4.

PRARETINKITE SAVO PĖDSAKUS

Jūsų telefono naršyklėje saugoma daugybė informacijos apie jus – jūsų buvimo vietą, ko jūs ieškote internete, kokiose svetainėse jūs lankotės. Ši informacija gali būti perduodama toliau. Jūs galite šiek tiek daugiau kontroliuoti tą informaciją padarydami keletą pakeitimų.

Telefonai, planšetės ir kompiuteriai paprastai mus pasiekia jau su instaliuotomis naršyklėmis, kurioms mūsų privatumas nėra prioritetinis klausimas. Vietoje to jūs galite parsisiųsti ir instaliuoti naršyklę, kuri yra **taip nustatyta, kad išlaikytų didesnį jūsų naršymo internete privatumą** ir taip apsaugotų jus nuo pėdsekių.

Siekiant dar labiau apsaugoti privatumą, jūs galite instaliuoti papildomus įrankius ir priedus (tai yra lengvai instaliuojamos mini programėlės jūsų naršyklei, kurios **gali užtikrinti didesnį jūsų naršymo privatumą**.

Norėdami užblokuoti šnipinėjimo skelbimus ir nematomus pėdsekius, instaliuokite **uBlock Origin** (Chrome, Safari, and Firefox naršyklėms) arba **Privacy Badger** (Chrome, Firefox ir Opera atveju).

Siekdami užtikrinti, kad jūsų prisijungimai prie svetainių būtų kaip įmanoma saugesni, instaliuokite **HTTPS Everywhere**: naršyklės plėtinį, užtikrinantį, kad jūsų komunikavimas su svarbiausiomis svetainėmis yra užkoduotas ir apsaugotas. Jei jūs esate Safari naudotojas, suinteresuotas šia funkcija, savo paieškos varikliu pasirinkite ne Google produktą, pavyzdžiui, DuckDuckGo, kuris jus automatiškai nukreips į užkoduotą ryšį.

5.

NUIMKITE ŽYMĄ NUO SAVĘS IR KITŲ

Ar jūs prisidėjote prie savo draugų duomenų kaupimo uždėdami žymą (angl. tagging) ant jų nuotraukų ir post'ų praeityje? Palengvinkite jų duomenų naštą (kartu nuramindami savo sąžinę), **nuimdami žymę** nuo jų nuotraukų ir post/ų, kur tik galite tai padaryti.

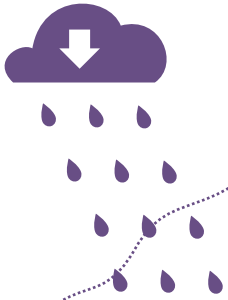
Paskatinkite savo draugus, šeimos nrius ir kolegas prisijungti ir imti kontroliuoti laisvai sklandančius duomenis. Jei mes visi įdėsime pastangų siekiant kontroliuoti mūsų duomenų pėdsakus, mes galėsime daugiau padėti vieni kitiems detoksikuojant duomenis.

A product of TACTICAL TECH

Supported by Firefox

Lietuvos bibliotekininkų draugija

datadetoxkit.org
#datadetox



DATA DETOX KIT

KONTROLIUOKITE SAVO IŠMANIOJO TELEFONO DUOMENIS

siekiant padidinti jūsų privatumą internete

Jei jūs imate galvoti, ką jūsų duomenys kitiems sako apie jus, tai gali nepasirodyti taip jau labai svarbu: kam gali rūpėti, kad jūs esate didelis country stiliaus muzikos gerbėjas, kad jums patinka pirkti daugiau batų nei jums iš tiesų reikia arba kad jūs planuojate savo būsimas atostogas metus į priekį?

Problema yra susijusi su tuo, kas vyksta su jūsų duomenimis. Per ilgesnį laiką iš jų **susiformuoja tam tikri asmeniniai skaitmeniniai modeliai**: jūsų įpročiai, judėjimas, santykiai, pasirinkimai, įsitikinimai ir paslaptys yra atskleidžiamos tiems, kurie visa tai analizuoja ir iš to pelnosi.

Analizuodami šį Duomenų detoksikacijos (angl. Data Detox) rinkinį, jūs sužinosite, kaip ir kodėl visa tai vyksta ir imsitės praktinių veiksmų, siekdami *kontroliuoti savo duomenų pėdsakus internete.

