CIVIC RESILIENCE INITIATIVE

Disinformation Tool-kit

Mākslīgā intelekta izrāviens: rokasgrāmata cīņai ar dezinformāciju

Izdevuma izdošanu sponsorē Google

Vairāk par mums!

www.cri.lt

CIVIC RESILIENCE INITIATIVE

@CivicResilience

@CRI

@civicresilienceinitiative

Šis izdevums ir sagatavots sadarbībā ar Baltijas drošības fondu, Igaunijas Nacionālo aizsardzības un drošības apziņas centru, un to apmaksā Google.

Mākslīgā intelekta izrāviens: rokasgrāmata cīņai ar dezinformāciju.

Pēdējo desmit gadu laikā digitālo mediju izplatība turpina pieaugt. Katru dienu mēs saskaramies ar arvien lielāku informācijas plūsmu daudzumu, kas nāk no dažādiem komunikācijas kanāliem: sociālajiem tīkliem, emuāriem, vietnēm, tradicionālajiem medijiem vai citām elektroniskām publikācijām.

Šāda informācijas plūsmu dažādība ļauj viegli izvēlēties avotu, kas vislabāk atspoguļo mūsu intereses un politiskos vai sociālos uzskatus. Pieaugot laikam, ko pavadam sociālajos tīklos, arvien vairāk cilvēku tos izvēlas par savu galveno informācijas avotu, bieži vien nenovērtējot tajos pastāvošos draudus. Ātra un ērta informācijas izplatīšana sociālajos tīklos rada ideālus apstākļus ātrai dezinformācijas izplatībai.

Pašreizējā mākslīgā intelekta (MI) popularitāte un uz to balstītie rīki sniedz plašas iespējas izplatīt dezinformāciju un ļaunprātīgu informāciju. Video un audio viltojumi, kuru izplatīšanu atvieglo lietu internets, var radīt būtisku kaitējumu sabiedrībai, izplatot viltus ziņas un tādējādi graujot iedzīvotāju uzticību plašsaziņas līdzekļiem. Tomēr lielajam ļaunprātīgo provokāciju potenciālam ir iespējams arī pretoties. Kad esam apguvuši lietu internetu (internet of things, IoT), šīs tehnoloģijas unikālās īpašības var izmantot arī cīņā pret dezinformāciju. Baltijas valstis ir pastāvīgs mērķis ļaunprātīgiem centieniem izplatīt nepatiesu informāciju, cenšoties aktīvi iedragāt valstu uzticamību.

Šādi centieni vairo neuzticību vietējai valdībai, mūsu partneriem NATO un Eiropas Savienībā un nepārtraukti cenšas demotivēt iedzīvotājus aktīvi piedalīties valsts pārvaldībā.

Lai gan profesionāļi paveic daudz, atmaskojot nepatiesus stāstus, bieži vien kaitējums tiek nodarīts jau uzreiz pēc dezinformācijas izplatīšanas.

Lai izglītotu sabiedrību nebeidzamajā cīņā pret dezinformāciju, Lietuvā 2019. gadā tika nodibināta Pilsoniskās izturētspējas iniciatīva (PII).

Organizācija sadarbojās ar dezinformācijas un mediju ekspertiem un nāca klajā ar ideju izstrādāt praktisku rokasgrāmatu „MI izrāviens: rokasgrāmata cīņai pret dezinformāciju.".

Šajā dezinformācijas identificēšanas rīku komplektā ir sniegts vienkāršs ceļvedis informācijas pārbaudes metodēm.

Mēs ceram, ka šī publikācija palīdzēs Jums viegli izveidot ieradumu pārbaudīt lasīto ziņu avotu un tiem pievienoto fotoattēlu un video autentiskumu.

PII komanda mērķē kļūt par galveno katalizatoru Baltijas reģionā, lai stiprinātu mūsu sabiedrību digitālo noturību.

"Pilsoniskās izturētspējas iniciatīvas" komanda

Šajā praktiskajā dezinformācijas rokasgrāmatā ir sniegti pamata rīki, kas Jums palīdzēs:

- pārbaudīt, vai informācija internetā ir īsta vai viltota;
- aprast, kā darbojas lietu internets un kā atpazīt attēlus, kuri manipulēti ar MI;
- identificēt troļļus un viltotus sociālo tīklu kontus;
- atpazīt viltotus attēlus un video internetā;
- rīkoties, ja redzat dezinformāciju;
- brīdināt citus par sociālajos tīklos izplatītiem meliem.

Šīs rokasgrāmatas mērķis ir veicināt digitālās noturības palielināšanu un informētības palielināšanu par drošību un nepieciešamību ievērot modrību informācijas telpā. Šīs publikācijas mērķis ir sniegt informāciju, lai palīdzētu skolēniem, studentiem un plašākai sabiedrībai stiprināt viņu digitālo pratību un noturību pret mānīšanu un nepatiesu informāciju.

Šis izdevums ir sagatavots sadarbībā ar Baltijas drošības fondu, Igaunijas Nacionālo aizsardzības un drošības apziņas centru, un to apmaksā Google.

Ir daudz dažādu viltus ziņu veidu:

Dezinformācija

Informācija, kas ir nepatiesa un tīši izstrādāta, lai kaitētu indivīdam, sociālajai grupai, organizācijai vai valstij.

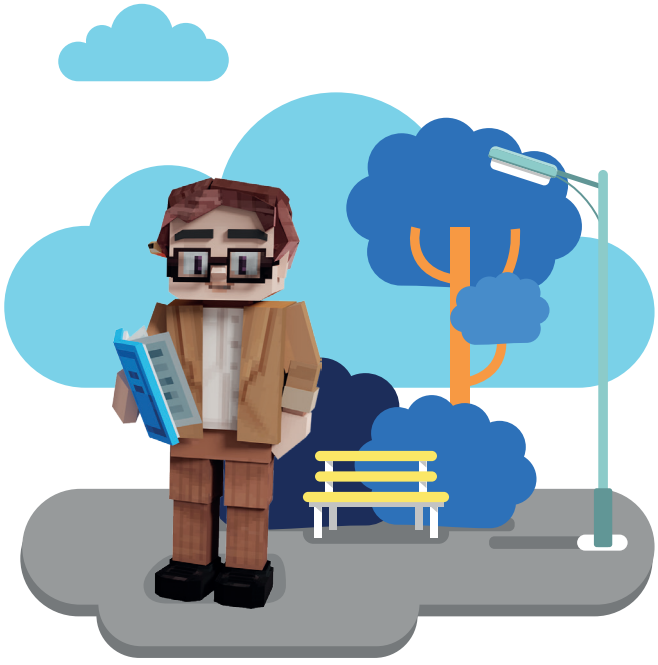
Viltus ziņas

Informācija, kas ir nepatiesa, bet nav izveidota ar nolūku nodarīt kaitējumu.

Ļaunprātīga informācija

Informācija, kas ir balstīta uz īstenību un tiek izmantota, lai nodarītu kaitējumu personai, organizācijai vai valstij.

Visi trīs informācijas veidi ir bīstami, jo tie ceļo tālu un ātri gluži kā vīrusi: tas notiek, ja daudz cilvēku un pat organizācijas atkārtoti publicē šos stāstus, jo tie šķiet interesanti un sensacionāli, par tiem īpaši nedomājot.



Identifikācija:

kā pārbaudīt ziņas vai ziņas?

Lasāt skandalozu ziņu ar tēmu vai saturu, kas izklausās neticami? Pārdomājiet lasīto un pārbaudiet informācijas ticamību. Kas Jums jādara?

Tālāk ir norādītas piecas vienkāršas darbības, kā pārbaudīt informāciju.

1. Novērtējiet avotu.	Izpētiet vietni vai sociālo mediju kontu. Padomājiet par to, kas varētu būt aiz ziņu izplatīšanas un kāds bija stāsta mērķis.
2. Izlasiet virs virsraksta.	Stāstu virsraksti var būt skandalozi, un tos izmanto, lai piesaistītu klikšķus un veicinātu dalīšanos. Ja iedziļinieties stāstā, var izrādīties, ka virsrakstā minētie apgalvojumi nav patiesi.
3. Iepazīstieties ar autoru.	Vai autors ir uzticams cilvēks? Vai nosauktais autors vispār pastāv?
4. Vai avoti apstiprina stāstu?	Bieži vien viltus ziņās nav saišu, ko varētu izmantot, lai pārbaudītu faktus. Ja stāstā ir atsauces uz avotiem, noklikšķiniet uz tiem. Var izrādīties, ka sākotnējais vēstījums ir izpušķots vai tā nozīme ir pārveidota.
5. Pārbaudiet datumu.	Veco ziņu atkārtota publicēšana nenozīmē, ka tās joprojām ir aktuālas.

Papildu padomi:

Izvēlieties drošu un uzticamu informāciju.

Ziņām latviešu valodā izmantojiet lielākos portālus, piemēram, LSM, DELFI, TVNET un tiem līdzīgus. Mazākus portālus var būt vieglāk ietekmēt, lai iegādātos noteiktu saturu, jo ir mazāki cilvēkresursi un finanšu resursi, tiek algoti mazāk žurnālistu, kas pārbauda informācijas ticamību, un tie var būt neaizsargātāki pret kiberuzbrukumiem un uzlaušanu.

Rūpīgi filtrējiet informāciju, kas nāk no ārvalstu portāliem vai sociālo tīklu grupām:

• Jūsu avotiem jābūt pietiekamam sekotāju skaitam. Pretējā gadījumā meklējiet, kurš vēl ir publicējis to pašu informāciju, un filtrējiet šos avotus atkārtoti.

• Ja apkopojat informāciju platformās X (agrāk pazīstama kā Twitter), TikTok vai YouTube, komentāri ir jāiespējo uzticamos kanālos. Uzticamākiem ierakstiem būs vairāk nekā viens komentārs, starp ierakstiem būs lielākas laika atstarpes, un šie ieraksti nebūs veidoti pēc standartizēta parauga. Ja minētās pazīmes neparādās, komentāri var būt nākuši no troļļiem vai robotiem.

• Avotos nedrīkst būt saites uz Krievijas valdības uzturētiem vai atbalstošiem portāliem (Sputnik, PBK, Rossija 24 un citiem). Lai gan šo portālu publicētajās ziņās var būt kāda patiesība, informatīvā kara kontekstā nav vērts riskēt ticēt Krievijas ziņu avotiem, ja vien tos neapstiprina arī Latvijas vai tās ārvalstu partneru portāli.

• Informācijai, kas ir sensacionāla, vienmēr jābūt balstītai uz uzticamiem avotiem. Ja internetā redzat jaunākās ziņas, pārliecinieties, vai jaunāko ziņu avotā ir minēti arī savi avoti. Ja tā nav, varat to pārbaudīt, izmantojot Google:

1) Pievienojiet pēdiņas svarīgākajiem atslēgvārdiem no ziņas vai raksta, ko lasāt, un ierakstiet tos Google meklētājā.

2) Noklikšķiniet uz pogas "Rīki" meklēšanas lodziņa labajā malā un izvēlieties, lai parādītu jaunāko.

3) Vēlreiz pārbaudiet avotus atbilstoši iepriekš minētajiem kritērijiem.

• Pajautājiet sev, vai šim avotam patiešām piemīt pierādījumi un analīze. Jautājiet, no kādas perspektīvas tiek pasniegtas ziņas? Vai varētu būt tā, ka ziņotie notikumi ir nepatiesi un tiek mēģināts manipulēt ar lasītāju iztēli un emocijām?

