Vokietijos ambasada Vilniuje

CRI CIVIC RESILIENCE INITIATIVE

LIETUVOS RESPUBLIKOS UŽSIENIO REIKALŲ MINISTERIJA

KOVOS SU DEZINFORMACIJA PRIEMONIŲ RINKINYS

KAIP NEAPSIGAUTI

Daugiau apie mus:
www.cri.lt

CIVIC RESILIENCE INITIATIVE
CivicResilience
CivicResilienceInitiative
civicresilienceinitiative

Kovos su dezinformacija priemonių rinkinys. Kaip neapsigauti?

Per pastaruosius dešimt metų socialinė žiniasklaida proporcingai augo. Šiais laikais informacija tiesiog plūsta iš tūkstančių skirtingų komunikacijos kanalų: žiniasklaidos, elektroninių leidinių, interneto svetainių, tinklaraščių ir, žinoma, daugybės socialinių tinklų. Dėl to mes galime laisvai pasirinkti šaltinį, kuris geriausiai atspindi mūsų interesus ir politines ar socialines pažiūras. Vis dėlto, nors daugelis vis dažniau pasirenka socialinius tinklus pagrindiniu informacijos šaltiniu, jie taip pat tapo minų lauku, per kurį greitai pasklinda dezinformacija. Kadangi į naujienas panašius formatus lengva atkurti, vis sunkiau pastebėti skirtumą tarp tikro straipsnio ir apgaulės. Tikros istorijos yra iškraipomos siekiant iškelti politinius klausimus, sena vaizdo medžiaga naudojama iliustruojant naujausius įvykius, siekiant sukelti išgalvotų istorijų sensaciją dalijamasi redaguotais vaizdais, trolių ir botų armijos dislokuojamos atakai prieš organizaciją arba konkretų visuomenės veikėją – darosi vis sunkiau atskirti, kuri naujiena yra tikra, o kuri melaginga.

Siekdama kovoti su dezinformacija, Vilniuje įsikūrusi „Pilietinio atsparumo iniciatyva“ (angl. Civic Resilience Initiative, toliau – CRI), nusprendė sukurti pirmąjį Baltijos šalyse „CRI kovos su dezinformacija priemonių rinkinį“. Šio priemonių rinkinio tikslas žurnalistams, žiniasklaidos atstovams ir pilietinei visuomenei parengti patogų dokumentą, padedantį ugdyti skaitmeninį raštingumą. Kadangi Baltijos šalyse šiuo metu nėra tokio rinkinio analogo, tikimės, kad ši iniciatyva paskatins struktūrinius pokyčius visuomenės skaitmeninio atsparumo srityje.

CRI komanda išsikėlė tikslą tapti pagrindiniu katalizatoriumi Lietuvoje ir Baltijos regione stiprinant visuomenės skaitmeninį atsparumą. Šis priemonių rinkinys kartu su skaitmeniniu atsparumu ir platesniu suvokimu, kaip likti saugiam ir budriam internete, mažiau patyrusiems informacijos vartotojams suteiks reikiamų priemonių ir žinių, kaip kasdieniam naudojimui patikrinti, patvirtinti ir

pasirinkti patikimą informaciją internete. Suprasti šią naują aplinką toli gražu nėra paprasta. Nustatyti „naujienas", kurios gali būti klaidinančios, ir užkirsti kelią tolesnei jų sklaidai yra tikras iššūkis.

Egzistuoja daugybė melagingų naujienų formų:

Dezinformacija – informacija, kuri yra melaginga ir sąmoningai sukurta siekiant pakenkti asmeniui, socialinei grupei, organizacijai arba šaliai.

Misinformacija – informacija, kuri yra melaginga, bet sukurta nesiekiant padaryti žalos.

Malinformacija – tikra informacija, naudojama siekiant padaryti žalos asmeniui, organizacijai arba šaliai.

Visi šie informacijos tipai yra pavojingi, nes keliauja toli ir greitai, jie pasklinda kaip virusai. O tai atsitinka, kai daugelis žmonių, ir net organizacijos, daug nesvarstydami pasidalina šiomis istorijomis, nes jos atrodo įdomios ir sensacingos. Nors negalime užkirsti kelio šių istorijų kūrimui, galime išmokti atpažinti tikrąją istoriją nuo melagingos. Daugiau žinodami apie skaitmeninį pasaulį mes galime išmokti naršyti painioje naujienų visatoje, atskirti tikras istorijas nuo melagingų ir įsitikinti, jog netyčia neprisidėsime prie tolesnės pastarųjų sklaidos.

Mes visi turime atsargiau skaityti naujienas, su kuriomis susiduriame, o tai galime padaryti atkreipdami dėmesį į kelis paprastus ženklus. Šioje brošiūroje pateikiame keletą pagrindinių būdų, kurie leis autentiškas naujienas atskirti nuo tų, kurios iškreipia tiesą. Čia rasite priemones, kurios jums padės:

- **patikrinti, ar informacija internete yra tikra ar melaginga;**
- **nustatyti trolius;**
- **nustatyti botus;**
- **nustatyti netikras socialinių tinklų paskyras;**
- **atpažinti suklastotus vaizdus internete;**
- **atpažinti suklastotus vaizdo įrašus;**
- **ir patars, ką daryti pastebėjus dezinformaciją.**

Tikimės, kad šis trumpas leidinys tam tikru būdu padidins mūsų atsparumą kenkėjiškos, melagingos informacijos plitimui skaitmeniniame amžiuje, pagerins mūsų įgūdžius atpažinti ir pašalinti neteisingą informaciją bei prisidės prie patikimų šaltinių sklaidos.

Atpažinimas

Kaip patikrinti naujienas arba įrašus?

Kai skaitote naujienas ir ypač įrašus socialiniuose tinkluose, kuriuose buvo pasidalyta naujiena arba straipsniu, gali būti sunku nuspręsti, ar turinys yra tikras, ar ne. Tais atvejais, kai tema yra skandalinga arba skamba neįtikėtinai, turėtumėte skirti minutę laiko ir atlikti paprastą patikrinimą, ar informacija yra teisinga ir patikima.

Kaip patikrinti?

Štai penki paprasti veiksmai, kuriuos galite atlikti tikrindami informaciją:

1. Įvertinkite šaltinį.

Panaršykite svetainėje arba socialinių tinklų paskyroje. Pagalvokite, kas išplatino naujienas ir koks istorijos tikslas.

2. Skaitykite ne tik antraštę.

Istorijų antraštės gali būti skandalingos, siekiant pritraukti paspaudimų ir paskatinti dalijimąsi. Pasigilinus į istoriją gali paaiškėti, kad antraštėje pateikti teiginiai nėra teisingi.

3. Patikrinkite autorių.

Ar nurodytas autorius tikrai egzistuoja? Ar autorius yra patikimas žmogus?

4. Ar šaltiniai patvirtina istoriją?

Dažnai melagingose naujienose nėra nuorodų, kurias paspaudus būtų galima patikrinti faktus. Jei istorijoje yra nuorodų į šaltinius, paspauskite jas. Gali paaiškėti, kad pradinė žinutė buvo pagražinta arba jos prasmė iškreipta.

5. Patikrinkite datą.

Iš naujo paskelbtos senos naujienos nereiškia, kad jos vis dar aktualios.

Informacijos (teksto) patikrinimas

Kaip patikrinti naujienas arba įrašus?

Ieškokite „Google“!