Tad pradėkime!

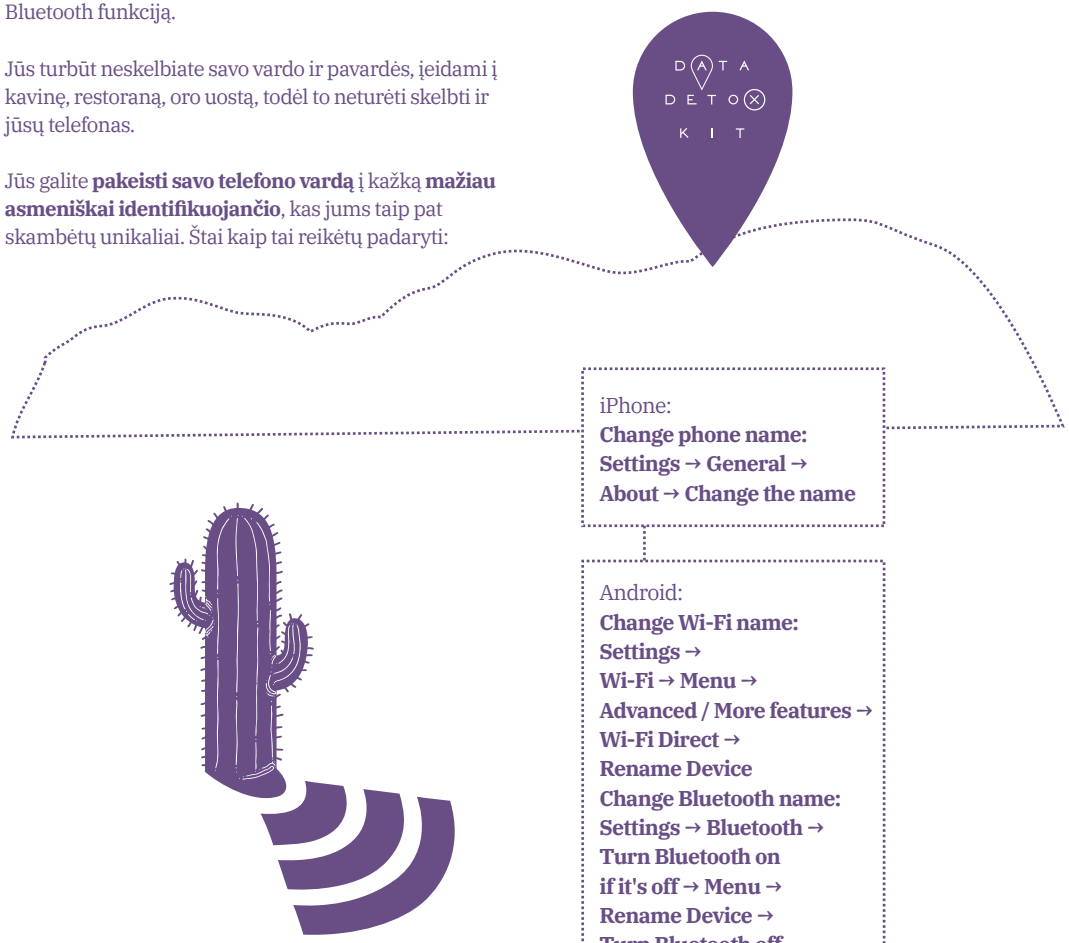
1.

PAKEISKITE SAVO ĮRENGINIO VARDĄ

Kažkuriuo momentu jūs galbūt įvardijote savo telefoną pagal Wi-fi, Bluetooth ar juos abu, o gal pavadinimas buvo automatiškai sugeneruotas tvarkant nustatymus. Tai reiškia, kad „Alekso Chung telefonas“ yra tai, ką gali matyti Wi-Fi tinklo savininkas arba, jei jūsų Bluetooth yra įjungtas, tai mato visi, kas jūsų rajone yra įsijungę Bluetooth funkciją.

Jūs turbūt neskelbiate savo vardo ir pavardės, įeidami į kavinę, restoraną, oro uostą, todėl to neturėti skelbti ir jūsų telefonas.