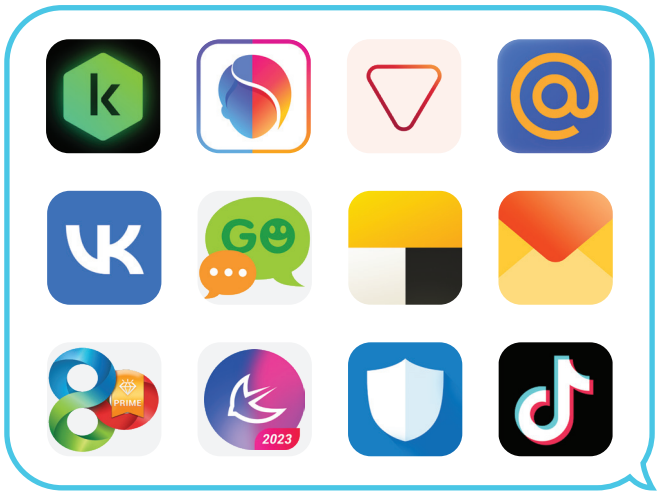
Visbeidzot, kad redzat sensacionālu ziņu kādā no mūsu valsts iestādes (piemēram, Ministru kabineta, Ārlietu ministrijas, u.c.) vietnēm, apmeklējiet atzītu ziņu portālu. Viens no informatīvā kara instrumentiem ir valdības vietņu uzlaušana un maldinošas informācijas izplatīšana tajās. Ja mūsu valsts iestāžu mājaslapas tiks uzlauztas, mediji noteikti par to ziņos. Tad mums nevajadzētu ticēt viņu publicētajai informācijai. Dažos gadījumos uzlaušana nav nepieciešama, un var tikt izmantotas viltotas vietņu adreses. Piemēram, interneta domēnu '.lv' aizstājot ar '.com', vai, gudrāk, '.lv' ar '.iv' (i, nevis l). Šādus trikus ir grūti pamanīt, tāpēc vienmēr pārbaudiet, vai adreses rindiņa tiešām izskatās tā, kā vajadzētu.

Piedāvājiet uzticamus informācijas avotus ne tikai saviem vecākiem, bet arī vecvecākiem.

Vai jūsu ģimenes locekļi skatās Krievijas televīziju? Militārā informācija pēdējos gados ir bijusi viena no populārākajām un apspriestākajām tēmām Krievijas televīzijas kanālos. Saprotams, ka daudziem mūsu vecākiem vai vecvecākiem krievu valoda ir galvenā un iecienītākā svešvaloda. Tāpēc mēs iesakām jūsu ģimenes locekļiem instalēt Netflix vai citu straumēšanas platformu, kas ietver krievu valodā tulkotu saturu. Tā kā Krievijas televīzija ir veidota tā, lai padarītu skatītāju apātisku pret informāciju, pārejai uz mājas kinoteātra platformu nevajadzētu būt sarežģītai.

Atinstalējiet Krievijas un Ķīnas izcelsmes lietotnes.

Atinstalējiet no saviem tālruņiem visas Krievijā ražotās vai tās potenciālo sabiedroto, piemēram, Ķīnas, lietotnes. Lietotnēm ir dažādas piekļuves Jūsu datiem vai atrašanās vietai, ko var izmantot pret Jums vai nu dezinformācijas izplatīšanai, vai militārās darbībās. Populārākās lietotnes ir: Kaspersky Antivirus, CheckScan, FaceApp, MyPocket, Mail.ru, Vkontakte, Go SMS Pro, Yandex Taxi, Yandex Mail, Go Launcher, APUS Launcher, Security Master un pat TikTok.



Ģeneratīvais mākslīgais intelekts (MI)

Ģeneratīvais MI ir saistīts ar mākslīgā intelekta modeļiem, kas var ģenerēt tādu saturu kā attēli, teksts, mūzika utt. Ģeneratīvā MI piemēri ietver labi zināmus modeļus, piemēram, ChatGPT, DALL-E un citus, kuros mēs varam viegli ievadīt datus. teksta vaicājumus un pretī saņem ģenerētu tekstu vai attēlus.

Lielo valodu modeļi (LVM) ir ģeneratīvā MI veids, kas var saprast, atpazīt, kontekstualizēt un ģenerēt tekstu. Lai LVM varētu veikt savus uzdevumus, ir jāapmāca modeļi, un šai apmācībai ir nepieciešams ievērojams teksta datu apjoms. Parasti datus iegūst, lasot atvērtā pirmkoda tekstu no interneta un pārveidojot tos apmācības nolūkos.

Valodu modeļus bieži izmanto, lai atbildētu uz jautājumiem, uz kuriem mēs nezinām atbildi, ģenerētu rakstītu tekstu, kad mums nav laika sagatavoties, vai pat rakstītu programmēšanas kodu, kad mēs nepārvaldām programmēšanas valodas. Tas ir lielisks rīks informācijas iegūšanai vai īsa satura izveidei, kura izveide pretējā gadījumā prasītu ievērojamu laiku un pūles.

Tomēr LVM tiek izmantoti ne tikai pozitīviem mērķiem, bet arī ļauj kibernoziedzniekiem daudz efektīvāk veikt kiberuzbrukumus:

1. Sociālā inženierija

LVM var izveidot izcilu tekstu jebkurā valodā, un šis teksts būs precīzāks nekā tulkojumi, kas veikti, izmantojot programmu "Google Translate". Teksts būs kvalitatīvs, ar nelielām kļūdām vai bez kļūdām. Tāpēc kibernoziedznieks var nezināt sava izvēlētā upura valodu, taču joprojām var rakstīt tekstu, kas mēģina pārliecināt upuri dot naudu vai noklikšķināt uz saites, kas mēģina piespiest viņu sniegt pieteikšanās informāciju. LVM rezultātā ļaunprātīgi e-pasta ziņojumi, ziņas un īsziņas būs kvalitatīvākas, un tos būs grūtāk identificēt kā krāpnieciskus. Ir īpaši valodu modeļi, kas īpaši izstrādāti šādu maldinošu ziņojumu ģenerēšanai.

2. Dezinformācijas izplatīšana

LVM programmu ģenerētā atbilde ne vienmēr ir precīza un var neatspoguļot realitāti, kā rezultātā lietotāji tiek maldināti, un neprecīzas vai nepareizas atbildes saņemšana var sākt izplatīties lietotāju sociālajās aprindās. Turklāt modeļi mācās no lietotāju jautājumiem un lietotāju sniegtajiem paskaidrojumiem, tāpēc modelis var uzzināt nepareizus "faktus" un parādīt tos kā precīzus citiem, veicinot dezinformācijas izplatīšanos.

Ģeneratīvais mākslīgais intelekts

Kā atpazīt tekstu, ko ģenerē LVM:

Pašlaik nav neviena rīka, kas varētu nekļūdīgi noteikt, vai teksts ir vai nav rakstīts ar mākslīgo intelektu. Pašlaik visprecīzākais atpazīšanas rīks ir cilvēka smadzenes.

Piemēram, zemāk esošais teksts ir rakstīts ar ChatGPT palīdzību. Vai pamanīsit tajā kļūdas?

Cienītais lietotāj!

Es ceru, ka esat pie labas veselības, saņemot šo vēstuli. Es rakstu, lai pievērstu jūsu uzmanību tam, cik svarīgi ir pabeigt reģistrācijas/pieteikšanās procesu mūsu platformā.

Kā daļu no mūsu apņemšanās nodrošināt jums nevainojamu pieredzi, mēs lūdzam pabeigt reģistrāciju vai pieteikties savā kontā pēc iespējas ātrāk. Tas ne tikai nodrošinās jūsu konta drošību, bet arī nodrošinās piekļuvi visam mūsu platformā pieejamo funkciju un priekšrocību klāstam.

Lai pabeigtu reģistrācijas/pieteikšanās procesu, lūdzu, sekojiet tālāk norādītajai saitei: Pieteikšanās saite

Ja rodas grūtības vai rodas jautājumi, lūdzu, sazinieties ar mūsu atbalsta komandu.

Pateicamies par sadarbību, un mēs ceram jūs apkalpot.

Šajā īsajā tekstā ir daži apgabali, kas izskatās aizdomīgi:
• Pirmais teikums neizklausās dabiski, un mūsdienās reti kad tiek saņemts šāds e-pastu ar tādu sākumu. Parasti šāds sākums liek domāt, ka teksts ir ticis ģenerēts.
• Arī pirmā rindkopa ir rakstīta pirmajā personā vienskaitlī (“es”), bet pārējais teksts ir rakstīts no daudzskaitlī (“mēs”), kas arī izskatās aizdomīgi.

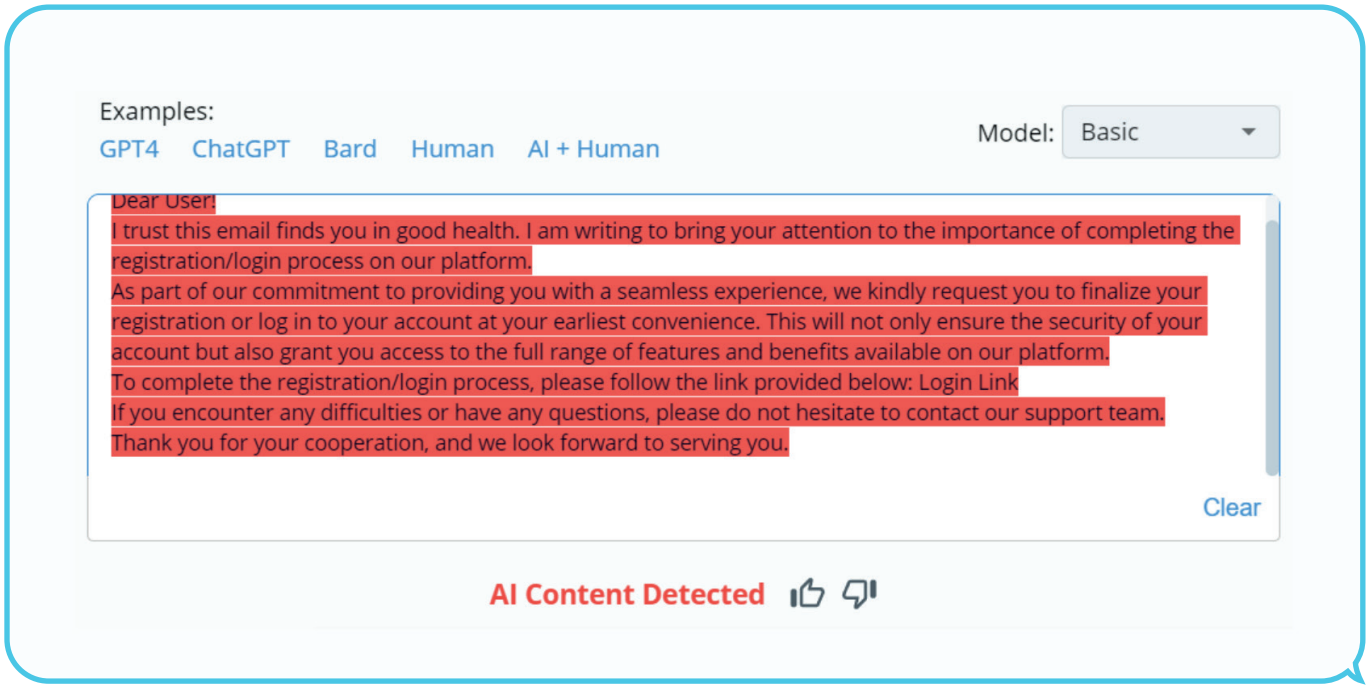
Tātad šis piemērs ilustrē, ka mākslīgais intelekts, ģenerējot tekstu, izmanto frāzes, kas ir biežāk sastopamas automātiski ģenerētā tekstā, un nekonsekventais vietniekvārdu lietojums rada jautājumus. Citas norādes var būt saistītas ar nepareizu locījumu lietošanu vai teikuma struktūras kļūdām. Turklāt, valodas kultūra un stils var atklāt mākslīgā intelekta darbību, pat ja tekstā nav kļūdu.