Paprasčiau tariant, paieškos sistema, pavyzdžiui, „Google“, yra geriausias jūsų draugas kovoje su dezinformacija. Visą informaciją galima patikrinti ir nustatyti, ar ji teisinga, ar melaginga. Paieškoje naudokite raktinius žodžius, kuriuos galite identifikuoti pagal jus dominančią informaciją, ir sužinoti, ar apie tai kalba patikimi šaltiniai. Jei pamatėte kažką įtartino socialiniuose tinkluose, yra didelė tikimybė, kad kažkas jau stengiasi sužinoti tiesą ir demaskuoti melagingos informacijos skleidėjus.

Didelis pranašumas yra tai, kad sėkmingai identifikavę raktinius žodžius galite patikrinti ir ne skaitmeninę informaciją.

Svarbu pabrėžti, kad tai leis jums rasti patikimą šaltinį su tuo pačiu turiniu, kurį bandote patikrinti, tačiau pirmiausia įsitikinkite šaltinio patikimumu.

Kaip patikrinti?

1. Nustatykite raktinius žodžius, geriausiai apibūdinančius jūsų ieškomą informaciją.

2. Norėdami rasti tą pačią informaciją, pasinaudokite viena iš galimų paieškos sistemų.

3. Atpažinkite patikimus šaltinius ir patikrinkite informaciją.

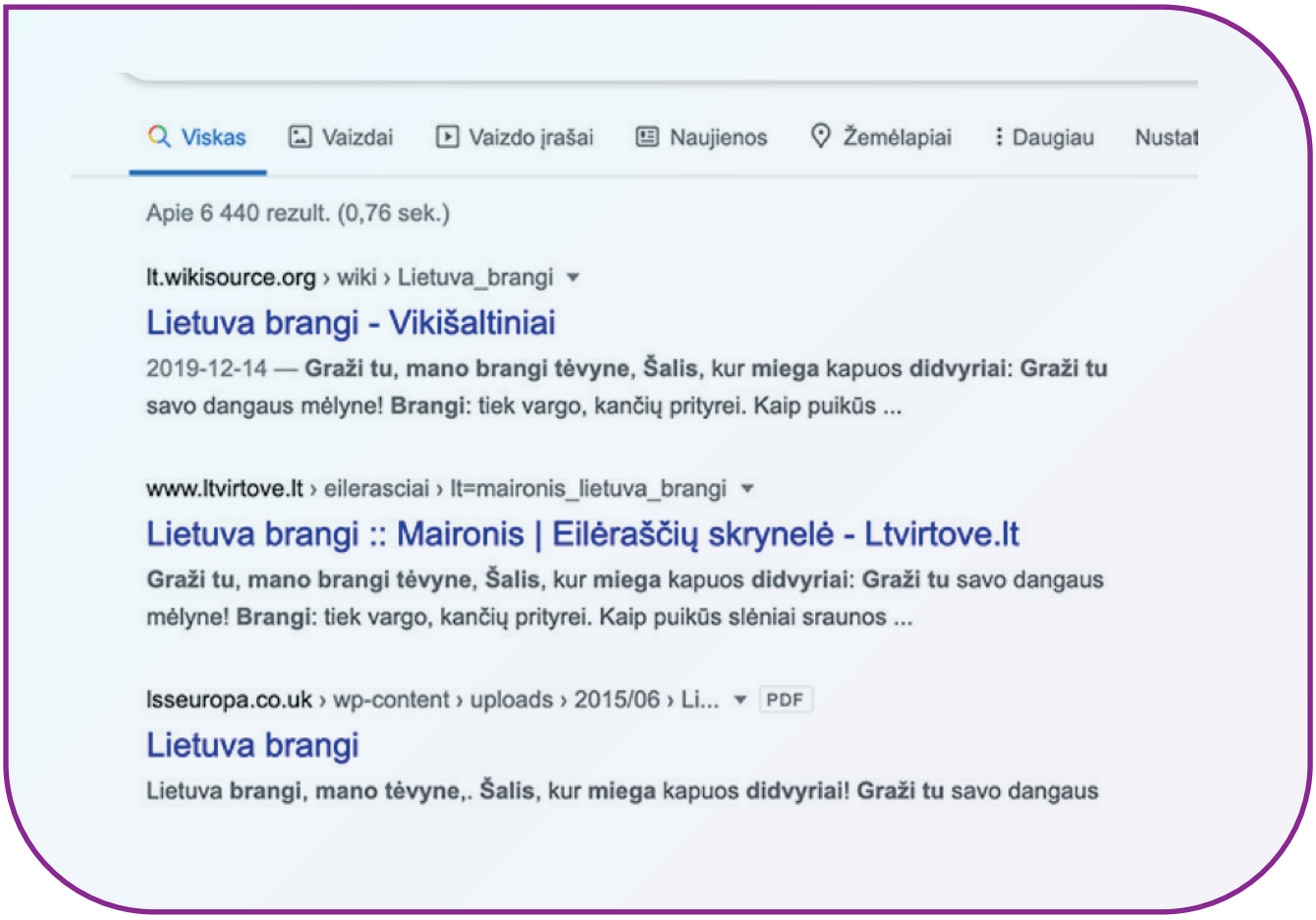
Pagrindinės taisyklės, kurias reikia atsiminti:

• „Google“ paieška yra geriausias pirmasis informacijos patikrinimo žingsnis. Jis yra labai greitas ir efektyvus;

• nesvarbu kokią informaciją norite patikrinti, ieškant teksto, nuotraukų ar vaizdo įrašų „Google“ paieška gali veikti labai gerai;

• svarbiausia yra naudoti raktinius žodžius, kad patikimame šaltinyje rastumėte tą pačią informaciją;

• norėdami efektyviau pasinaudoti „Google“ paieška, naudokite pagrindines „Google Dorking“ funkcijas, t. y., jei ieškote frazės, rašykite ją tarp kabučių („...“); jei jūsų paieškos rezultatuose yra labai populiarus raktinis žodis, prirašykite minusą (-) ir šį raktinį žodį, kad jo neįtrauktumėte į paieškos rezultatus; jei nežinote tikslios žodžio rašybos, tikslaus skaičiaus ar datos, galite prirašyti „*“ kaip pakaitos simbolį, kad pakeistumėte trūkstamą raidę žodyje arba visą žodį, skaičių ar datą;



• jei kalbate kita kalba, galite tuo pasinaudoti. Ieškokite, ką kiti šaltiniai kitomis kalbomis rašo apie šią naujieną;

• jei puikiai mokate tik vieną kalbą, paprašykite žmogaus, kuriuo pasitikite, padėti patikrinti svarbią informaciją kitomis kalbomis. Aptarkite su juo, kaip apie tai pranešama kitose kalbinėse erdvėse.

Naudingos priemonės:

• „Google“ – www.google.com
• „Bing“ – www.bing.com
• „Yandex“ – www.yandex.com

Vaizdų patikrinimas

Kaip patikrinti, ar vizuali informacija yra tikra?

