, (u tisku)
2. Astuti, S. I., Giri, L., & Hidayah, N. (2020). *Video Web Drama Series for Combating Disinformation an Innovation in Reaching and Teaching Audience*. Aspiration Journal, 1(1), 1–31. https://doi.org/10.56353/aspiration.v1i1.9
3. Bertelsmann Stiftung (2023). *Europeans want decisive action against disinformation on the Internet,* https://techxplore.com/news/2023-08-europeans-decisive-action-disinformation-internet.html
4. Erasmus + KA220-HED - *Cooperation partnerships in higher education* (2022./2025.)
5. Farmer, L. S. (2019). *News Literacy and Fake News Curriculum: School Librarians' Perceptions of Pedagogical Practices*. Journal of Media Literacy Education, 11(3), 1-11.
6. Galarza-Molina, R. (2023). *Youth in the face of disinformation: A qualitative exploration of Mexican college students' attitudes, motivations, and abilities around false news*. Communication & Society, 97-113.
7. Howard, P. N., Neudert, L. M., Prakash, N., & Vosloo, S. (2021). *Digital misinformation/disinformation and children*. UNICEF. Retrieved on February, 20, 2021.
8. Ismael Alvarez, Marcin Golizda, Istvan Heredi, Joseph Jones, Gianluigi Me, Ioan-Cosmin Mihai, Peter Pots, Ionuț Stoica, Cătălin Zetu: *The Osint For Analyzing Fake News Guide*
9. Pérez-Escolar, M., Ordóñez-Olmedo, E., & Alcaide-Pulido, P. (2021). *Fact-checking skills and project-based learning about infodemic and disinformation*. Thinking Skills and Creativity, 41, 100887.
10. Richard Rogers , Sabine Niederer, *Politika manipulacije društvenim medijima*, Amsterdam University Press , 23. listopada 2020.

11. Tynes, B. M., Stewart, A., Hamilton, M., & Willis, H. A. (2021). *From Google Searches to Russian Disinformation: Adolescent Critical Race Digital Literacy Needs and Skills*. International Journal of Multicultural Education, 23(1), 110-130.
12. UNHCR (2021). *Using Social Media in Community Based Protection.* A Guide. https://www.unhcr.org/innovation/wp-content/uploads/2021/01/Using-Social-Media-in-CBP.pdf
13. Van der Linden S, Roozenbeek J, Compton J. (2000). *Inoculating Against Fake News About COVID-19*. Front Psychol.
14. Vartiainen, H., Kahila, J., Tedre, M., Sointu, E., & Valtonen, T. (2023). More than fabricated news reports: Children's perspectives and experiences of fake news. *Journal of Media Literacy Education*, 15(2), 17-30.

KRUNOSLAV ANTOLIŠ*

DISINFORMATION IN THE DIGITAL AGE

Abstract

The paper investigates the emergence of disinformation and fake news in the modern digital environment. It emphasises that misinformers use advanced technology, including bots, troll factories and targeted advertising, to manipulate information on social networks. Disinformation represents a serious threat to democracy and requires a systematic approach to their suppression.

The paper also points out that even digitally literate people sometimes find it difficult to recognise manipulated news. Therefore, the importance of recognising disinformation at the individual and institutional level is emphasised, and it is recommended to check the content, author, source, date and other elements before sharing information. The paper offers a number of tools for analysing video material, images and web pages, including tools for checking credibility, geolocation, plagiarism detection, similarity analysis and other information analysis techniques. It also highlights the importance of protecting privacy and security online through virtual machines, VPNs and other tools. Furthermore, the paper emphasises the need for a systematic approach in the fight against misinformation in order to protect the integrity of the information and communication infrastructure because the preservation of information is essential for public trust and the health of democracy.

The paper also discusses ad-blocking browser extensions like Adblock Plus, AdGuard, and uBlock Origin, highlighting their various features. It also offers advanced search techniques, including search operators to filter search results precisely. In addition, the paper addresses email analysis, file security aspects and social media information collection and analysis (SOCMINT) tools. The importance of monitoring online activity and social media metadata analysis is emphasised. Through all these topics, the paper provides valuable information for online research, privacy protection and analysis of social media information in the digital age.

Keywords: *misinformation, digital age, social networks, metadata, education.*

* Prof. Krunoslav Antoliš, University of Applied Science in Criminal Investigation and Public Security, Zagreb