Jūs galite **pakeisti savo telefono vardą** į kažką **mažiau asmeniškai identifikuojančio**, kas jums taip pat skambėtų unikaliai. Štai kaip tai reikėtų padaryti:



iPhone:
Change phone name:
Settings → General →
About → Change the name

Android:
Change Wi-Fi name:
Settings →
Wi-Fi → Menu →
Advanced / More features →
Wi-Fi Direct →
Rename Device
Change Bluetooth name:
Settings → Bluetooth →
Turn Bluetooth on
if it's off → Menu →
Rename Device →
Turn Bluetooth off

2.

IŠTRINKITE SAVO BUVIMO VIETOS PĖDSAKUS

Nors jums gali atrodyti, kad jūsų buvimo vietos duomenys yra tiesiog truputis atsitiktinės informacijos, kai visa tai matoma kartu, jie gali atskleisti **svarbią informaciją apie jus** ir jūsų įpročius, tokius kaip, kur jūs gyvenate, kur dirbate ir kur jūs mėgstate lankytis su draugais. Gali atrodyti visiškai normalu, kad jūsų maps programėlė gali žinoti, kur jūs esate tam tikru metu. Tačiau jūs nustebtumėte sužinoję, kokiam kiekiui įvairių proramėlių jūs davėte leidimą žinoti jūsų buvimo vietą.

Jūs galite **peržiūrėti kiekvienos programėlės leidimus ir išjungti vietos nustatymo paslaugą**. Paieškokite programėlių, kurios teikia paslaugas visai nebūtinai žinodamos jūsų buvimo vietą (ar tam žaidimui tikrai reikia žinoti, kur jūs esate?) bei tų, kur jūs nepageidaujate, kad jūsų buvimo vieta joms būtų žinoma:

Android:
Settings →Apps → Manage location access on a per-app basis

iPhone:
Settings →Privacy →Location services →Manage location access on a per-app basis

3.

SUSITVARKYKITE SAVO PROGRAMĖLES

Jūsų socialinių medijų programas, žaidimus ir oro prognozių programėles domina jūsų duomenys (data@nbsp)... ir tokių duomenų jos gali surinkti daugybę. **Visokių niekada nenaudojamų programėlių jūsų telefone ištrynimas gali būti galingas būdas detoksikuoti jūsų skaitmeninį „aš“.**

Be to, toks susitvarkymas gali taip pat atlaisvinti vietos jūsų telefone, sumažinti duomenų naudojimą ir prailginti baterijos gyvenimą. Priklausomai nuo programėlės, tai gali netgi pagerinti bendrą veikimą.

Android:
Settings → Apps →
Pasirinkite programėlę, kurią norite pašalinti → Uninstall

iPhone:
Spustelėkite ant programėlės, kol kiekvienos programėlės kairiajame viršutiniame kampe atsiras maži kryžiukai.

Norėdami ištrinti programėlę, spustelėkite mažą tos programėlės kryžiuką.

Norėdami grįžti, paspauskite Home mygtuką.

4.

APSAUGOKITE SAVO VIRTUALIAS VERTYBES

Panašiai kaip jūs rūpinatės savo vertingais daiktais namuose, jūs turėtumėte tą patį daryti ir su savo virtualiai saugoma informacija, ar tai būtų jūsų finansiniai įrašai, jūsų paso skenuotos nuotraukos ar netgi jūsų adresas ir telefono numeris. Visuomet verta pagalvoti, kur jūs saugosite vertingą asmeninę informaciją ir kaip jūs galite ją apsaugoti.

Ištrinti kažką nedidelio yra labai patogu, jei gerdami kavą jūs tiesiog norite padaryti keletą greitų patobulinimų. Susirasti konkrečią informaciją, kuri guli jūsų elektroninio pašto ar kitose paskyrose ir po to ją ištrinti: nuskenuota jūsų tapatybės kortelė, banko duomenys ar jūsų sveikatos draudimo informacija, t.t. Jei šių duomenų jums reikės vėliau, jūs visuomet galite juos parsisiųsti arba atsispausdinti prieš ištrindami juos iš savo elektroninio pašto paskyros.

Giluminis valymas yra kruopštesnis procesas. Jis turėtų būti atliekams maždaug kartą per metus. Suarchyvuokite viską, ką turite sukaupę savo elektroninio pašto ar socialinų tinklų paskyroje, parsisiųskite visa tai į savo kompiuterį ir ištrinkite savo paskyros turinį, kad vėl galėtumėte „pradėti viską iš naujo“.