Tiešsaistē ir vairākas vietnes, kas mēģina noteikt, vai tekstu ģenerē mākslīgais intelekts vai nē. Lai saprastu, kā automatizētie rīki mēģina noteikt, vai tekstu ir uzrakstījis MI, mums ir jāatgriežas pie teksta ģenerēšanas pamatiem.

Vienkāršotā nozīmē tekstu ģenerējošie modeļi mēģina paredzēt nākamo piemērotāko vārdu teikumā, kas padara modeļus paredzamus. Jo vairāk datu tika izmantots modeļa apmācīšanai, jo labāk MI var uzminēt nākamo vārdu. Daži automatizēti noteikšanas rīki mēģina noteikt, vai vārdu secība teikumā ir statistiski optimāla, norādot, ka tekstu ir rakstījis MI. Tikmēr citi rīki iesaistās apgrieztā procesā, aprēķina varbūtību, ka tekstu ir uzrakstījis cilvēks, analizējot cilvēka rakstīšanas struktūras.

Tālāk ir sniegti daži automatizētu rīku piemēri. Rīkiem ir lauks, kurā varat iekopēt aizdomīgu tekstu. Pēc noklikšķināšanas uz analīzes pogas rīks parasti nodrošina varbūtības rādītāju, cik iespējams, ka tekstu ģenerējis MI. Daži rīki izcels teksta daļas, kuras, iespējams, ir ģenerētas, nevis rakstījis cilvēks.

Copyleaks



Zerogpt

Your Text is AI/GPT Generated

98.45%
AI GPT*

Dear User!

I trust this email finds you in good health. I am writing to bring your attention to the importance of completing the registration/login process on our platform.

As part of our commitment to providing you with a seamless experience, we kindly request you to finalize your registration or log in to your account at your earliest convenience. This will not only ensure the security of your account but also grant you access to the full range of features and benefits available on our platform.

To complete the registration/login process, please follow the link provided below: Login Link

If you encounter any difficulties or have any questions, please do not hesitate to contact our support team.

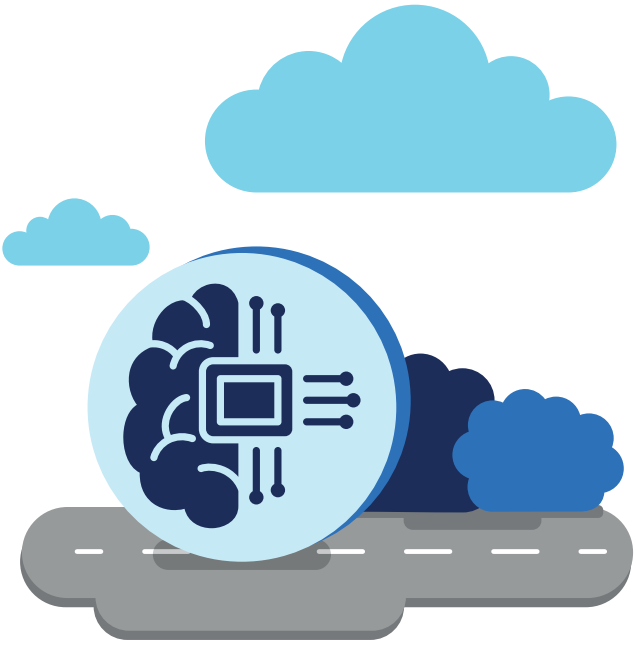
Thank you for your cooperation, and we look forward to serving you.

Highlighted text is suspected to be most likely generated by AI*
774 Characters
129 Words

Writer

Gptzero

Ilm



Informācijas (teksta) pārbaude

Kā pārbaudīt, vai teksta informācija ir patiesa?

Iegūglē! Iegūglē! Iegūglē!

Meklētājprogrammas, piemēram, Google, ir Jūsu labākie draugi cīņā pret dezinformāciju. Tās palīdz pārbaudīt visu informāciju pārlūkprogrammā, lai noskaidrotu, vai tā ir patiesa vai nepatiesa.

Meklējot izmantojiet atslēgvārdus, kurus varat identificēt, pamatojoties uz interesējošo informāciju, lai varētu uzzināt, vai interesējošos jaunumus ziņo ticami avoti. Ja sociālajos tīklos redzat aizdomīgu informāciju, pastāv liela iespēja, ka kāds jau strādā, lai atmaskotu nepatieso informāciju un atklātu patiesību.

Mums ir lielas priekšrocības cīņā pret dezinformāciju, jo, ja mēs varam veiksmīgi identificēt atslēgvārdus, mēs varam arī pārbaudīt nedigitālo informāciju un tādējādi novērtēt informāciju, kas pie mums nonāk no dažādiem avotiem. Ir svarīgi uzsvērt, ka meklētājprogrammas izmantošana ļaus jums atrast uzticamu avotu ar tādu pašu saturu, ko mēģināt pārbaudīt, taču vispirms pārliecinieties, vai avots ir ticams.

Kā pārbaudīt?

1. Identificējiet atslēgvārdus, kas vislabāk apraksta Jūsu meklēto informāciju.
2. Izmantojiet kādu no pieejamajām meklētājprogrammām, lai meklētu to pašu informāciju.
3. Izvēlieties filtrēt avotus pēc „Ziņām" un jaunākajām ziņām, kas publicētas pēdējās stundas vai dienas laikā.
4. Identificējiet uzticamus avotus un pārbaudiet informāciju.

Galvenie noteikumi, kas jāatceras:

• Informācijas meklēšana Google tīklā ir labs pirmais solis informācijas pārbaudei.

• Neatkarīgi no tā, kādu informāciju vēlaties pārbaudīt (teksts, fotoattēli vai videoklipi), Google meklēšana var darboties labi un būt efektīva.

• Vissvarīgākais ir izmantot atslēgvārdus, lai Jūs varētu atrast meklēto informāciju uzticamā avotā.

Lai efektīvāk izmantotu Google meklēšanu:

1) Izmantojiet pamata Google Dorking trikus, t.i., ja meklējat frāzi, ievietojiet to pēdiņās („...“ vai „....“).

2) Ja jūsu meklēšanas rezultātos ir ļoti populārs atslēgvārds, ievietojiet tam blakus mīnusa zīmi (-), lai tas neparādītos meklēšanas rezultātos.

3) Ja nezināt precīzu vārda pareizrakstību vai precīzu skaitli vai datumu, varat pievienot „*“ kā aizstājējzīmi, lai aizstātu trūkstošo burtu vārdā, veselā vārdā, ciparā vai datumā.

• Ja jūs runājat svešvalodās, varat to izmantot. Meklējiet, ko avoti kaimiņvalstīs vai visā reģionā saka par jaunumiem, kas jūs interesē.

• Ja labi runājat tikai vienā valodā, saņemiet palīdzību no kāda, kuram uzticaties, kurš var pārbaudīt attiecīgo informāciju citās valodās. Vēlāk pārrunājiet, kā interesējošā informācija tiek pasniegta citās valodu telpās. Šāda prakse var bagātināt gan jūsu, gan Jums uzticamās personas zināšanas.

Noderīgi rīki:

Google

Bing

Yandex

(PII atgādina: esiet piesardzīgs, šī ir vietne no Krievijas, tāpēc izmantojiet papildu drošības pasākumus savā datorā. Cik zināms, vietne ir droša lietošanai, taču iesakām neizmantot mobilo lietotni - tā prasa piekļuvi personas datiem instalēšanas laikā.)

Attēla pārbaude

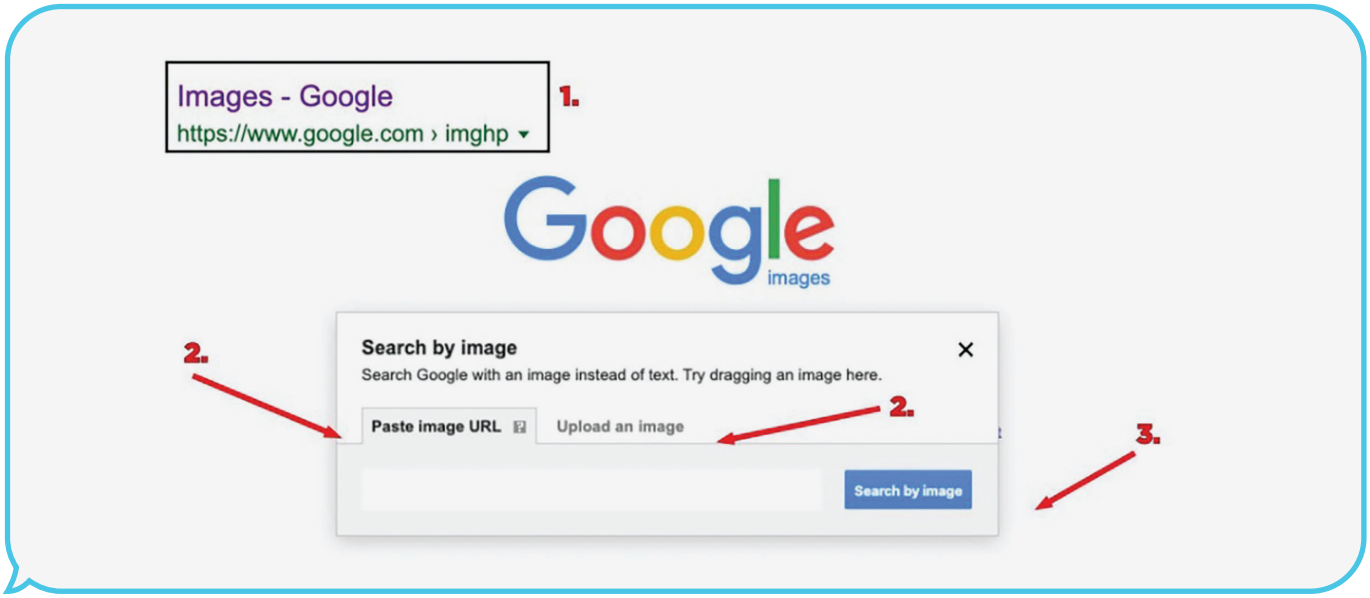
Kā pārbaudīt, vai vizuālā informācija ir patiesa?

Reversā attēlu meklēšana:

Attēlu pārveidošana – iepriekšējā attēla ievietošana un apgalvojums, ka tas uzņemts nesen – joprojām ir viena no galvenajām problēmām dezinformācijas telpā. Ja runa ir par viltotiem vai modificētiem attēliem, labākais paņēmiens to identificēšanai un pārbaudei ir reversā jeb apgrieztā attēlu meklēšana. Tas ļauj mums atrast visus iepriekš publicētos attēlus, kas ir identiski vai ļoti līdzīgi. Ja attēls ir publicēts iepriekš, tas ir uzticams veids, kā apstiprināt, ka attēls jau ilgu laiku atrodas internetā. Citos gadījumos, ja attēls, kas izraisīja aizdomas, ir mainīts, apgrieztā attēlu meklēšana var palīdzēt atrast sākotnējo attēlu.

Kā pārbaudīt?

