Interneto žemėlapis: interneto medijų raštingumo metodologinė priemonė mokytojams

Autoriai:
Laura Gintalaitė, Džina Donauskaitė, Akvilė Venckutė, Ignas Krasauskas

Recenzentas: Marius Pareščius

Kalbos redaktorė: Jurgita Radzevičiūtė

Vilnius, 2019

Turinys

1. Interneto infrastruktūra 3
UŽDUOTYS 5
ŠALTINIAI 6
2. Duomenų rinkimas internete 7
2.1 Didieji duomenys 7
2.2 Ką galima daryti su duomenimis? 8
2.3 Sekimas komerciniais tikslais 9
2.4 Valstybių institucijų vykdomas sekimas 9
2.5 Sekimas nusikalstamais tikslais 11
UŽDUOTYS 12
ŠALTINIAI 13
3. Duomenų šaltiniai 14
3.1 Metaduomenys 14
3.2 Naršyklės kaip duomenų šaltinis 16
3.3 Slapukai 16
3.4 Nešifruotos svetainės 17

3.5 Mobiliosios programėlės 17
3.6 Elektroninis paštas 18
3.7 Dirbtinis intelektas 18
UŽDUOTYS 19
ŠALTINIAI 19
4. Didesnį privatumą užtikrinančios paslaugų internete alternatyvos 20
4.1 Techninis saugumas vs. privatumas 20
4.2 Naršyklių nustatymai ir alternatyvos 21
4.3 Paieškos sistemos 22
4.4 Elektroninio pašto duomenų šifravimas 23
4.5 Alternatyvios mobiliosios programėlės 24
4.6 Slaptažodžių kūrimo ypatumai 24
UŽDUOTYS 28
ŠALTINIAI 28
5. Socialinių tinklų ypatumai 29
5.1 Melagingos žinios 31
5.2 Neapykantos kalba 34
5.3 Patyčios 35
5.4 Sekstingas 36
UŽDUOTYS 39
ŠALTINIAI 41
6. Hakeriai, interneto chuliganai ir nusikaltėliai 43
UŽDUOTYS 47
ŠALTINIAI 47
7. Duomenų apsauga Europoje ir Lietuvoje 48
7.1 Kas yra BDAR 48
7.2 Kokias teises įtvirtina BDAR 49
7.3 Didieji interneto koncernai ir BDAR 51
7.4 BDAR – daugiau atskaitomybės ir atsakomybės 51
UŽDUOTYS 52
ŠALTINIAI 53
Apie autorius 55

1. Interneto infrastruktūra

Suformuoti vaizdų ir suprantamą interneto apibrėžimą gali būti nemenkas iššūkis. Kompiuteriai, planšetės, išmanieji laikrodžiai ar telefonai – tai daiktai, kuriuos galima pačiupinėti, o štai interneto ryšys iki mūsų prietaisų nebūtinai atkeliauja plika akimi matomais kabeliais – jis gali atkeliauti mobiliuoju ar palydoviniu ryšiu. Be to, interneto ryšiui, vaizdžiai tariant, netrūksta magijos.

Galima pabandyti internetą įsivaizduoti kaip didžiulį miestą, megapolį, turintį daugybę įvairios paskirties ir architektūros pastatų – sporto rūmų, koncertų salių, gyvenamųjų kvartalų, butų, sandėliukų ar apleistų užmiesčio namukų. Kiekvienas namas turi adresą, o visus juos į vieną tinklą jungia gatvės, metro ar troleibusų linijos, šaligatviai, takai ir takeliai. Taip pat ir mūsų kompiuteriai, planšetės, telefonai, išmanieji laikrodžiai bei kiti prietaisai ryšiu susijungia į vieną tinklą. Interneto greitkelį (t. y. po visą pasaulį išvedžiotą kabelį) kompiuteris pasiekia jungdamasis įvairia tinklo įranga, dažniausiai tam naudojamas maršruto parinktuvas (angl. router), suteikiantis prieigą interneto tiekėjo (angl. Internet Service Provider) dėka. Kaip ir daugiafunkciai kompiuteriai, įvairūs daiktai – automobiliai, laikrodžiai, šaldytuvai ar net lygintuvai – yra prijungiami prie interneto, taip juos galime stebėti ar valdyti nuotoliniu būdu. Todėl internetas jau vadinamas ir daiktų internetu.

Miestuose esama gyvenamųjų namų ir žmonėms įvairiausias paslaugas teikti skirtų pastatų (bankų, darželių, prekybos centrų, ligoninių ir t. t.). Didžioji dalis kompiuterių ir kitų prietaisų daugiausia tik naudojasi internetu teikiamomis paslaugomis, o kita dalis kompiuterių paslaugas teikia. Pastarieji dar kitaip vadinami serveriais. Jų paskirtis – aptarnauti kiekvieną kompiuterį ar išmanųjį prietaisą, pasibeldžiantį į serverio duris (pavyzdžiui, kai prašoma atidaryti dominantį internetinį puslapį), taip pat kaupti ir saugoti duomenis apie tokį kompiuterį, kaip paslaugos gavėją. Elektroniniai laiškai, kuriuos gauname į internetu pasiekiamas savo elektroninio pašto dėžutes, saugomi serveriuose, o ne mūsų kompiuteriuose (nors kartais būna retų išimčių, kad laiškų kopijas saugo ir mūsų įrenginiai). Kai nutrūksta interneto ryšys ar neveikia serveris, laiškų nei išsiųsti, nei gauti, nei peržiūrėti mums nepavyksta.