Atvirkštinė vaizdo paieška

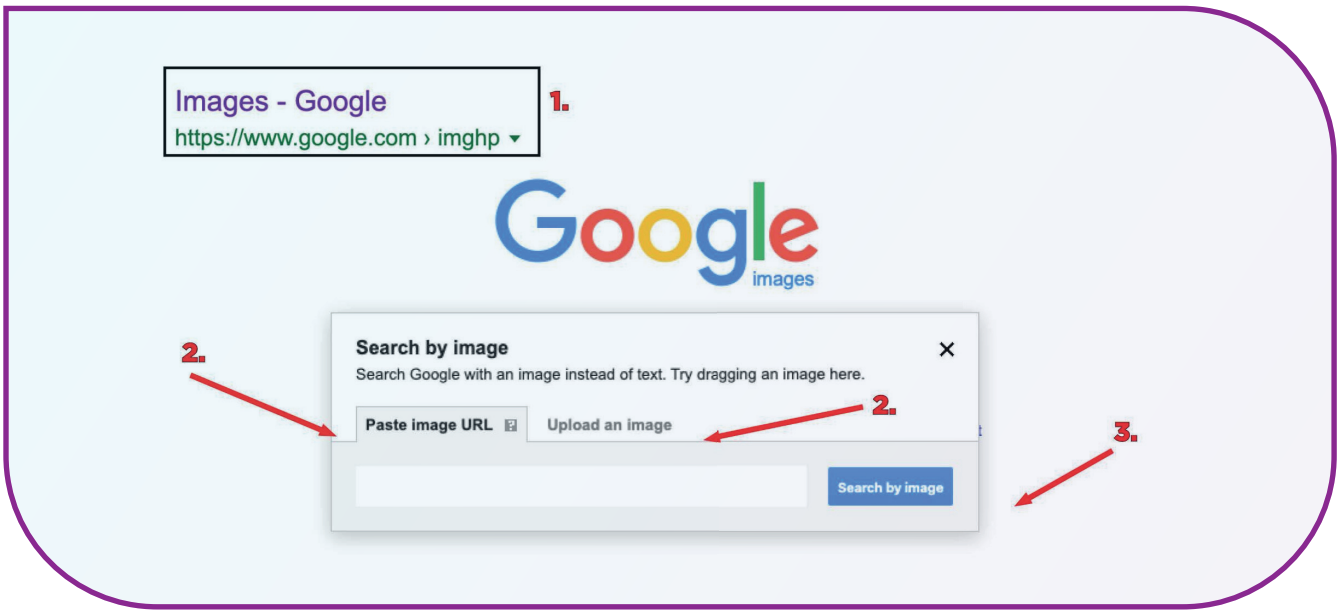
Geriausia metodika atpažinti netikrus vaizdus yra atvirkštinė vaizdo paieška. Metodikos idėja yra paieškos sistemos panaudojimas, bet ieškant ne raktinių žodžių, o vaizdų. Tai leidžia mums surasti visus identiškus arba labai panašius vaizdus, paskelbtus anksčiau. Kadangi vaizdų perdirbimas (prieš tai buvusio vaizdo paskelbimas ir teigimas, kad jis buvo užfiksuotas neseniai) išlieka viena iš pagrindinių dezinformacijos erdvės problemų, viena geriausių strategijų yra patikrinti, ar vaizdas nebuvo paskelbtas kada nors anksčiau. Kitais atvejais, jei jūsų turimas vaizdas buvo pakeistas, atvirkštinė vaizdo paieška gali padėti rasti originalų vaizdą.

Kaip patikrinti?

1. Atidarykite vieną iš paieškos sistemų (nuorodos pateikiamos ties „Naudingos priemonės“).

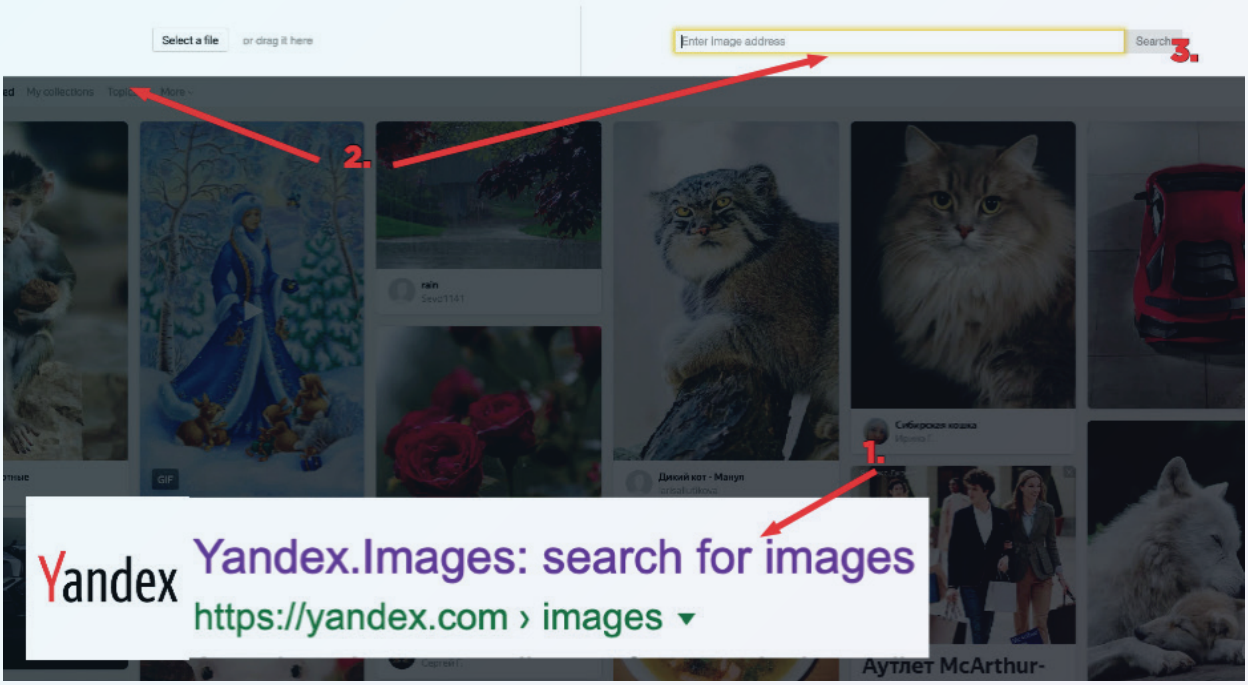
2. Nukopijuokite nuorodą arba patį atsisiųstą vaizdą.

3. Ištirkite, ar tie patys arba labai panašūs vaizdai buvo paskelbti anksčiau.



Veido atpažinimas

Kai kurios paieškos sistemos turi ir veidų atpažinimo funkcijas. Šios funkcijos gali padėti atpažinti nuotraukose rastus nepažįstamus žmones. „Yandex" atvirkštinis vaizdas suranda panašiausiai atrodančius žmones, kurie paskelbė savo nuotraukas internete, ir pasiūlo galimas šių žmonių tapatybes. Tai ypač naudinga, kai nuotraukoje yra keli asmenys, tačiau kai kurių iš jų veidai buvo pakoreguoti, arba pakeisti. Paprasta atvirkštinio atvaizdo paieška padės pastebėti skirtumus.



Klaidų lygio analizė

Klaidų lygio analizė (KLA) yra pažangesnis metodas, leidžiantis atpažinti vaizdo vietas, kuriose yra skirtingas glaudinimo lygis. JPEG formato vaizduose visas vaizdas turėtų būti maždaug tokio paties lygio. Jei vienos vaizdo dalies klaidų lygis žymiai skiriasi, greičiausiai vaizdas buvo pakeistas skaitmeniniu būdu. Praktiškai tiesiog turėtumėte gerai apžiūrėti paveikslėlį ir nustatyti skirtingus didelio kontrasto kraštus, mažo kontrasto kraštus, paviršius ir tekstūras. Palyginkite tokias vietas su KLA rezultatais – jeigu tam tikros vaizdo dalys žymiai skiriasi, analizė nustato įtartinas vietas, kurios galėjo būti pakeistos skaitmeniniu būdu.