1. Atveriet kādu no meklētājprogrammām (piemēri atrodami tālāk, pie "Noderīgi rīki").
2. Iekopējiet saiti vai pašu lejupielādēto attēlu.
3. Pārbaudiet, vai iepriekš tika ievietoti tādi paši vai ļoti līdzīgi attēli.



Kļūdu līmeņa analīze.

Kļūdu līmeņa analīze (KLA) ir progresīvāka metode, kas ļauj identificēt attēla daļas, kas atrodas dažādos saspiešanas līmeņos. Izmantojot JPEG attēlus, visam attēlam jābūt aptuveni vienā līmenī. Ja attēla sadaļai ir ievērojami atšķirīgs kļūdu līmenis, iespējams, tas norāda uz digitālu modifikāciju. Praktiski Jums vajadzētu apskatīt attēlu un noteikt dažādas augsta kontrasta vietas, zema kontrasta vietas, virsmas un faktūras. Salīdziniet šīs jomas ar ELA rezultātiem. Ja ir būtiskas atšķirības, tas identificē aizdomīgās daļas, kas varētu būt digitāli pārveidotas.

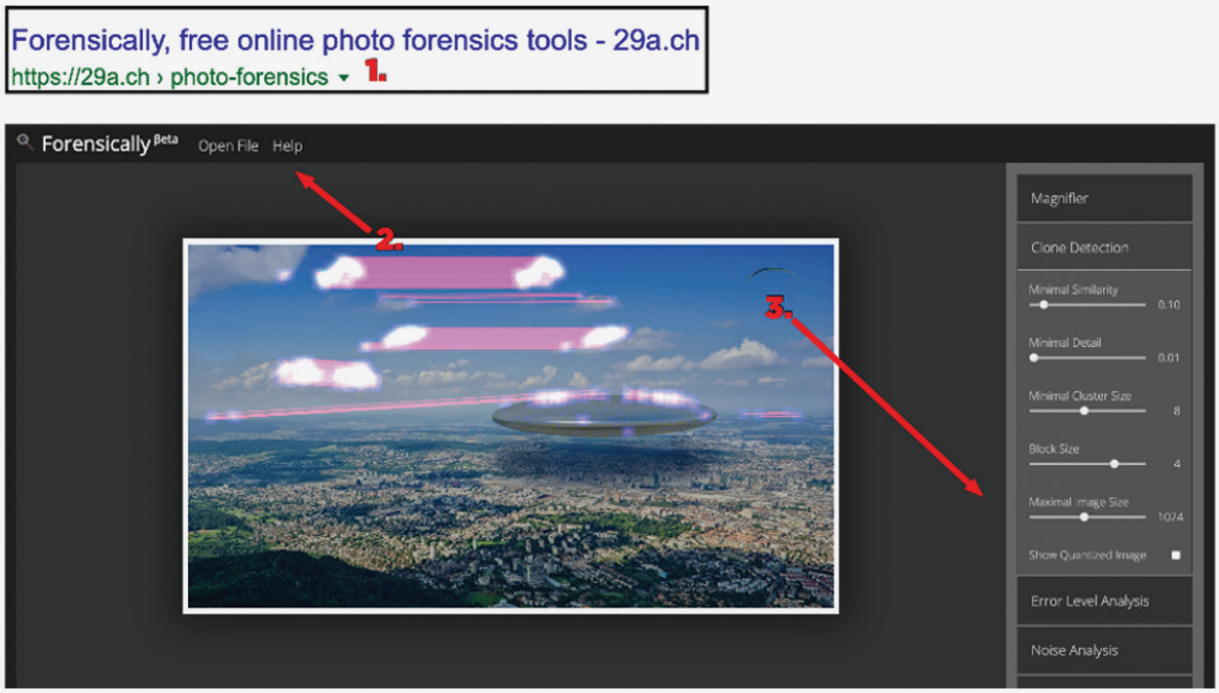
Ir svarīgi atzīmēt, ka, lai gan šī metode nav nekļūdīga, tā tomēr ir uzticams pirmais solis digitālo izmaiņu identificēšanai. Fotoattēlu ekspertīze ir atsevišķa zinātnes nozare, un, lai atmaskotu prasmīgi pārveidotus attēlus, ir vajadzīgas padziļinātas zināšanas un prasmes. Tomēr, runājot par ikdienas propagandas vēstījumiem, attēli nav labi izstrādāti un ir viegli identificējami.

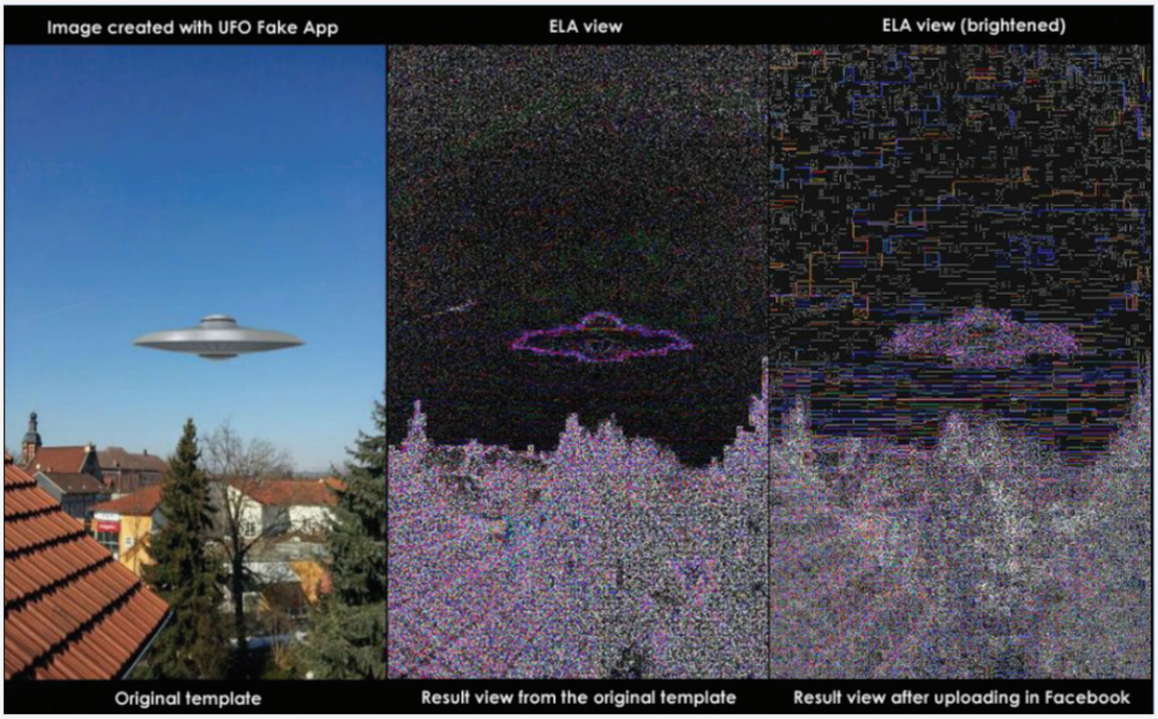
Galvenie noteikumi, kas jāatceras:

• Pirms uzticaties attēla autentiskumam, vienmēr pārbaudiet to ar reverso attēlu meklēšanu.. Ja attēls ir ticis pārveidots, tas var novirzīt no tā īstā vēstījuma;

• KLA nav nekļūdīga metode, taču tas ir lielisks un ātrs veids, kā pārbaudīt, vai attēls ir pārveidots.

• Reverso attēlu meklēšanu var izmantot, lai attēlā identificētu nezināmus cilvēkus.





Noderīgi rīki:

- **Google** / Attēla pārbaude
- **Yandex** / Attēla pārbaude
- **Google** / RevEye paplašinājums
- **Forensically**
- **Foto Forensics**

Ģeneratīvais MI

Kā identificēt MI ģenerētu attēlu:

Atšķirībā no ģenerētā teksta, ģenerētu attēlu ir vieglāk identificēt, it īpaši, ja mēģināt ģenerēt reālistiskus fotoattēlus.

Zemāk ir daži piemēri. Fotogrāfijās redzami cilvēki Viļņas vecpilsētā. No pirmā acu uzmetiena fotogrāfijas šķiet īstas, bet paskatīsimies tuvāk:

• Krāsas – fotoattēlā labajā pusē krāsas šķiet nedabiskas un pārāk spilgtas, noslogojot acis.

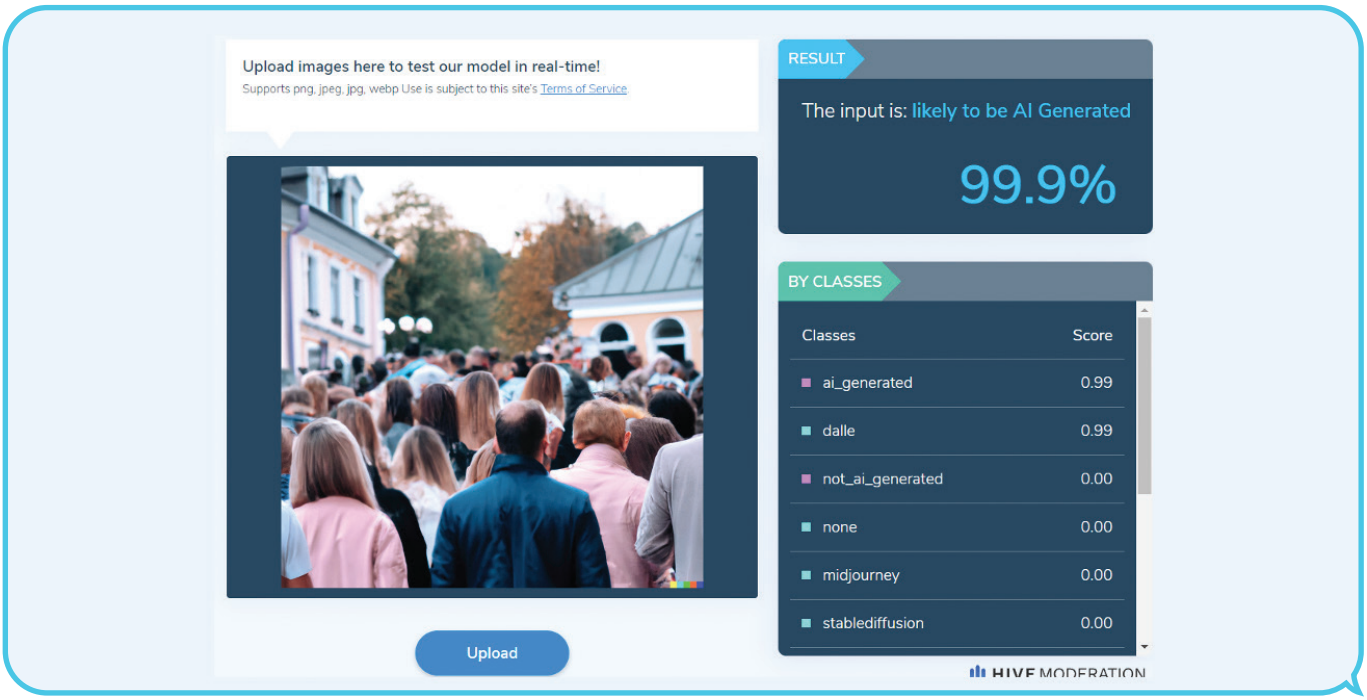
• Fons — bieži vien ģenerētajām fotogrāfijām ir neskaidrs fons, vai arī ēku vai automašīnu līnijas fonā bieži tiek nepareizi pārveidotas.