Patarimas: Vien ištrinti nepakanka – jūs dar turite ištuštinti šiukšliadėžę ir pažalinti laikinus failus!

Jūs patys turite nuspręsti, ar norite turėti savo archyvo ir dokumentų atsarginę kopiją debesyje, išsaugoti visa tai išoriniame kietajame diske ar USB atmintuke. Nepriklausomai nuo to kaip jūs tai saugosite, įsitikinkite, kad viso to neprarasite, kad pasirinkote stiprų slaptažodį, kuris jums kažką reiškia.

5.

PERDUOKITE TAI KITIEMS

Nors apie tai dažnai užmirštame, žiniatinklis (angl. web) taip yra pavadintas ne be pagrindo. **Mus visus internete jungia** įvairūs tinklai. Esame ne vien tik „draugai“ socialiniuose tinkluose, bet taip pat esame susieti ir per kontaktus mūsų elektroninio pašto paskyrose bei per nuotraukas, kuriomis dalijamės.

Kai imsite valyti savo elektroninio pašto ir socialinių tinklų paskyras, pagalvokite, ką dar jūs galėtumėte parsisiųsti ir po to ištrinti, siekiant padėti jūsų draugams ir bendradarbiams. Pvz., jūsų sesers banko duomenis, užrakto kodą patekimui į jūsų biurą, galbūt jūsų sūnaus paso skenuotą nuotrauką, – visa tai yra tik keletas pavyzdžių, kas galėtų sukelti tikrą galvos skausmą, jei netikėtai patektų į blogas rankas.

Perduokite tai kitiems! Jūsų skaitmenį saugumą galima sustiprinti tesiog atliekant keletą paprastų pagrindinių veiksmų. Pasidalinkite šiuo Duomenų detoksikacijos (Data Detox) patarimų rinkiniu su savo draugais, šeimos nariais, kolegomis. Galbūt tai padės jiems pakeisti savo įpročius taip, kaip tai jiems atrodo prasminga.

DATA DETOX KIT

PAKEISKITE NUSTATYMUS

kad apsaugotumėte savo nuomenis

Jei internetas būtų vien tik vieta, kur žmonės keičiasi šunų, vilkinčių dinozaurų kostiumus, nuotraukomis, slaptažodžių poreikis nelabai būtų ir juntamas. Tačiau internetas yra ta vieta, kur jūs apmokate sąskaitas, kur patalpinami jūsų vaistų receptai ir kur jūs registruojatės rengdamiesi balsuoti rinkimuose.

Gerai pagalvojus apie visas jūsų „virtualias vertybes“, kurios pasiekiamos interneto pagalba ir kurias jūs saugote savo įrenginiuose – **argi jūs neturėtumėte jų laikyti taip pat saugiai kaip ir savo piniginės ar raktų?**

Vienas ir paprastų būdų užkirsti kelią kitiems lengvai pasiekti jūsų virtualias vertybes – **tai neleisti jiems lengvai nuspėti jūsų slaptažodžių**. Daugybei žmonių net nereikia specialių techninių įgūdžių, kad patektų į jūsų paskyras – jie tiesiog pamėgina keletą kartų atspėti jūsų slaptažodžius ar paleidžia automatinę programą.

Kuomet jie jau gali patekti į jūsų paskyrą, jie gali pamėginti panaudoti tą kompromisinį slaptažodį ir kitoms paskyroms, surinkti infomaciją apie jus ir jūsų įpročius, perimti jūsų sąskaitas ar netgi pasinaudoti jūsų skaitmenine tapatybe.

Analizuodami šiuo Duomenų detoksikacijos (angl. Data Detox) rinkiniu jūs išmoksite praktinių veiksmų savo saugumui internete sustiprinti.

Taigi pradėkime!

A product of TACTICAL TECH

Supported by Firefox

Lietuvos bibliotekininkų draugija

datadetoxkit.org
#datadetox

1.

UŽRAKINKITE SAVO SKAITMENINES DURIS

Ekrano užraktai: slaptažodis, derinys, piršto antspaudas ar veido atpažinimo funkcija, kuria jūs naudojatės norėdami patekti į savo įrenginį, yra tam tikra **geriausia jūsų apsauga** nuo tų, kurie galėtų būti suinteresuoti patekti į jūsų įrenginį. Tačiau šių priemonių yra daugybė ir kartais gali būti sunku išsirinkti, kuri jums yra tinkamiausia.