Svarbu pažymėti, kad šis metodas nėra be trūkumų, tačiau tai yra pirmasis patikimas žingsnis, leidžiantis identifikuoti skaitmeninius vaizdo pakeitimus. Nuotraukų kriminalistika yra atskira mokslo šaka, o norint demaskuoti gerai perdirbtus vaizdus reikia daugybės metų patirties. Visgi, kalbant apie kasdienes propagandines žinutes, dažniausiai šie vaizdai nėra gerai perdirbti ir juos gana lengva atpažinti.

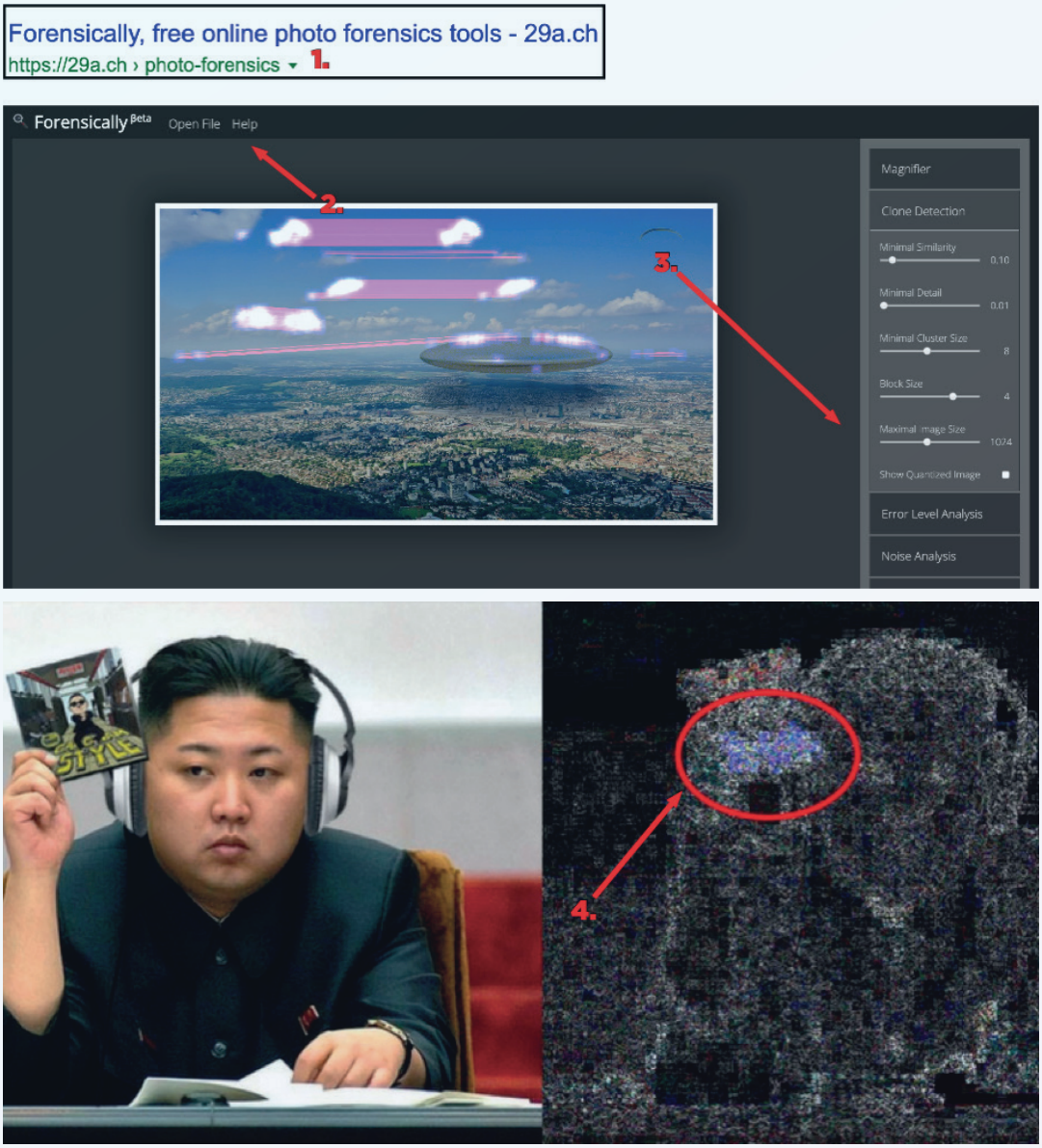
Kaip patikrinti?

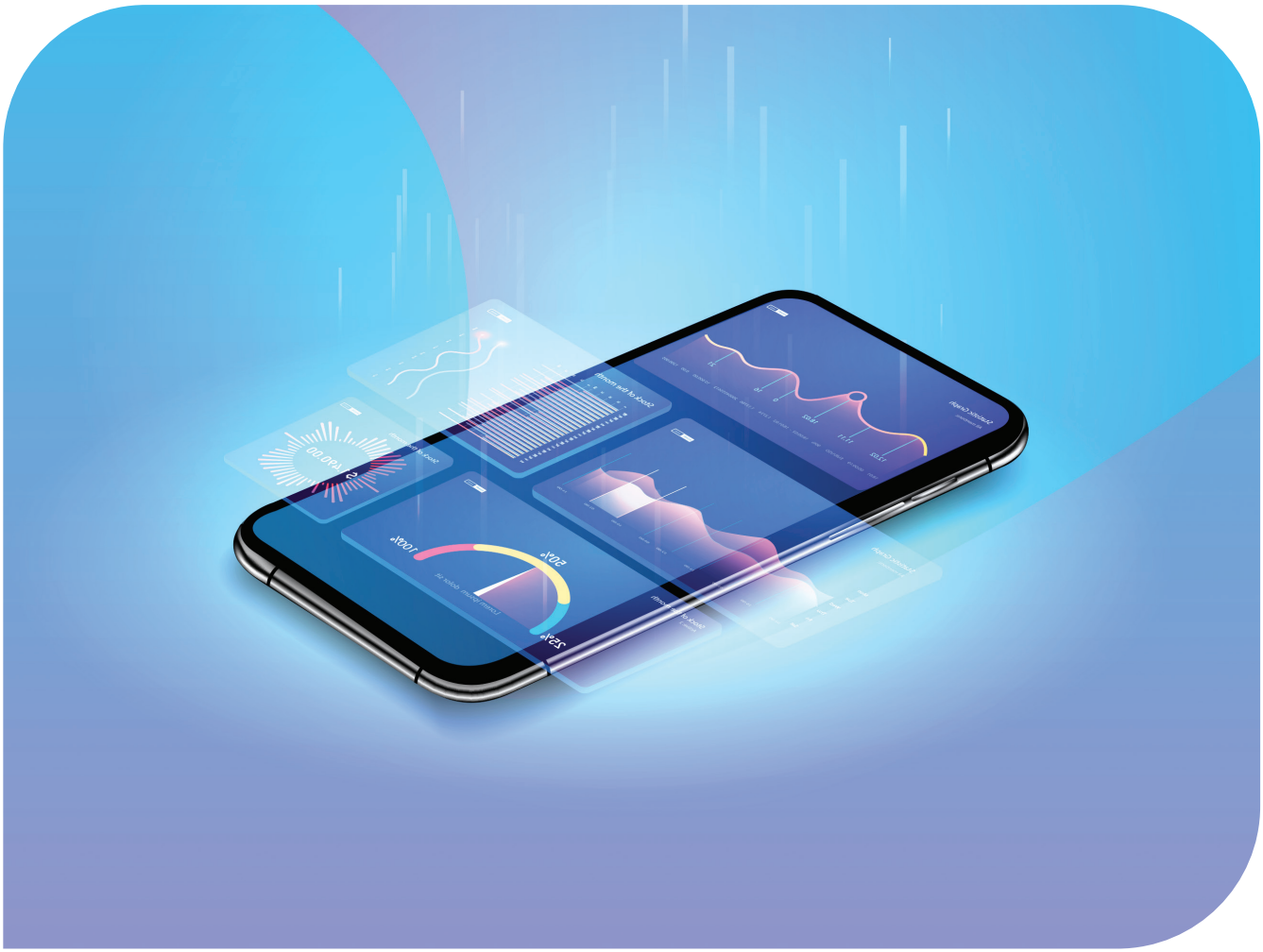
1. Atidarykite programėlę „Forensically" arba „FotoForensics" (nuorodos pateikiamos toliau).