• Anomālijas un izkropļojumi – pietuvinot fotoattēlus, uzreiz pamanīsiet, ka atsevišķas ķermeņa daļas izskatās nedabiskas un izmainītas: ausis izskatās savdabīgi, galvas šķiet kā ar otu nokrāsotas utt. Turklāt mākslīgais intelekts bieži pievieno vairāk nekā 5 pirkstus vai vairāk zobu nekā ierasts. Ir svarīgi pievērst uzmanību detaļām.

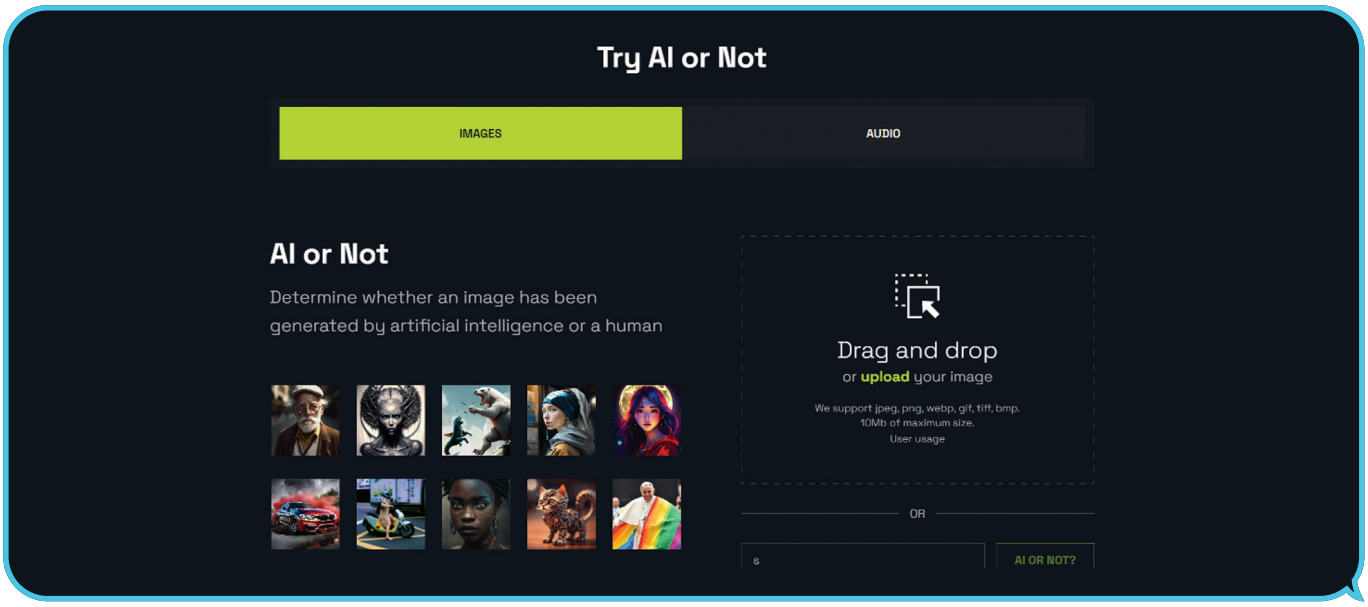
• Ūdenszīmes — rīki, īpaši bezmaksas, bieži fotoattēliem pievieno ūdenszīmes. Iepriekš minētajos piemēros varat pamanīt krāsainos kvadrātus apakšējā labajā stūrī, kas norāda, ka attēli tika ģenerēti ar DALL-E palīdzību. Protams, mēs varam manuāli noņemt šo ūdenszīmi. Tomēr platformas, kas ļauj ģenerēt attēlus, sāka pievienot neredzamas ūdenszīmes, kuras nav redzamas ar neapbruņotu aci. Ja fotoattēls tiek augšupielādēts verifikācijas rīkā, tas nekavējoties noteiks, ka tas ir ģenerēts attēls, jo tas identificēs slēpto ūdenszīmi.

Vairāki automatizēti rīki var palīdzēt identificēt ģenerētos fotoattēlus. Šo rīku izmantošanas princips ir vienkāršs. Velciet un nometiet vai augšupielādējiet fotoattēlu noteiktā lapas sadaļā un noklikšķiniet analizēt. Pēc dažām sekundēm jūs saņemsit rezultātu:

Hivemoderation



Aiornot



Video verifikācija

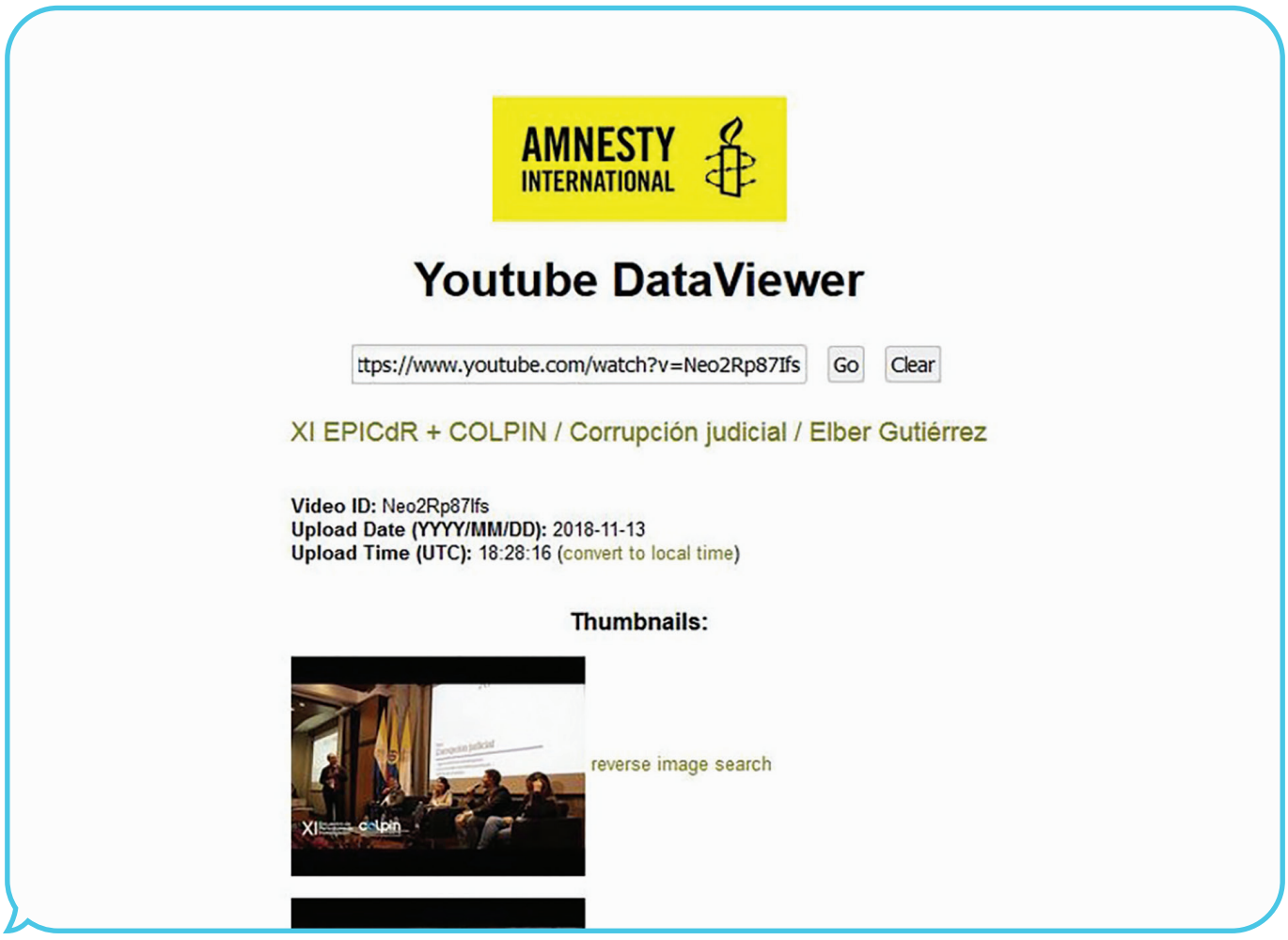
Kā pārbaudīt, vai video ir īsts?

Reversā attēlu meklēšana.

Līdzīgi kā attēlu pārbaudei, labākā metode, lai pārbaudītu, vai videoklips ir īsts, ir attēlu meklēšana. Tā kā videoklipi ir attēlu virkne, kadra izņemšana un tā meklēšana ir lielisks veids, kā to izdarīt. Abi rīki InVid un Amnesty Data Viewer ļaus atrast līdzīgus vai identiskus videoklipus, kas jau ir publicēti tiešsaistē, meklējot gan kadrus, gan sīktēlus.

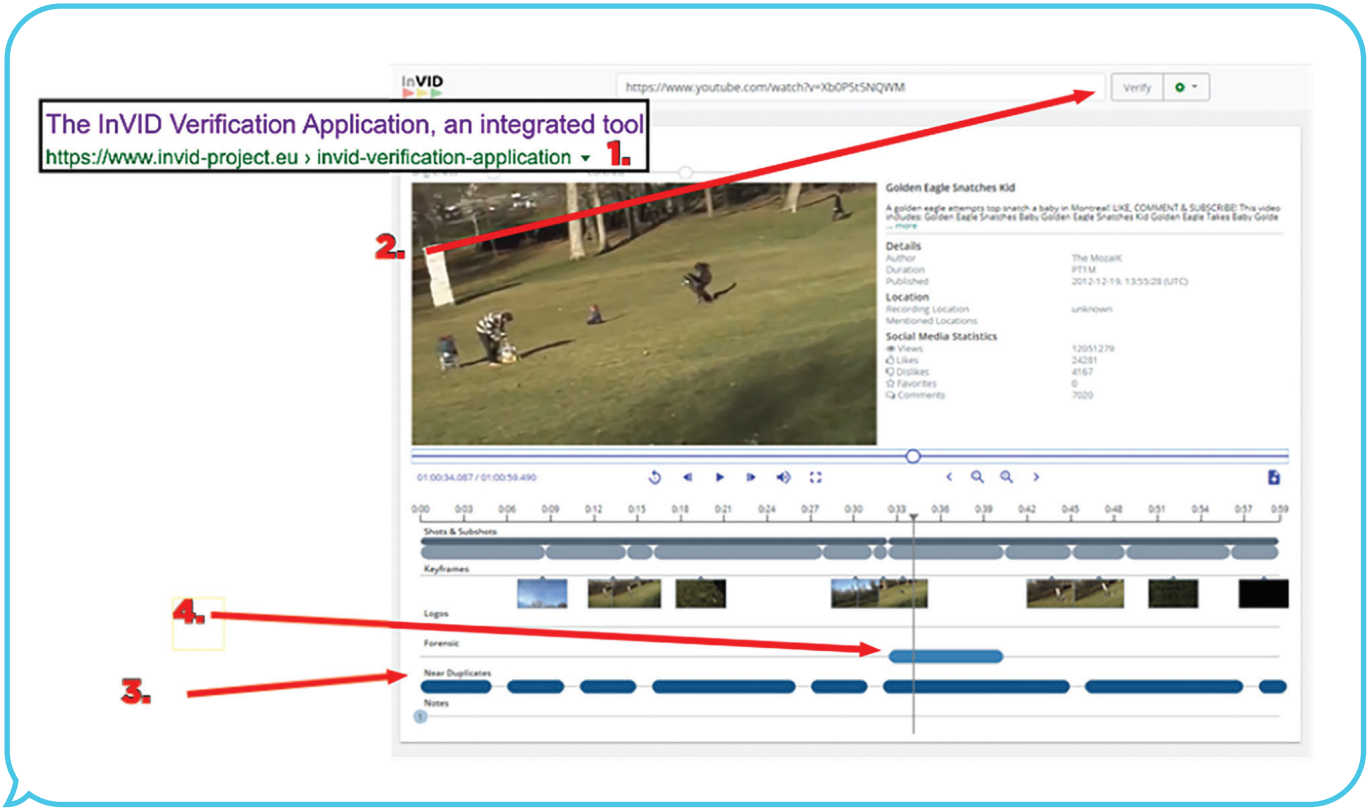
Kā pārbaudīt?