Bet koks jūsų telefono, planšetės ar kompiuterio užraktas suteikia tam tikrą apsaugą ir yra geriau negu nieko. Panašiai, kaip ir durų spynų atveju, **kai kurie ekrano užraktai yra stipresni už kitus.**

Iš visų čia paminėtų užraktų ilgi, unikalūs slaptažodžiai yra stipriusi. Tai reiškia, kad, jeigu jūs naudojate slaptažodį savo įrenginiui atrakinti, jis turi susidėti iš raidžių, skaičių ir specialių simbolių.

Sakykime, jūs savo telefoną atidarote tiesiog perbraukdami per ekraną. Jūs galite padidinti jo saugumą nustatydami ilgą slaptažodį. Ar galbūt jūs naudojate kažkokį derinį? Galbūt tuomet vertėtų jį prailginti? Jūsų slaptažodis yra 1234? Gal tuomet tiesiog vertėtų mesti kauliuką septynis kartus ir įsiminti tą slaptažodį?

2.

ĮSILEISKITE TINKAMĄ

Sukurti puikų slaptažodį yra lengva. Jums tiesiog reikia laikytis keleto pagrindinių principų. Jūsų sklaptažodžiai turėtų būti:

Ilgi: **jie turi susidėti iš ne mažiau kaip aštuonių simbolių. Dar geriau būtų 16-20 simbolių.**

Unikalūs: **kiekvienai svetainei naudojami slaptažodžiai turėtų būti skirtingi.**

Parenkami atsitiktinai: **jūsų slaptažodžiai neturėtų būti kažkokie loginiai deriniai, kuriuos lengva nuspėti. Čia jums gali labai padėti slaptažodžių generatorius (angl. password manager).**

Stipriausiuose slaptažodžiuose naudojamos raidžių, skaičių ir specialių simbolių kombinacijos. Šis laiko išbandytas patarimas padeda sukurti stipresnius, sunkiau nuspėjamus slaptažodžius. Tenka apgailestauti, kad kai kurios slaptažodžių sistemos neleidžia naudoti tam tikrų specialių simbolių (pavyzdžiui, @#$%-=+), tačiau ilga raidžių ir skaičių kombinacija vistiek yra geriau nei trumpa.

Idealiu atveju jūs turėtumėte naudoti **slaptažodžių generatorių**, kuris jums sugeneruos slaptažodžius ir visus juos saugos. Slaptažodžių generatoriai, tokie kaip 1Password ir KeePassXC, rekomenduojami saugos ekspertų, iš esmės yra programėlė, kurios vienintelis tikslas yra apsaugoti jūsų kredencialus ir kitus jautrius duomenis.

3.

PRIDĖKITE ANTRĄ UŽRAKTĄ

Dviejų veiksnių atpažinimo (2FA) arba daugialypio atpažinimo (MFA) sistemos nustatymas reiškia, kad net jei kažkas ir suras jūsų slaptažodį, **jie greičiausiai neturės reikiamo papildomo veiksnio, kad galėtų patekti į įrenginį.**

Pmėginkite pasižiūrėti į jūsų dažniausiai naudojamos svetainės saugumo nustatymus ir programėles, ar nėra galimybės sukurti tokį papildomą užraktą. Pradėkite nuo pačių svarbiausių – finansinių programėlių ar paslaugų, tokių kaip elektroninis paštas, kurias jūs naudojate norėdami atkurti kitas savo paskyras.

Google:
Sign in to: myaccount.google.com →
Security →
2-Step Verification →
Get Started

Facebook:
Menu →
Settings →
Security and Login →
Use Two-factor Authentication

Patarimas: Kuriant kitą patikrinimo sluoksnį, jums reikės rasti būdą patvirtinti, kad tai jūs. Venkite naudoti SMS (į jūsų telefono numerį atsiunčiamas teksto žinutes) kaip antrąjį veiksnį, jei netikėtai pamestumėte savo telefoną. El.paštas paprastai yra patikimesnis variantas.

5.