2. Įkelkite norimą JPEG formato vaizdą.

3. Pasirinkite KLA analizę.

4. Analizėje ieškokite neatitikimų.





Pagrindinės taisyklės, kurias reikia atsiminti:

• prieš pasitikint vaizdu, atvirkštinė vaizdo paieška turėtų būti įprasta praktika. Jei vaizdas nebus toks, koks apibūdintas, jis gali perkreipti tikrąją žinutę;

• atvirkštine vaizdo paieška galite pasinaudoti norėdami paveikslėlyje atpažinti nežinomus žmones;

• KLA nėra metodas, kuriuo galite aklai pasitikėti, tačiau tai puikus ir greitas būdas patikrinti, ar vaizdas yra perdarytas.

Naudingos priemonės:

• „Google" atvirkštinė vaizdo paieška – https://images.google.com/

• „Yandex" atvirkštinė vaizdo paieška – https://yandex.com/images/

• „Google" plėtinys „RevEye" – http://tiny.cc/ejcgdz

• „Forensically" – https://29a.ch

• „Foto Forensics" – https://fotoforensics.com

Vaizdo įrašų patikrinimas

Kaip patikrinti, ar vaizdo įrašas yra tikras?

Atvirkštinė vaizdo paieška

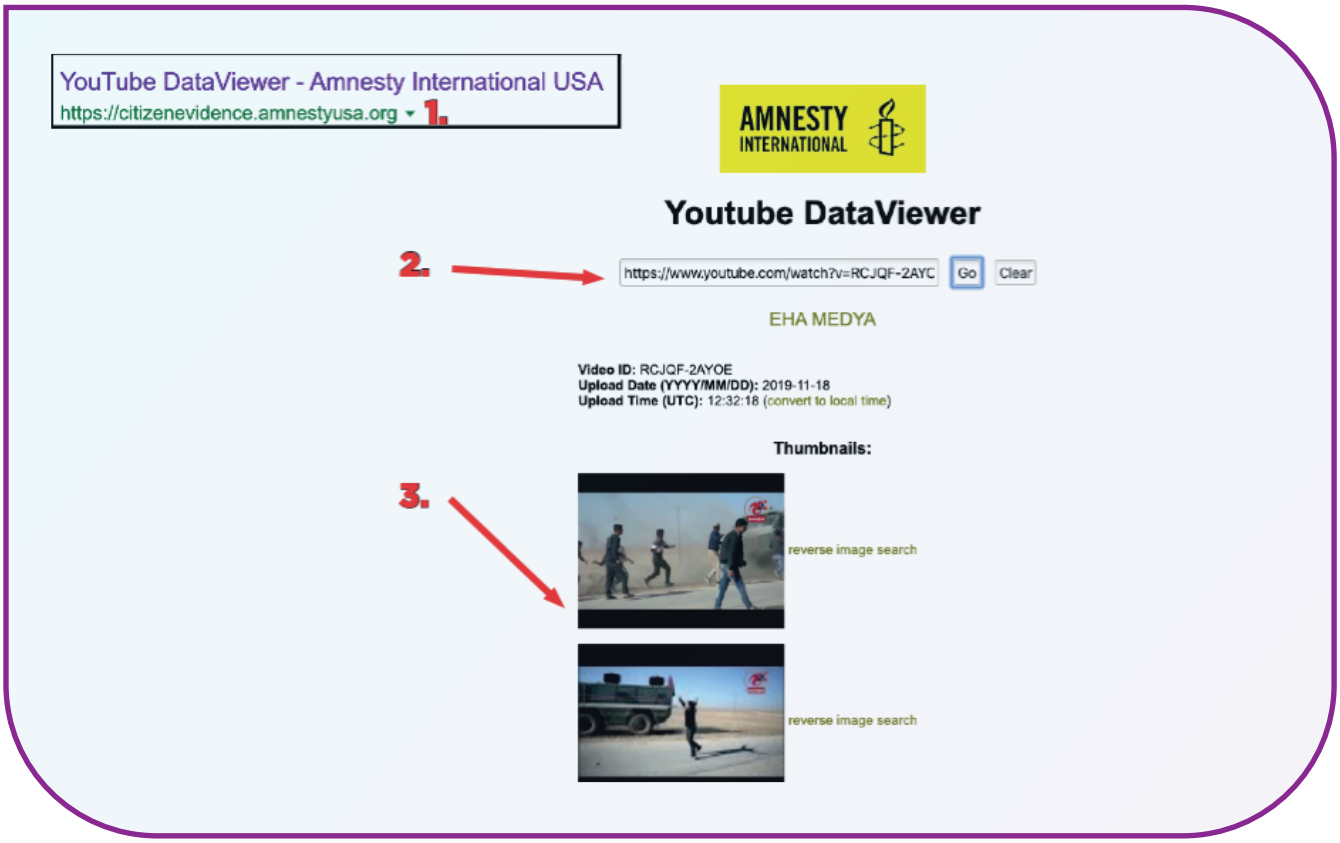
Geriausia metodika atpažinti netikrus vaizdo įrašus, kaip ir statiškus vaizdus, yra atvirkštinė vaizdo paieška. Kadangi vaizdo įrašai yra tik vaizdų serija, puikus būdas tai padaryti yra atskiro kadro išėmimas ir individuali jo paieška. Tiek „InVid" ir „Amnesty Data Viewer" įrankiai leis jums atrasti jau anksčiau internete paskelbtus panašius arba identiškus vaizdo įrašus, ieškant tiek kadrų, tiek miniatiūrų.

Kaip patikrinti?