1. Atveriet kādu no meklētājprogrammām (Amnesty DataViewer vai InVid).
2. Ievietojiet videoklipa video saiti.
3. Pārbaudiet, vai videoklips ir redzams starp dublikātiem.



Ekspertīzes analīze

InVid ir pieejama arī ekspertīzes analīzes iespēja, kad programmatūra identificē potenciāli izmainītus kadrus. Potenciāli mainītie kadri tiek parādīti analīzes logā blakus zīmei *"Forensic"*. Ja InVid identificē kadrus kā potenciāli mainītus, pastāv liela iespēja, ka videoklips ir viltots.



Galvenie noteikumi, kas jāatceras:

• Galvenais izaicinājums ar videoklipiem ir tāds pats kā attēliem – materiālu atkārtota izmantošana. Iepriekš izveidotie videoklipi tiek atkārtoti publicēti un pasniegti kā viltus ziņas;

• Šie rīki nav tik efektīvi kā attēlu verifikācijas rīki, taču tie var uzrādīt daudzus viltotus videoklipus;

Noderīgi rīki:

InVid

Amnesty International YouTube Viewer

Troļļi

Kā atpazīt trolli internetā?

Kas ir trollis?

Trollis ir persona, kas tīši ierosina tiešsaistes konfliktu vai aizskar citus lietotājus, lai novērstu uzmanību un radītu šķelšanos, tiešsaistes kopienā vai sociālajā tīklā ievietojot emocionālus vai ar diskusiju nesaistītus ierakstus. Viņu mērķis ir provocēt citus uz emocionālu reakciju un izjaukt diskusijas. Trollis atšķiras no robota, jo trollis ir īsts lietotājs, savukārt robotprogrammatūra ir automatizēta.

Pamanīt trolli ir grūtāk nekā pamanīt robotu, jo šie konti parasti ir sarežģītāki un aktīvi izliekas par īstiem cilvēkiem. Zemāk jūs varat atrast vairākus kritērijus, kas palīdzēs jums identificēt trolli, taču jāatceras, ka tie ir orientējoši ieteikumi. Reti kad ir iespējams ar 100% pārliecību apgalvot, ka konkrētais konts liecina par troļļu darbību, nevis tikai atbalsta noteiktus ļaunprātīgus stāstus.

Tālāk ir minēti daži kritēriji, kas palīdzēs jums identificēt troļļus, taču ņemiet vērā, ka šie padomi ir orientējoši, nevis galīgi. Reti kad iespējams pilnībā pārliecināties, ka konts pieder trollim, nevis vienkārši negatīvi noskaņotam lietotājam.

1. Kļūdas rakstos: angļu valodas nenoteiktie un noteiktie artikuli "a" un "the"	Viena no lingvistiskajām pazīmēm, kas raksturīga daudziem zināmiem Krievijas izcelsmes aprakstiem, ir kļūdas angļu valodas artikulu lietojumā - "a" un "the", jo krievu valodā tādu nav.
2. Kļūdas jautājuma formulēšanā	Vēl viens izplatīts lingvistiskais rādītājs ir nespēja formulēt jautājumu. Krievu valodā vārdu kārtība jautājumiem nemainās, atšķirībā no literārās angļu, vācu un franču valodas. Daudzos zināmos Krievijas troļļu kontos ir ievietoti jautājumi citās valodās, kas saglabā krievu valodas vārdu kārtību.

3. Neskaidra vai apšaubāma identitāte

Daži troļļi izmanto viltotus vārdus, kas attiecīgajā valodā ir ļoti izplatīti, tādējādi apgrūtinot konkrētā autora atšķiršanu vai apzināti liekot to sajaukt ar citu, piemēram, atzītu žurnālistu.

Arī troļļu lietotos vārdus paredzēts uztvert kā tradicionālus jeb "pareizi izskanējušus", lai ikviens lasītājs varētu uzticēties vai neapšaubīt kāda raksta vai komentāra autora autentiskumu sociālajos tīklos. Var būt noderīgi arī pārbaudīt viņu profila attēlus, ja tādi ir. Šādi attēli, kas pievienoti, lai iegūtu papildu uzticību, var būt fonda fotoattēli, kurus varat viegli atrast internetā. Šādi attēli var būt arī apzināti neskaidri, skatoties tuvāk (fotoattēlu rediģēšana, piemēram, attēlojot personu ar saulesbrillēm utt.), tāpēc personu nav iespējams skaidri identificēt.

4. Prokremlisko naratīvu pastiprināšana

Krievijas valdība ir izstrādājusi atšķirīgu stāstījumu par galvenajiem ģeopolitiskajiem notikumiem pēdējo piecu gadu laikā. Tas atbilst principiem, kas noteikti Krievijas Federācijas Informācijas drošības doktrīnā (2000) par valsts politikas un oficiālo pozīciju nodošanu Krievijas valdībai svarīgos jautājumos.

Tā kā prokremliskie naratīvi ir plaši pieejami tiešsaistes avotos, piemēram, Krievijas Ārlietu ministrijā vai RT X/Twitter kontā, ir viegli pārbaudīt, vai aizdomās turamajā kontā parādās tās pašas tēmas. Kontu, kurā atkārtoti tiek apspriesta Krievijas valdības pozīcija par lielāko daļu vai visiem šiem notikumiem, var pamatoti uzskatīt par prokremlisku.

Citas iespējamās norādes

Troļļiem ir vienreizējas lietošanas e-pasta adreses:

Tā kā daudzās lapās vai emuāros, kas ļauj komentēt rakstus, ir nepieciešama arī e-pasta adrese, troļļi to apiet, ievadot fiktīvas adreses. Lielākā daļa vienreizējās lietošanas e-pasta adrešu ir nejaušas un neuzkrītošas, jo tās neatspoguļo personas īsto vārdu.

Troļļu mērķis ir izraisīt cilvēku sašutumu:

Viņi nav pieklājīgi un nekautrējas iesaistīties atklātā konfliktā. Viņi izsaka apsūdzības un parasti šķiet dusmīgi.

Troļļi izmanto anonīmus starpniekserverus:

Troļļi bieži izmanto anonīmas lietojumprogrammas vai starpniekserverus, kas parāda citu interneta protokola (IP) adresi.

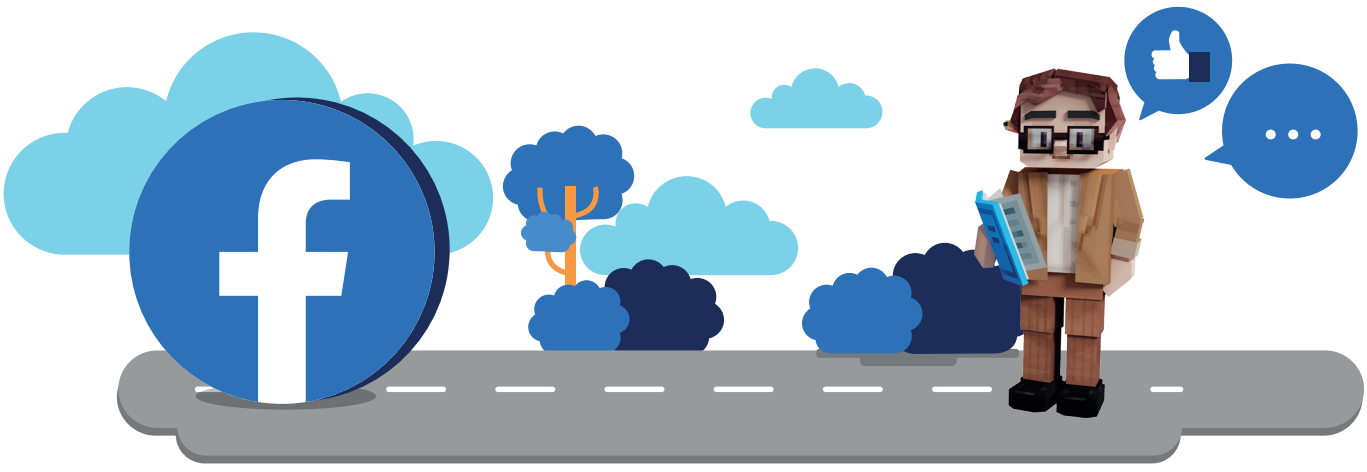
Troļļi sarunas laikā reti saka kaut ko vērtīgu:

Kad troļļi iesaistās kopienas diskusijā, viņi tai neko jēgpilnu nepievieno. Tā vietā viņi joko, pārmet un apvaino.

Viltus Facebook konti

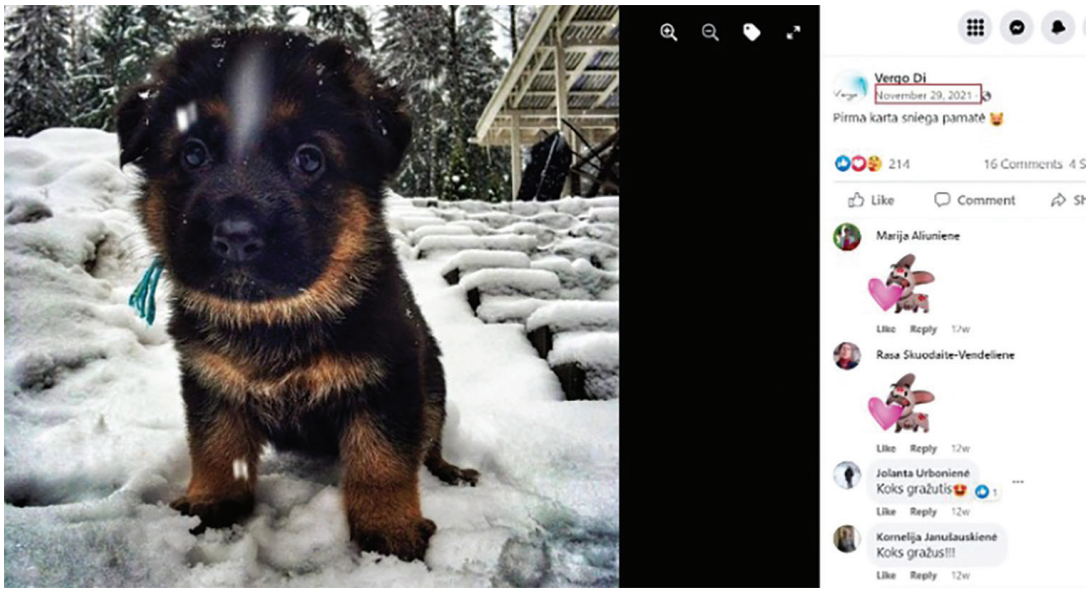
Kā noteikt, vai Facebook konts ir viltots?

Viltus sociālo tīklu konti nav tik aktīvi kā troļļi un parasti spēlē kluso skatītāju lomu. Līdzīgi kritēriji viltus kontiem attiecas uz lielāko daļu sociālo mediju platformu, taču par galveno piemēru šeit esam izvēlējušies Facebook. Īsti Facebook lietotāji savos kontos bieži kopīgo personisko informāciju, tāpēc viltotie konti aktīvi censās kļūt par Jūsu draugiem divu galveno iemeslu dēļ: lai izskatītos īstāki, jo viņu draugu sarakstā ir daudz īstu cilvēku, un kļūt par Jūsu draugiem, lai redzētu vairāk personas informācijas. Atkarībā no viltotā konta mērķa šo situāciju var izmantot, lai vāktu personisku informāciju no dažādu organizāciju darbiniekiem.