IEŠKOKITE TIESOS INTERNETE

Terminas „melagingos naujienos“ yra naudojamas apibūdinti įvairiai netiksliai ar klaidinančiai informacijai, įskaitant satyrą, prastai ištirtą ar nepatikrintą turinį, melagingas žinutes ir suktybes. Melagingos naujienos ne visada skleidžiamos piktavališkai, tačiau, nežiūrint į tai, kodėl žmonės jomis dalijasi, rezultatas paprastai yra tas pats: naujienas gaunantys žmonės mano, kad tai, kas nėra teisinga, yra tiesa arba kad atsitiko tai, ko iš tikrųjų niekada neatsitiko.

Geriausiu atveju tai gali būti juokingas memas. Blogiausiu atveju tai gali būti netiksli informacija apie sveikatą arba klaidinga politinė informacija.

Net ir dedant visas pastangas išanalizuoti perskaitytus straipsnius ir užduoti svarbius klausimus apie juos, jums vis tiek gali kilti painiavos pojūtis. Tačiau žinokite: jūs ne vienas toks!

Patarimas. Pasitelkite visą įmanomą pagalbą
Vien dėl to, kad interneto svetainė neprisipažįsta daranti klaidų, dar nereiškia, kad ji jų nedaro. Iš tiesų patikimiausi leidiniai yra tie, kurie ypač atsargiai elgiasi su tiesa ir kuriuose dirba žmonės arba ištisi departamentai, kurių vienintelis darbas – tikrinti faktus.

Ieškokite skaidrių šaltinių, kurie nebijo paneigti informacijos, kai susivokia suklydę. Dar geriau, jei atnaujinta informacija yra apibendrinama straipsnio viršuje ir pateikiama socialiniuose tinkluose.

6.

SUSPROGDINKITE SAVO FILTRO BURBULĄ

Kai interneto svetainės ir programėlėse sukuria jūsų profilį ir išsiaiškina jūsų interesus, jūs galite atsidurti **filtro burbule**.Taip yra tada, kai jums yra pateikiama daugiau pasakojimų, panašių į tuos, į kuriuos jūs jau investavote. Kaip tai apriboja arba keičia tai, ką jūs girdite?

Filtro burbulai gali paskatinti žmones perkaityti visiškai kitokias istorijas, naujienų antraštes, straipsnius ir reklamą, o tai gali reikšti, kad jie gaus informacijos rinkinius, kurie neturi nieko bendro, kaip tai yra pademonstruota interaktyviajame straipsnyje „Blue Feed“, „Red Feed“ (graphics.wsj.com/blue-feed-red-feed).

Jei jūs išsiaiškinote, kad savo programėlių ir interneto svetainių filtrų burbuluose matote algoritmu apdorotą turinį, kyla klausimas: o kaip gi išeiti už to filtro burbulo ribų?

Patarimas. Keiskite vėjo kryptį ir permaišykite savo naujienas
Geras būdas susprogdinti filtro burbulą – tai užsisakyti paslaugas, kurios atrenka žinias ir informaciją iš įvairių šaltinių ir pateikia visa tai iš įvairių perspektyvų. RSS šaltiniai, forumai ir adresatų sąrašai, kuriuose pateikiama daug įvairių nuomonių ir temų, gali padėti jums pažvegti už savo burbulo ribų.„Global Voices“ (globalvoices.org) ir „The Syllabus“ (the-syllabus.com) būtų puikus pasirinkimas pradžiai.

DATA DETOX KIT

6 PATARIMAI, PADĖSIANTYS IŠVENGTI INTERNETE SKLEIDŽIAMOS DEZINFORMACIJOS

Taikomosios programos, interneto svetainės ir internetinė žiniasklaida gali būti puiki platforma, norint gauti naujienas, gyvenimiškus patarimus ir ieškant pramogų. Tačiau, žvelgiant į visą tą gausų turinį, gali būti sunku nesiblaškant tiesiog rasti tai, ko jūs iš tikrųjų ieškote.

Be to, internete susidūrus su vaizdo įrašu, nuotrauka ar straipsniu, gali būti sunku atskirti tikrus faktus nuo pramano. Nuo asmenybės testų, kuriose bandoma priskirti jus kažkuriam asmenybės tipui, iki šokiruojančių antraščių ir pakeistų nuotraukų ar vaizdo įrašų, kurie gali jus įtikinti, kad realybė yra visiškai kitokia. Taigi, ką matote internete, ne visada yra tai, kaip jums gali atrodyti.