1. Atidarykite vieną iš paieškos sistemų („Amnesty DataViewer" arba „InVid").

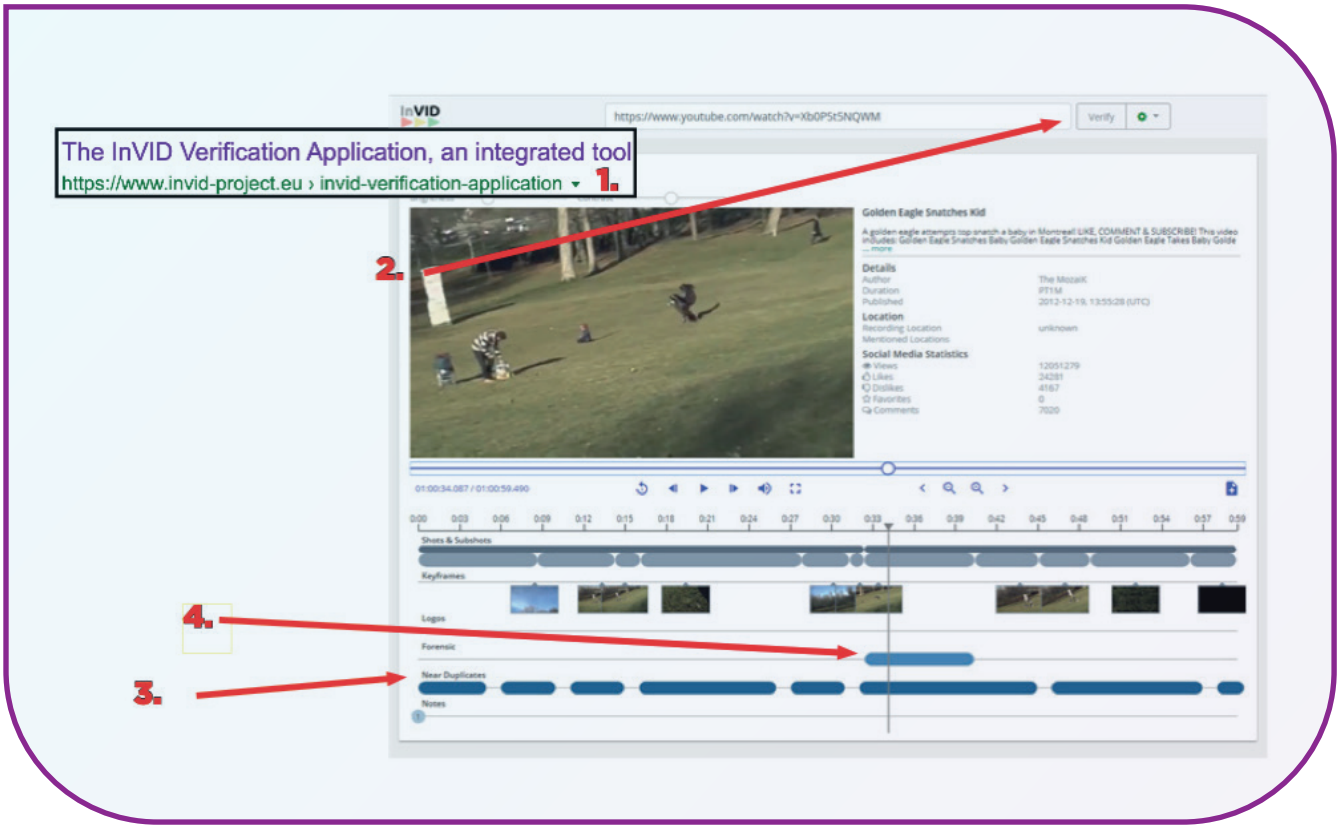
2. Įklijuokite vaizdo įrašo nuorodą.

3. Patikrinkite, ar vaizdo įrašas rodomas tarp dublikatų.



Mokslinė analizė

„InVid" taip pat turi mokslinės analizės funkciją, kai programinė įranga nustato galimai pakeistus kadrus. Galimai pakeisti kadrai pasirodo analizės lange, šalia ženklo „Forensic". Jei „InVid" nustato kadrus kaip galimai pakeistus, tikimybė, kad vaizdo įrašas yra melagingas, yra didelė.



Pagrindinės taisyklės, kurias reikia atsiminti:

• pagrindinė grėsmė su vaizdo įrašais yra tokia pati kaip ir su vaizdais – vaizdo įrašų perdirbimas. Vaizdo įrašai, kurie buvo nufilmuoti anksčiau, vėl paskelbiami ir pateikiami kaip melagingos naujienos;

• šios priemonės nėra tokios veiksmingos kaip vaizdų patikrinimo priemonės, tačiau gali užfiksuoti daug melagingų vaizdo įrašų;

• abi priemonės pateikia šiek tiek skirtingus rezultatus, todėl norint padidinti galimybę atpažinti melagingus vaizdo įrašus, verta išbandyti jas abi.

Naudingos priemonės:

• „InVid" – https://www.invid-project.eu/

• „Amnesty International YouTube Viewer" – https://citizenevidence.amnestyusa.org/

Botai

Kaip atpažinti botą internete?

Kas yra botas?

Botai – automatizuotos socialinių tinklų paskyros, kurios apsimeta tikrais žmonėmis – ypač aktyviai naudojami tokiose platformose kaip „Twitter". Jų yra milijonai ir jie nuolat ištrinami bei kuriami iš naujo. Šie botai gali rimtai iškreipti diskusijas, ypač kai jie dirba kartu.

Dažniausiai botai naudojami:

- **siekiant sukurti frazės arba grotažymės tendenciją;**
- **žinutei sustiprinti;**
- **žinutei atakuoti;**
- **priekabiauti prie kitų naudotojų.**

Daugelį botų ir botnetų (botų tinklų) gana lengva pamatyti plika akimi, net ir neturint prieigos prie specializuotos programinės įrangos arba komercinių analizės priemonių. Programinės įrangos įrankiai, pavyzdžiui „Sysomos", „FireEye" arba „Crimson Hexagon", gali būti naudojami siekiant palengvinti paiešką platesniu mastu, tačiau jei jums reikia patikrinti, ar paskyra yra netikra, galite atlikti šiuos 12 paprastų veiksmų:

1. Aktyvumas – akivaizdžiausias rodiklis. Jį galima lengvai apskaičiuoti peržiūrėjus profilio puslapį ir padalijus įrašų skaičių iš dienų, kai asmuo buvo aktyvus. Daugiau nei 50 įrašų per dieną sukuriantis profilis gali būti laikomas įtartinu.

2. Anonimiškumas – kuo mažiau asmeninės informacijos suteikiama, tuo didesnė tikimybė, kad paskyra nepriklauso tikram žmogui. Jei nėra aprašymo, nuotraukos ar fono paveiksliuko – labiau tikėtina, kad tai botas.

3. Platinimas – vienas iš pagrindinių botų vaidmenų yra platinti kitų naudotojų žinutes jomis besidalijant, paspaudžiant „patinka" arba cituojant. Tipinio boto laiko juosta susideda iš pasidalijimų ir pažodinio naujienų antraščių citatų kartojimo, joje nedaug originalių įrašų arba jų visai nėra.

4. Mažai įrašų / daug rezultatų – minėti botai pasiekia savo efektą masiškai dalydamiesi turiniu iš vienos paskyros. Kitas būdas pasiekti tą patį efektą yra sukurti daugybę paskyrų, kurios kiekvieną kartą pasidalija tuo pačiu įrašu – taip veikia botnetas.

5. Bendras turinys – tikimybę, kad paskyros priklauso vienam tinklui, galima patvirtinti peržiūrėjus tų paskyrų įrašus. Jei jos visos tuo pačiu metu skelbia tą patį ar tokio pačio tipo turinį, jos tikriausiai yra užprogramuotos tai daryti.

6. Siluetai – primityviausius botus ypač lengva atpažinti, nes jų kūrėjai nesivargino sukurti bei priskirti jiems pseudoportretus.

7. Neoriginali nuotrauka – kiti botų kūrėjai yra kruopštesni ir bando užmaskuoti savo anonimiškumą paimdami nuotraukas iš kitų šaltinių.