1. Pievilcības faktors

Vizuāli pievilcīgu lietotāju konti, kurus nezināt, kuri aicina Jūs kļūt par viņu draugu, var būt viltoti.



Mēs varam viegli pārbaudīt, vai tas nav no interneta kopēts attēls, kuru izvēlējies viltus konta īpašnieks, lai piesaistītu uzmanību un jaunus draugus.

1 result

Searched over 52.5 billion images in 0.5 seconds for:

lh3.googleusercontent.com/J3zMaRV__qxt5dSuOpuflhxiMfP39e...

Sort by best match

Filter by website / collection

instagom.com

explore/tags/germanshepherdpuppies - First found on May 28, 2017

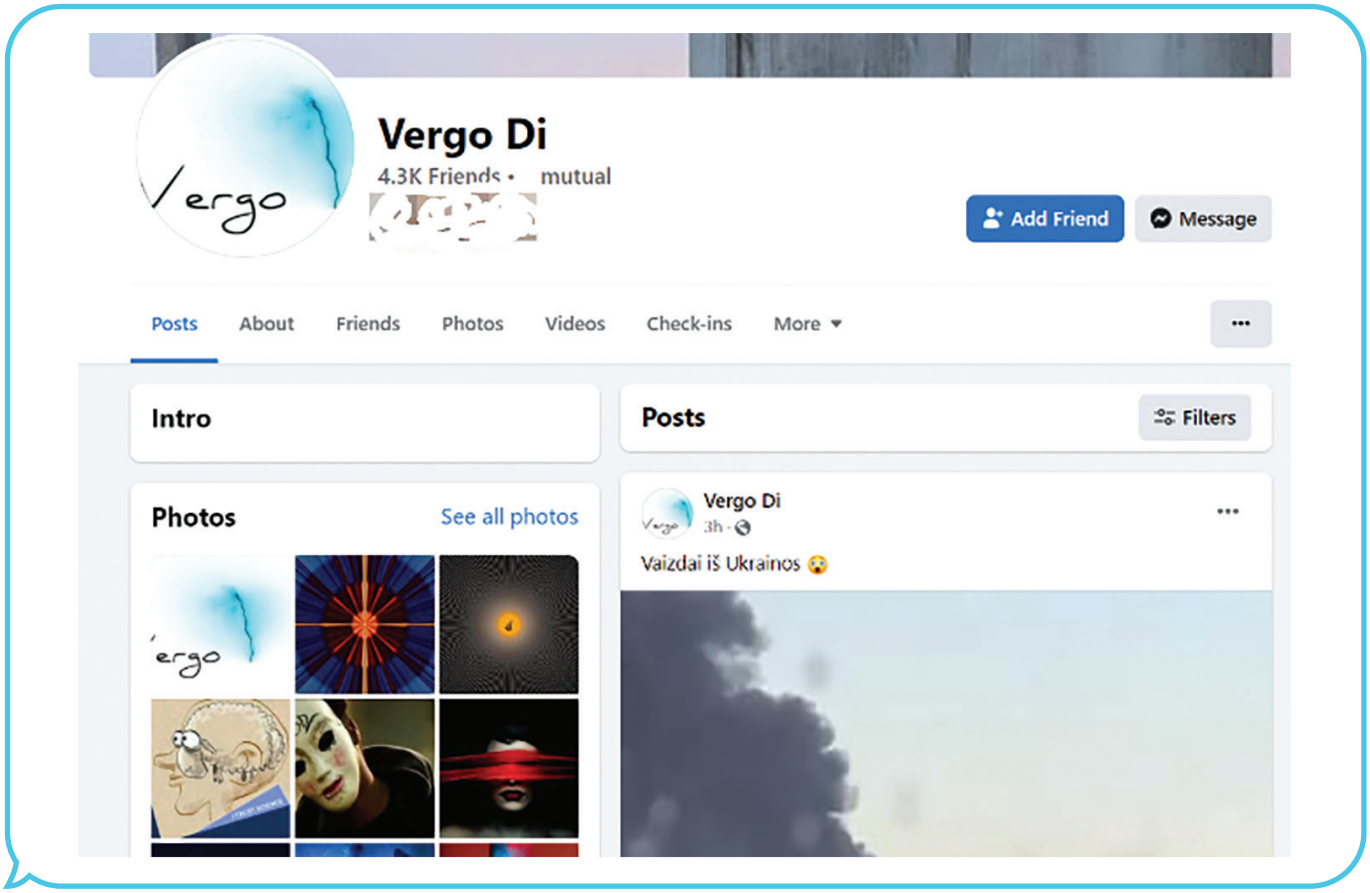
Filename: 18722090_1019473188187238_8466430548250722304_n.jpg
(960 x 960, 151.9 kB)

2. Dažas fotoattēlu augšupielādes

Lielākajā daļā viltus kontu netiek publicēts daudz fotoattēlu — parasti trīs vai četri, dažreiz ar dažādiem cilvēkiem. Tas ir pietiekami daudz, lai radītu īslaicīgu ilūziju, ka konts pieder reālai personai.

3. Dīvainas biogrāfijas

Lielākajai daļai viltus kontu ir biogrāfijas, kas satur ļoti maz informācijas vai šķiet dīvainas. Piemēram, nav neiespējami, bet ļoti maz ticams, ka cilvēks, kurš dzīvo Bronksā, ir mācījies Helsinku Universitātē, ir arī ļoti jauns un jau strādā Ņujorkas sabiedrisko attiecību firmā. Ātra viņa vārda pārbaude Google meklēšanā un apgrieztā profila attēla meklēšana var parādīt, ka konts ir viltots.



4. Nereaģēšana

Ja nosūtāt ziņu uz viltotu kontu, maz ticams, ka saņemsiet atbildi pat uz īsu jautājumu. Vislabāk pat nemēģināt sazināties vai citādi iesaistīties sarunā.

5. Pārsvarā tukša Facebook siena

Vienīgās lietas, ko atradīsit vienā no šīm viltotajām Facebook kontu sienām, ir jaunas atzīmes "Patīk" Facebook biznesa vai produktu lapās un jauni draugi.

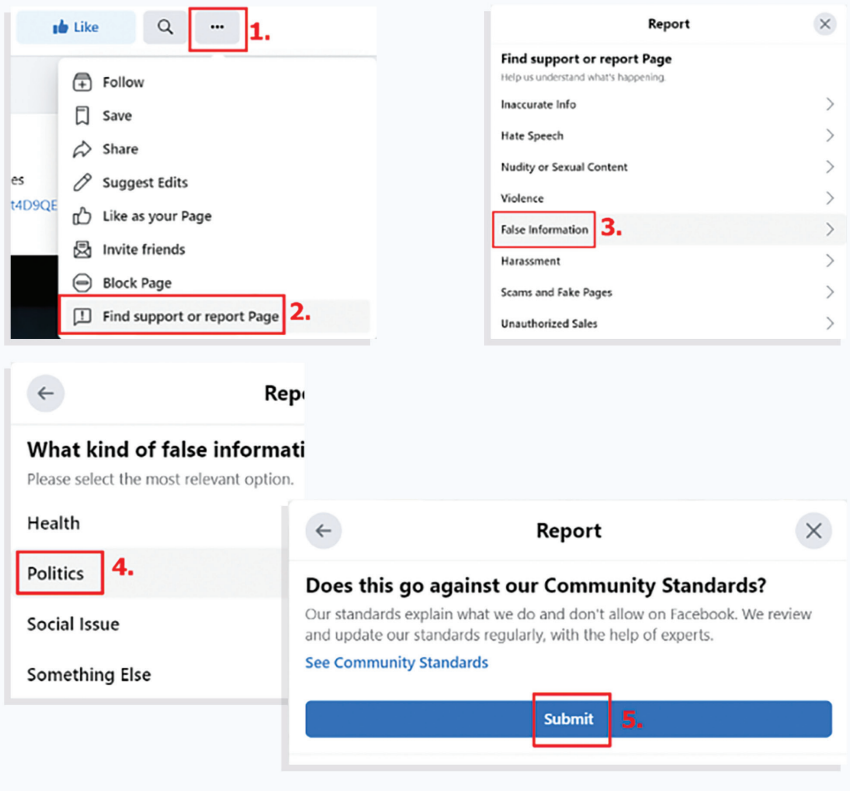
Kā cīnīties?

Lai aktīvi cīnītos pret dezinformāciju internetā, ir jāveic divas darbības: tās atklāšana un ziņošana.

Facebook / X / mediju ziņojumi

Ir ļoti svarīgi, lai Jūsu draugi, klasesbiedri vai kolēģi būtu informēti par dezinformāciju, kas tiek izplatīta pret Jūsu organizāciju. Katrai organizācijai ir jāievieš skaidras procedūras, lai nodrošinātu, ka tās dalībnieki zina, kur nosūtīt ziņojumu par redzētu nepatiesu stāstu. Tās galvenais mērķis ir vienotā veidā informēt organizācijas dalībniekus, ka konkrētais izplatītais ziņojums ir nepatiess, un neļaut viņiem dalīties stāstā un tam noticēt.

Otrais solis ir ziņot par to sociālā tīkla platformā. Visām sociālo tīklu platformām ir funkcija ziņot par ziņu vai ierakstu jebkurā formātā, norādot konkrētu iemeslu, kāpēc tas tiek ziņots. Ja sociālo tīklu platforma saņems pietiekami daudz lietotāju paziņojumu, izveidotais stāsts vai viltus ieraksts tiks dzēsts. Šo metodi pilsoniskās sabiedrības organizācijas izmanto tiešsaistes dezinformācijas apkarošanai. Ja plašsaziņas līdzekļi izplata viltus stāstus, atkarībā no plašsaziņas līdzekļu veida, par to ir jāziņo vai nu pašam medijam, vai valsts plašsaziņas līdzekļu pārraudzības iestādēm (piemēram, SEPLP, u.c.).



"Telegram" lietošanas riski un briesmas

Tā kā daudzi jaunieši ikdienas sarakstei izmanto Telegram, viņi ir informēti arī par citām platformas iespējām – grupām un kanāliem, kas var būt privāti un anonīmi. Lai gan atvērtas komunikācijas plūsmas ir izplatītas sociālajos medijos, slēgtas kopienas var izplatīt konkrētu saturu, tostarp neobjektīvu un izkropļotu informāciju, kuras izcelsmi ir ļoti grūti pārbaudīt.

Pētījumi liecina, ka Telegram kanāli un grupas ir izmantotas dažās dezinformācijas kampaņās, lai izplatītu viltus. Piemēram, dažādās valodās izplatītajos ziņojumos bija iekļauta informācija par COVID-19 pandēmiju, kā arī prokremliskie uzskati par karu pret Ukrainu, galēji labējā retorika un sazvērestības teorijas.

"Telegram" kanālus un grupas var izmantot arī, lai mobilizētu lietotājus ideoloģiskiem mītiņiem vai politiskiem protestiem. Ja šie pasākumi tiek organizēti demokrātiski un caurskatāmi, nav ne jautājumu, ne problēmu, bet dažkārt patiesie labuma guvēji tiek slēpti un informācija par tiem ir maz vai neparādās vispār.