Šiame „Duomenų detoksikacijos“ (angl. Data Detox) projekte jūs galėsite panagrinėti su dezinformacija susijusias temas ir terminus, taip pat gausite patarimų, kaip tarp viso to rasti tai, ko ieškote.

Pradėkime!

datadetoxkit.org **#datadetox**

A product of TACTICAL TECH

Project partners Save the Children 100 ANNI IFLA

Funded by the European Union

1.

SUVOKITE SAVO GALIĄ, KAD GALĖTUMĖTE KELTI BANGAS

„Patinka" paspaudimas, tviterio pranešimų persiuntimas ar pasidalijimas post'u – visi šie veiksmai atskleidžia, kaip jūs sąveikaujate su tuo, ką matote internete, o jūsų sąveikavimas turi didelę reikšmę. Kai paveikslėlis, vaizdo įrašas ar post'as pritraukia pakankamai didelį žmonių skaičių, jis sparčiai plinta ir iš esmės tampa „virusiniu" (angl. viral).

Pasiteiraukite savęs: „Kokia yra mano įtaka internete?" Kada paskutinį kartą jūs matėte šokiruojantį ar juokingą straipsnį, antraštę, vaizdo įrašą ar atvaizdą ir per kelias sekundes jau persiuntėte jį savo draugams? Tyrėjai nustatė, kad labiausiai tikėtina, jog „virusiniais" taps pasakojimai ir vaizdai, kurie jums kelia baimę, pasibjaurėjimą, susižavėjimą, pyktį ar nerimą. Visdėlto, jei taip jums nutiko kaip tik šį rytą, nesijauskite blogai!

Patarimas. Dalintis reiškia rūpintis
Dalijimasis yra viena iš dalyvavimo formų. Kažkuo (bet kuo) pasidalindami su kitais, jūs prisidedate prie tikimybės, kad tai gali tapti „virusiniu" reiškiniu. Jei paaiškėtų, kad informacija yra, pavyzdžui, klaidinga, ar jūs tikrai norite, kad su ja būtų siejamas jūsų vardas ir reputacija? Prieš pasidalydami nuoroda apsvarstykite, ar gali nutikti taip, kad jūs paskleisite netiesą, kažką destruktyvaus ar toksiško.

2.

GERAI PAGALVOKITE PRIEŠ ATLIKDAMI ASMENYBĖS TESTĄ

Kada paskutinį kartą jūs matėte testą (teksto arba nuotraukos pavidalu), pavadintą, pavyzdžiui:

- Į kokį gyvūną jūs esate panašus?
- Koks Disney veikėjas esate jūs?
- Kokios yra jūsų tobulos atostogos?
- ... ir taip sąrašą galima tęsti be galo!

Nors tikimybė, kad tai tiesiog smagus testas, kuriuo siekta paskatinti jus susidomėti, išlieka, taip pat gali būti, kad klausimai buvo kruopščiai parengti siekiant surinkti duomenis, norint suklasifikuoti jūsų asmenybę, remiantis vadinamaisiais psichometriniais modeliais.

Jūsų atsakymai į testo klausimus, kaip antai „Kuris Simpsonų personažas esate jūs?", kartu su kitais jūsų įpročiais, kuriuos gali stebėti jūsų naršyklė, taikomoji programėlė ar kokie nors susiję dalykai, pvz., lojalumo kortelės, duomenų analitikams gali suteikti galimybę suprasti, koks žmogus jūs esate, kas jums rūpi ir kaip daryti įtaką jums, kad jūs nusipirktumėte batų porą (pavyzdžiui,)... arba netgi sukurti jūsų profilį, kad būtų galima nuspręsti, kaip jums bandyti daryti įtaką, kad jūs atitinkamai balsuotumėte kituose rinkimuose.

Patarimas. Labiau saugokite paslaptis
Kai jūs galvojate apie asmeninę informaciją, pirmiausia jums į galvą gali ateiti jūsų slaptažodžiai, identifikacijos numeris ir banko sąskaitos numeris. Tačiau tam tikra informacija apie jus, pavyzdžiui, kas jus baugina, erzina ir kokie yra jūsų siekiai, yra tokia pat asmenininė informacija. Šie duomenys gali būti vertingi analitikams, kadangi jie suteikia informacijos apie tai, prie kokio asmenybės tipo jus reikėtų priskirti. Prieš pateikdami tokią informaciją apklausoje ar atlikdami testą gerai pagalvokite.