8. Keistas vardas – dar vienas tikėtino boto rodiklis yra jo vardas, pavardė. Daugelis botų turi vardus, kurie yra tiesiog algoritmo sukurti raidiniai ir skaitiniai kodai.

9. Daugiakalbystė – kai kurie botai yra komerciniai ir atrodo tarsi būtų išnuomoti didžiausią kainą pasiūliusiam asmeniui, neatsižvelgiant į planuojamą dalytis turinį. Tokie botnetai dažnai pasižymi

ypatinga kalbų vartojimo įvairove.

10. Komercinis turinys – atrodo, kad kai kurie botnetai pirmiausia egzistuoja šiam tikslui ir tik retkarčiais yra įtraukiami į politiką. Tokiais atvejais tikrąją paskirtį išduoda jų dėmesys reklamai.

11. Automatizuota programinė įranga – kita užuomina apie galimą automatizavimą yra URL sutrumpinimų naudojimas. Jie pirmiausia naudojami tam tikros nuorodos srautui stebėti, tačiau jų naudojimo dažnis gali būti automatizavimo rodiklis.

12. Pasidalijimų ir paspaudimų „patinka" santykis – galutinį rodiklį, rodantį, kad tai botas, galime atpažinti palyginę tam tikrų įrašų pasidalijimų ir paspaudimų „patinka" santykį. Kai kurie botai yra užprogramuoti pasidalyti tuo pačiu įrašu ir paspausti „patinka" – tokiais atvejais pasidalijimų ir paspaudimų „patinka" skaičius bus beveik identiškas.

Pagrindinės taisyklės, kurias reikia atsiminti:

• kuo daugiau kriterijų atitinka paskyra, tuo didesnė tikimybė, kad tai botas. Vis dėlto, jei ji atitinka bent du ar tris sąrašo kriterijus, irgi galimai pagrįstai įtarti, kad tai fiktyvi paskyra;
• būkite atsargūs, paskyras viešai vadindami botais. Geriausias būdas jas apibūdinti – teigti, kad tai yra į botus panašios paskyros. Tai užkerta kelią neteisingiems kaltinimams, o taip pat botų savininkai negalės jūsų apgauti po identifikavimo išjungdami paskyros automatizavimą;
• siekdami nustatyti daugiau strateginio lygio tendencijų bei identifikuoti botus kuriantį asmenį, galite pasinaudoti programine įranga;
• daugiausia botų yra „Twitter", tačiau jų gali būti ir socialiniame tinkle „Facebook". Būtina užsiminti, kad dauguma netikrų paskyrų svetainėje „Facebook" yra labiau panašios į trolius ir bus plačiau aptariamos kitoje skiltyje.

Troliai

Kaip atpažinti trolį internete?

Kas yra trolis?

Trolis yra asmuo, kuris tyčia inicijuoja konfliktą internete arba įžeidžia kitus naudotojus, paskelbdamas emocijas kurstančius arba su tema nesusijusius įrašus internetinėje bendruomenėje arba socialiniame tinkle, kad pasėtų susiskaldymą. Jie siekia išprovokuoti kitų emocinį atsaką ir nutraukti konstruktyvias diskusijas. Trolis skiriasi nuo boto, nes trolis yra tikras naudotojas, o botai yra automatizuoti, šie du paskyrų tipai tarpusavyje nėra susiję.

Pastebėti trolį yra sunkiau nei pastebėti botą, nes tokia paskyra paprastai yra sudėtingesnė ir aktyviai apsimeta tikrais žmonėmis. Toliau rasite daugybę kriterijų, kurie padės atpažinti trolį, tačiau šios užuominos yra orientacinės, o ne galutinės. Šie patarimai skiriami Baltijos šalių regionui, tad geriausiai atpažįsta trolius veikiančius šiose šalyse - prokremliškus trolius. Tik retais atvejais galima užtikrintai pasakyti, kad tam tikra paskyra priklauso troliui, o ne šiaip pa-giežingam žmogui. Prieš nagrinėjant veiksnius, kurie patikimai padeda atpažinti prokremliškų pažiūrų trolį, svarbu pažvelgti į vieną veiksnį, kuris trolio neapibūdina – tai itin patriotiškas turinys. Realūs šių laikų socialinių tinklų naudotojai yra labai patriotiški, ypač kai kalbama politinėmis temomis.

1. Klaidos straipsniuose.

Anglų kalbos artikeliai „a" ir „the". Vienas iš kalbinių ženklų, būdingų daugeliui žinomų rusiškų trolių paskyrų, yra nesugebėjimas tinkamai naudoti gramatinių artikelių „a" ir „the". Rusų kalboje nėra nei vieno iš jų.

2. Klaidos formuojant klausimą.

Kitas dažnai kalbinis rodiklis yra nesugebėjimas suformuluoti gramatiškai taisyklingo klausimo. Rusų kalboje žodžių tvarka sudarant klausimus nesikeičia, skirtingai nei anglų, vokiečių ir oficialioje prancūzų kalboje. Daugelis žinomų trolių paskyrų skelbia klausimus, kuriuose žodžių tvarka tokia pati kaip ir paprastuose sakiniuose.

3. Neaiški arba abejotina tapatybė.

Kai kurie troliai pasivadina netikrais vardais, kurie yra labai paplitę tam tikroje kalboje, todėl sunku

atskirti konkretų autorių arba lengva sąmoningai supainioti jį su kitu, pavyzdžiui, žinomu žurnalistu. Troliai taip pat siekia, kad jų vardai būtų suvokiami kaip tradiciniai arba „teisingi", kad kiekvienas skaitytojas būtų linkęs jais pasitikėti ar jam nekiltų abejonių tokiu straipsnio ar komentaro socialiniuose tinkluose autoriumi. Taip pat gali būti naudinga patikrinti jų profilio nuotraukas, jei tokių yra. Nuotraukos įkeliamos siekiant sukurti didesnį pasitikėjimą, jos gali būti paimtos iš „Stock" puslapių ir jas galite lengvai rasti internete. Pažvelgus į jas atidžiau, tokios nuotraukos taip pat gali būti sąmoningai neaiškios (redaguotos, tariamas asmuo su saulės akiniais ir pan.), todėl neįmanoma aiškiai identifikuoti asmens.

4. Prokremliškų pasakojimų platinimas.
Rusijos vyriausybė sukūrė savitą pasakojimą apie pagrindinius pastarųjų penkerių metų geopolitinius įvykius. Tai grindžiama principais, įtvirtintais Rusijos Federacijos informacijos saugumo doktrinoje „Dėl valstybės politikos ir oficialios pozicijos Rusijos vyriausybei svarbiais klausimais perteikimo" (2000). Kadangi prokremliški pasakojimai yra plačiai prieinami internetiniuose šaltiniuose, pavyzdžiui, Rusijos užsienio reikalų ministerijos arba Russia Today „Twitter" paskyrose, nesunku patikrinti, ar tos pačios temos atsikartoja įtariamoje paskyroje. Paskyra, kurioje nuolat arba vien tik dalijamasi Rusijos vyriausybės skelbiama informacija, gali būti pagrįstai laikoma prokremliškų pažiūrų.

Jei paskyroje dalijamasi daug arba visais Kremliaus pasakojimais, daromos būdingos kalbinės klaidos ir žmogus apsimeta amerikiečių ar britų naudotoju, tai gali būti Rusijos valdomas trolis.