Tā kā daudzi dezinformācijas izplatītāji un propagandisti (tostarp prokremliskie) izmanto "Telegram", ir viegli kopīgot to saturu ar citām grupām un kopienām, kuras vada anonīmi administratori. Tas ir viens no visizplatītākajiem kanāliem pret Rietumiem vērstas vai antiliberālas dezinformācijas digitālai izplatīšanai. Piemēram, "Telegram" kanāls "Antifашисты Прибалтики" (Antifašistiskā Baltija) ir bijis atbildīgs par "rusofobijas" naratīva skatījumu skaita palielināšanu, katrs tā ieraksts savācis pat dažus simtus tūkstošu skatījumu. Vienā no kanāla ierakstiem tika runāts par Latvijas it kā rusofobiju, jo leļļu teātris nolēma aizliegt izrādi ar "čeburaškas" (padomju animācijas filmu tēls Pekausis) tēlu. Ieraksts arī izraisīja naidu pret Latvijas kultūras ministru, augšupielādējot (viltus) fotogrāfiju, kurā viņš pozē grotesku objektu priekšā, apgalvojot, ka "tā ir Latvijas kultūras un nacionālās identitātes seja".

Citā ierakstā bija teikts, ka ikviens "brīvo Rietumu" cilvēks, kurš uzdrošināsies pat pieminēt Krievijas tiesības aizstāvēt krievus, nekavējoties tiks iesēdināts aiz restēm, konfiscējot viņu īpašumus un aizliedzot veikt visas saimnieciskās un radošās darbības. Šie ieraksti liecina, ka Krievija ir aktīvi mēģinājusi izplatīt naratīvu, ka Baltijas valstīs tiek uzbrukts krievu kultūrai un ka krievvalodīgā minoritāte valstīs nespēj izteikties, baidoties no represijām.

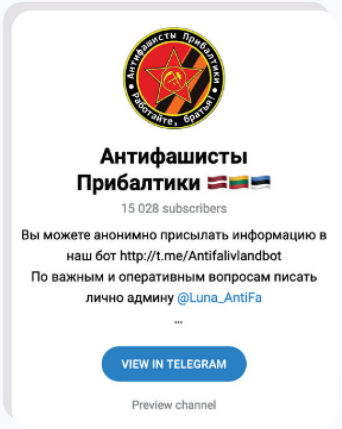
Daži vienkārši padomi, kas var palīdzēt stiprināt digitālo higiēnu "Telegram" kanālā:

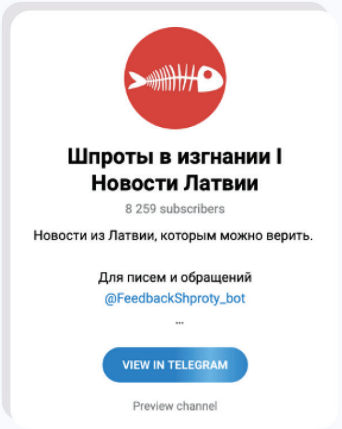
• Pirms pievienošanās grupai vai kanālam pārliecinieties, vai saturs pilnībā Jūs interesē, un meklējiet un pieprasiet vairāk informācijas par tiešsaistes kopienas administratoru.

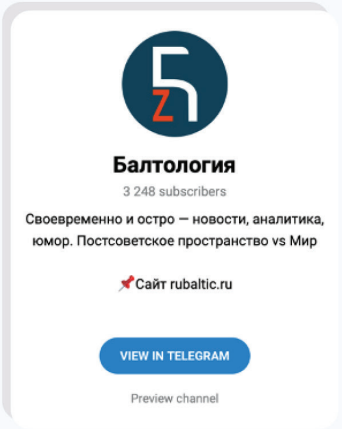
• Esiet piesardzīgs — anonīmās grupās un kanālos, ļoti iespējams, ir nepārbaudīta un/vai neskaidra informācija, ja tēma ir atbilstoša un svarīga. Saturam ir jānāk no ticamiem avotiem, un tas nedrīkst saturēt spekulatīvus viedokļus, „alternatīvus faktus" vai vienkāršotas propagandas klišejas.

• Ja Jūs emocionāli provocē kāda informācija „Telegram" grupā vai kanālā, pajautājiet sev, kāpēc tas ir noticis un kāpēc tas ir noderīgi – nesteidzieties reaģēt un nedalīties ar informāciju, kas var būt neobjektīva, polarizējoša, aizskaroša vai vienkārši nepatiesa.

• Par jebkuru aizdomīgu ziņu „Telegram" grupā vai kanālā var ziņot administratoriem, tīmekļa policijai un digitālās faktu pārbaudes kopienai. Pirms to darāt, noteikti saglabājiet pēc iespējas vairāk oriģinālo ierakstu, piemēram, ekrānuzņēmumu ar tekstuālu vai vizuālu informāciju.







TikTok lietošanas riski un briesmas

TikTok, kas pēdējā laikā ir ieguvis popularitāti jauniešu vidū, ir radīts Ķīnā, un to raksturo augsts dezinformācijas līmenis tiešsaistē. Paši lietotnes veidotāji saka, ka viņi smagi strādā, lai cīnītos pret dezinformāciju, radikālu ekstrēmismu un naidpilnu uzvedību, bet kā viņiem klājas patiesībā?

Lai gan sākotnēji sociālais tīkls nešķita bīstams, laika gaitā lietotāju skaitam augot, saturs sāka mainīties. Tagad tīklā netrūkst ierakstu, kas izplata prokremliskus **naratīvus***.

***Naratīvs** ir sistemātisks un saskaņots stāstījums, kas tiek veidots, atkārtojot ziņojumus par noteiktu tēmu, pievienojot šiem ziņojumiem jaunus faktus un kontekstu.

Naratīvs ir stāsts, kas pārliecinoši pauž galveno vēstījumu un veicina tam atbilstoša viedokļa nostiprināšanos.

TikTok platformu raksturo ļoti neskaidri algoritmi un autoritāru režīmu likumu ievērošana. Šis sociālais tīkls no citiem atšķiras arī ar atkarību izraisošo efektu. Tas izpaužas, pastāvīgi skatoties īsus video, kas ir bagāti ar emocionāliem elementiem un kuriem ir lipīgs skaņu celiņš. Jo vairāk laika tiek pavadīts TikTok, jo labāka kļūst informācijas algoritmiskā prezentācija, un propagandas ziņojumi parādās kopējā patērētā satura plūsmā.

TikTok lietošanai ir divas galvenās problēmas:

• **Agresīva datu vākšana.** Kad lietotne ir instalēta tālrunī vai citā viedierīcē, tā pieprasa papildu piekļuvi datiem un pēc tam tos apkopo. TikTok lietošanas risks ir tāds, ka lietotne var redzēt lietotāja kontaktpersonas, kā arī to, kuras citas lietotnes ierīcē tiek izmantotas, lai uzzinātu sīkāku informāciju par atrašanās vietu un noteiktu, kur atrodas konkrēta ierīce. Pastāv arī risks, ka korespondence, kas notiek lietotnē, var tikt izsekota arī pēc noteiktiem atslēgvārdiem un nonākt uzņēmuma radara pakļautībā.

• **Noēnošana.** Ja lietotājs ievieto kaut ko, kas nepatīk TikTok izstrādātājiem, ziņa var tikt "noēnota", t.i., tiks piemērots aizliegums ziņas izplatībai sociālajā medijā.

TikTok izmanto algoritmu kā līdzekli, lai piesaistītu un noturētu uzmanību, un tā cenšas nodrošināt personalizētu pieredzi katram lietotājam. Algoritms izmanto datus, kas savākti no lietotājiem, lai noteiktu, kāds saturs viņus varētu interesēt. Piemēram, jo ilgāk skatāties videoklipu, jo lielāka iespēja, ka nākotnē TikTok redzēsit līdzīgus videoklipus. Lietotne arī atceras jūsu meklēšanas atslēgvārdus, lai tā varētu ieteikt tāda paša stila videoklipus. Turklāt TikTok algoritms savieno lietotājus ar kopīgām interesēm, parādot viņiem līdzīgu saturu. Ja redzat tādus pašus videoklipus kā daži no saviem draugiem, tā nav nejaušība.

Atcerieties, ka TikTok nebija paredzēts ziņu sniegšanai — īsi video ir vairāk pielāgoti lietotāja izklaidei. Ritinot un skatoties video TikTok, tiek aktivizētas smadzeņu daļas, kas ir atbildīgas par laimes sajūtu – tāpat kā azartspēles, cerot uzlabot garastāvokli, taču reālas peļņas vietā tiek tērēts daudz laika. Tā kā TikTok videoklipi ir īsi, izklaidējoši un viegli pieejami, tie rada sava veida atkarību, kas noved pie fokusa un laika zuduma.

TikTok izmanto arī jūsu zinātkāri un bailes palaist garām kaut ko svarīgu. Vai esat dzirdējuši teicienu "Ja Jūs neesat TikTokā, Jūs nemaz neeksistējat"? To sauc par manipulāciju, un tas ir paredzēts, lai piespiestu jauniešus turpināt lietot lietotni.

Vēl viens triks, ko izmanto TikTok, ir dusmu pārvaldība. Lietotnē tiek piedāvāti videoklipi, kas aizskar cilvēku grupu, ideoloģiju vai kustību, cerot, ka šāds saturs aizskars skatītājus un sāks emocionāli karstas debates, kas piesaista lielāku uzmanību un videoklipi kļūst populāri. Šīs metodes tiek izmantotas, lai palielinātu klikšķu un sekotāju skaitu.

TikTok nomoka kiberhuligānisms, un tāpēc lietotājiem ir liels risks kļūt par uzmākšanās vai naida runas upuri. Turklāt TikTok saturu var izveidot ikviens, tāpēc tas noteikti satur neobjektīvu vai manipulētu informāciju. Lielais personalizētā satura daudzums vietnē TikTok jauniem lietotājiem padara vēl grūtāku atšķirību starp noteiktu lietotāju viedokļiem un faktiem.

TikTok var lietot, ja ievērojat vienkāršus tā lietošanas padomus:

• Ierobežojiet laiku, ko ikdienā pavadāt TikTok — satikties ar draugiem reālajā dzīvē vienmēr ir jautrāk nekā tiešsaistē.

• Atcerieties būt kritiski pret ziņām līdzīgu saturu TikTok — vēlreiz pārbaudiet informāciju, kas Jūs interesē no citiem avotiem (nevis sociālajiem medijiem).

• Ziņojiet par kiberhuligānismu un naida runu — neizplatiet aizskarošus videoklipus vai emocionāli sensitīvu saturu.

• Ja jūtaties apmānīts vai manipulēts, aprunājieties ar vecākiem vai e-policiju.

Paplašināti pasākumi un palīdzības sniegšana

Nopietnākiem dezinformācijas gadījumiem ir divas galvenās pieejas: izmantot sarežģītākas atvērtā pirmkoda metodes vai meklēt palīdzību no tiešsaistes pētniecības kopienas.

Lielākā daļa tiešsaistes rīku ir salīdzinoši viegli lietojami, un tie sniedz detalizētas instrukcijas, kā to izdarīt. Tālāk ir norādīti divi noderīgākie rīki:

Bellingcat's Online Investigation Toolkit

Online Open Source Tool Box

Ja jautājumu joprojām ir vairāk nekā atbilžu, lūdzu, sazinieties ar tiešsaistes pētniecības kopienu un sniedziet viņiem informāciju par atrasto viltus stāstu. Lielākā daļa pētnieku labprāt atmasko viltus stāstus un dalīsies ar atspēkojošo saturu tiešsaistē.

Viļņa, Lietuva
Aprite 500

Izdevuma izdošanu sponsorē
Google