3.

NEUŽKIBKITE ANT JAUKO

Antraštinis jaukas (angl. click bait) – tai terminas, kuris yra naudojamas apibūdinti perspaustoms (sensacingoms), nesąžiningoms arba dirbtinai sukurtoms antraštėms, kurios yra sukurtos paskatinti žmones spustelėti antraštę arba nuorodą. Kuo daugiau veiksmo rezultatų gaunama iš straipsnio, vaizdo įrašo ar nuotraukos, tuo daugiau lėšų galima uždirbti. Tai reiškia, kad kūrėjai yra motyvuoti teigti bet ką, kad tik jūs spustelėtumėte mygtuką arba pasidalytumėte jų turiniu.

Remdamiesi jūsų asmenybės profiliu, kurį sukūrė jūsų naudojamos platformos (pvz., „Facebook" ir „Instagram"), jūs galite gauti individualizuotas antraštes, kurios sukurtos taip, kad paveiktų jūsų emocijas ir kad jūs spustelėtumėte mygtuką.

Tokį jauką galima rasti šalia dezinformacijos, tačiau ne visada. Kai jūs tik pradėsite atpažinti „antraštinį jauką", pradėsite pastebėti jį visur YouTube kanale, tinklaraščiuose ir tabloidėse.

Patarimas. Suraskite šaltinį
Susidūrę su „antraštiniu jauku", nesustokite prie antraštės. Jei nuoroda atrodo saugi, spustelėkite ją ir perskaitykite visą straipsnį. Sužinokite, kas yra autorius, kada straipsnis buvo išspausdintas ir kokiais šaltiniais jis remiasi. Gali būti, kad straispnio viduryje jūs rasite pastabą, kad turinys ar reklama yra mokami, arba jis gali priklausyti nuomonių kategorijai. Šie duomenys gali padėti jums nuspręsti, ar dėl viso to verta švaistyti jūsų energiją.

4.

STEBĖKITE, AR TAI NĖRA MELAGINGOS NAUJIENOS („FAKES")

Gilios melagingos naujienos (angl. deep fakes) – tai skaitmeniniu būdu pakeisti vaizdo įrašai, garso klipai arba nuotraukos, paprastai sukuriamos pakeičiant asmens veidą, judesius arba keičiantys jo žodžius. Nors sąvoka „gilios melagingos naujienos" yra nesenas terminas, iš tiesų viena ar kita forma jos egistavo per amžius (kaip, pvz.1917 m.„Cottingley fairies" nuotrauka arba 1994 m. filmas „Forestas Gampas" (angl. Forrest Gump). Dar lengviau yra sukurti vadinamąsias **pigias melagingas naujienas (angl. cheap fakes)** – klaidinantį turinį, kuriam nereikia sudėtingų technologijų. Jį galima sukurti tiesiog suteikiant klaidingą pavadinimą nuotraukai ar vaizdo įrašui arba naudojant pasenusį turinį dabartiniam įvykiui iliustruoti.

Patarimas. Likite nuleidę inkarą ir pasidomėkite
Kaip ir tuomet, kai susiduriate su „antraštiniu jauku", nieko nepriimkite už gryną pinigą. Jei matote vaizdo įrašą arba nuotrauką, kuri jus stebina arba šokiruoja, atpažinkite tą jausmą ir pagalvokite, galbūt už to slypi kažkas daugiau nei jūs matote. Kitu atveju, jei pastebėjote, kad vėl ir vėl vis susiduriate su tuo pačiu vaizdu arba juo su jumis buvo ne kartą pasidalinta, tai gali būti priežastis pasigilinti į tikrąjį informacijos šaltinį. Verta užduoti daugiau klausimų: kas paskelbė informaciją (kuri interneto svetainė, kas jos autorius)? Kada ji buvo paskelbta?Jei tai yra vaizdas, atlikite atvirkštinio vaizdo paiešką TinEye sistemoje ir pažiūrėkite, kur dar jį surasite.

Prieš nuspręsdami, kad naujienos yra teisingos ir prieš pasidalindami jomis su draugais ir šeimos nariais, atlikite jų kryžminį patikrinimą su kitais patikimais naujienų šaltiniais.