Kitos galimos užuominos:

• Troliai išlaiko anonimiškumą. Dauguma trolių pasivadina neaiškiu vardu, kuris gali reikšti bet ką – jei jie išvis pasivadina bet kokiu vardu.
• Troliai turi vienkartinius el. pašto adresus. Kadangi daugelyje vietų, kuriose leidžiama komentuoti, reikia įvesti ir el. pašto adresą, troliai apeina šį punktą įvesdami išgalvotus el. pašto adresus. Dauguma vienkartinių el. pašto adresų yra atsitiktiniai ir lengvai pastebimi, nes jie neatspindi tikrojo asmens vardo.
• Trolių tikslas yra sukelti žmonių pasipiktinimą. Jie nėra mandagūs ir nesigėdija veltis į atvirą kovą. Jie prasivardžiuoja, mėtosi kaltinimais ir dažniausiai skamba piktai.
• Troliai naudojasi anonimiškais tarpiniais serveriais. Troliai dažnai naudojasi anoniminėmis programomis arba tarpiniais serveriais, kurie rodo kitokį interneto protokolo (IP) adresą, nei esate įpratę.
• Troliai retai pasako ką nors vertingo viso pokalbio metu. Kai troliai atsako į bendruomenės diskusiją, jie į diskusiją neįneša nieko prasmingo. Vietoj to, jie juokauja, priekaištauja ir įžeidinėja.

Netikros „Facebook“ paskiros

Kaip pastebėti, kad „Facebook“ paskyra yra netikra?

Kitas svarbus dalykas, kurį reikia turėti omenyje, yra netikros paskyros. Paprastai šios paskyros nėra tokios aktyvios kaip troliai ir dažniausiai jos atlieka tylių žiūrovų vaidmenį. Panašūs kriterijai taikomi netikroms paskyroms daugumoje platformų, tačiau šįkart „Facebook“ pasirinkome kaip pagrindinį pavyzdį. Panašu, kad „Facebook“ paskyra yra svarbiausia, nes naudotojai šiose paskyrose dažniausiai dalinasi asmenine informacija. Šios paskyros aktyviai bando tapti jūsų draugais dėl dviejų pagrindinių priežasčių: siekdamos atrodyti tikresnės, nes draugų sąraše turi daugybę tikrų žmonių, ir būti draugais, kad pamatytų daugiau asmeninės informacijos. Priklausomai nuo netikros paskyros tikslų, ji gali būti naudojama renkant asmeninę organizacijos darbuotojų informaciją.

1. Patrauklumo veiksnys.

Ne visos nepažįstamų patrauklių jaunų vyrų arba moterų socialinių tinklų paskyros, kurios kviečia jus tapti draugais, yra netikros, tačiau panašu, kad didžioji dauguma netikrų paskyrų yra būtent tokios. Didesnė tikimybė, kad jie bus priimti į draugų sąrašą ir galiausiai pamatys jūsų asmeninius duomenis.

2. Nedaug įkeltų nuotraukų.

Dauguma netikrų paskyrų neskelbia daug nuotraukų – dažniausiai tris arba keturias, o kartais tai yra skirtingų žmonių nuotraukos. Tiek nuotraukų pakanka siekiant sukurti laikiną iliuziją, kad už paskyros slypi tikras žmogus.

3. Keistos biografijos.

Daugumos netikrų paskyrų biografijose yra labai mažai informacijos arba pateikta informacija atrodo keista. Pavyzdžiui, tai nėra neįmanoma, bet labai mažai tikėtina, kad žmogus gyvenantis Bronkse lankė Helsinkio universitetą, taip pat yra labai jaunas ir dirba Niujorko viešųjų ryšių įmonėje. Greitai patikrinę jo vardą „Google" paieškoje kartu su atvirkštine jo profilio nuotraukos paieška, galite įsitikinti, kad jo paskyra yra netikra.

4. Neatsakomumas.

Jei parašysite netikrai paskyrai žinutę, mažai tikėtina, kad ji atsakys net ir į trumpą klausimą. Geriausia net nebandyti jai rašyti ar kitais būdais užmegzti pokalbį.

5. Dažniausiai tuščia „Facebook" siena.

Apskritai, vieninteliai dalykai, kuriuos rasite vienoje iš šių netikrų „Facebook" paskyrų sienų, yra nauji paspaudimai „patinka" „Facebook" įmonių arba produktų puslapyje ir nauji draugai.

Reagavimas

Norint aktyviai kovoti su dezinformacija internete, reikia atlikti du veiksmus – ją atskleisti ir apie ją pranešti. Organizacija neturėtų vargintis ir viešai paneigti kiekvieną į ją nukreiptą netikrą istoriją, o verčiau turėtų sutelkti dėmesį į teigiamus ir atvirus pranešimus. Strateginis tikslas turėtų būti stipri strateginė įvykius paaiškinanti komunikacija, besiremiant faktais, o ne dezinformacijos atskleidimu ir paneigimu.

Kitų sąmoningumo didinimas

Labai svarbu, kad jūsų kolegos žinotų apie atsirandančią dezinformaciją, nukreiptą į organizaciją. Kiekviena organizacija privalo turėti aiškią tvarką, leidžiančią darbuotojams pranešti apie netikrą istoriją. Pagrindinis šio žingsnio tikslas yra informuoti kolegas, kad tam tikras skleidžiamas pranešimas yra netikras ir užkirsti jiems kelią dalytis istorija bei ja tikėti.

„Facebook“ / „Twitter“ / žiniasklaidos pranešimai

Antras žingsnis – pranešti apie tai socialinių tinklų platformoje. Visos socialinių tinklų platformos turi galimybę pranešti apie istoriją, nurodant konkrečią priežastį, kodėl apie ją pranešama. Jei socialinio tinklo platforma gaus pakankamai naudotojų pranešimų, sukurta istorija arba netikras

pranešimas bus panaikinti. Tai yra metodas, kurį pilietinės organizacijos (dar vadinamos elfais) naudoja kovai su dezinformacija internete. Jei žiniasklaidos priemonės skleidžia netikras istorijas, atsižvelgiant į žiniasklaidos priemonių pobūdį (ar jos yra tikros, ar propagandinės), apie tai reikėtų pranešti arba joms, arba nacionalinėms žiniasklaidos kontrolės institucijoms.

Išplėstinės priemonės ir kreipimasis pagalbos

Galimi du pagrindiniai būdai atskleisti apie sunkesnius dezinformacijos atvejus: pasinaudojant sudėtingesniais atvirojo kodo metodais arba kreipiantis pagalbos į internetinę tyrimų bendruomenę.

Dauguma internetinių priemonių gana lengva naudotis ir jose pateikiamos nuoseklios instrukcijos, kaip jomis pasinaudoti. Toliau pateikiamos dvi didelės ir naudingiausios priemonės:

„Bellingcat Tool Box“: http://bit.ly/2nIBYzF
„Online Open Source Tool Box“: https://start.me/p/Wrrzk0/tools

Kita galimybė yra susisiekti su internetinių tyrimų bendruomene ir pateikti jiems informaciją apie tam tikrą melagingą istoriją. Dauguma tyrėjų mielai demaskuos netikrą istoriją ir pasidalins ją paneigiančiu turiniu internete.

Leidinio sudarytojai:

Lukas Andriukaitis
Tomas Kazulėnas
Linas Skirius

Vilnius, Lietuva
Tiražas – 1000
©CRI, 2022 Lapkritis

Be autorių sutikimo platinti leidinį draudžiama. Dėl galimybės tą daryti galite kreiptis į info@cri.lt