Internetu paslaugas teikiančios įmonės ar organizacijos gali turėti nuosavą serverį, keletą serverių arba net visą serverinę ar duomenų centrą, kuriame į vieną tinklą sujungiami tūkstančiai serverių. Didieji duomenų centrai elektros gali sunaudoti tiek, kiek nedideli miesteliai. Amerikiečiai buvo suskaičiavę, kad visi kartu JAV esantys duomenų centrai išeikvojo 2 proc. šalyje per metus sunaudotos energijos. Veikiantys duomenų centrai gerokai įšyla, todėl jiems prireikia galingų aušintuvų. Dėl klimato kaitos susirūpinę žmonės nerimauja, kad duomenų centrai prisideda prie klimato atšilimą sukeliančio šiltnamio efekto.

Viena pelningiausių interneto įmonių yra „Alphabet“ – puikiai visiems žinomų „Google“ paieškos sistemos, „Google“ žemėlapių, „Gmail“ elektroninio pašto ir „Youtube“ savininkė. Ji turi net 14 didžiulių duomenų centrų visame pasaulyje – Šiaurės ir Pietų Amerikoje, JAV, Europoje, Azijoje. Juose – maždaug milijonas serverių, kuriuose saugoma informacija apie nemažą dalį pasaulio gyventojų

Tiesa, reikia trumpai pristatyti ir interneto mieste vykstančius magiškus dalykus, kurie šiek tiek primena miestus iš knygų apie Harį Poterį – čia klesti baltoji ir juodoji magija. Esama namų vaiduoklių, kurie atsiranda ir išnyksta vien to panorėję, pastatų, kurie gali akimirksniu persikelti iš vienos vietos į kitą, pastatų, kurie be vargo keičia savo adresus. Tiesą pasakius, adresus, vadinamus IP (interneto protokolo) adresais, keičia kiekvienas elektroninis prietaisas tada, kai iš naujo jungiamasi prie interneto. Ne vienas prie tinklo prisijungęs kompiuteris tuo pat metu gali svečiuotis duomenų centruose, esančiuose skirtinguose ir vienas nuo kito gerokai nutolusiuose pasaulio kampeliuose. Jei, pavyzdžiui, aktyviai naudojamasi „Facebook“, „Google“ ar „Gmail“, kompiuteris šių paslaugų duomenų centruose jau ne kartą pabuvojo ir ten paliko informacijos apie vartotoją bei jo veiklą internete. Ir gal tai padarė net keliskart per dieną.

Keliautojai miestų gatvėmis lengvai pastebi aplinkui iškilusius pastatus. Pastatuose esantys žmonės keliautojus taip pat gali stebėti pro langus ar prieangiuose įrengtas kameras. Keliautojams tinklu taip pat neįmanoma likti nepastebėtiems. Jei kada savo prietaisu mėginote prie interneto prisijungti viešoje vietoje, turbūt pastebėjote, kiek daug esama skirtingų ryšio galimybių, bet prisijungti galite tik prie to interneto tiekėjo, kurio slaptažodį turite. Tad kompiuteriai vienas kitą pastebi. Tačiau į kiekvieno mūsų namus neįmanoma patekti tiesiog iš gatvės, jei prašalaitis neturi raktų, o durys užrakintos ir niekas jų neatidaro. Lygiai taip pat ir internetas ar internetu teikiamos paslaugos į mūsų prietaisus atkeliauja tik tada, kai jiems atlapojame duris.

Visas stebuklingas kompiuterių ir kitų elektroninių prietaisų galias vartotojai gali panaudoti ir geriems, ir blogiems tikslams. Kadangi interneto infrastruktūra atrodo painoka, dažnai interneto miestų naujakuriai baiminasi grėsmių. Todėl įtikinamos atrodo teorijos apie neatitaisomą technologijų žalą, neišvengiamus pavojus, kai nėra galimybių apsisaugoti, trūkinėjančius ir paviršutiniškais virstančius socialinius santykius. Be abejo, technologijos turi poveikį socialiniams santykiams, o naudotis tinklu rizikinga. Bet ir gyvenimas anapus virtualios erdvės yra rizikingas.

Vis dėlto vargu ar daugelis norėtume grįžti į iki technologinius laikus, kai nebuvo interneto, galėjusio padėti greičiau tvarkyti reikalus ir bendrauti. Be to, internete, kaip ir dideliuose miestuose, verda kultūrinis, mokslo gyvenimas, vyksta prekyba ir mainai. Ryšys mums atveria labai įdomių galimybių, todėl interneto miestas – puiki vieta, kurioje verta turiningai leisti bent dalį savo laiko.

Kita vertus, toli nenuves ir naivus entuziazmas. Internete, kaip ir bet kuriame didmiestyje, netrūksta keistų, pavojingų užkaborių. Po juos saugumo sumetimais geriau nelandžioti. Puikiai suprantame: tikrovėje taip pat ne visus praeivius ir ne visada verta įsileisti į namus. Lygiai tos pačios taisyklės galioja ir virtualiam interneto miestui.

Naršydami internete, pasivadinę išgalvotais vardais, kartais galime pamanyti esantys anonimai, o tapatybės niekam nežinomos. Tačiau yra ne visai taip. Arba – tiksliau – yra visiškai ne taip. Kompiuterių IP adresai ar rankinėje pūpsantis mobilusis telefonas gali gan tiksliai bet kam, turinčiam prietaiso IP adresą, parodyti, kur naudodamiesi internetu esame fiziškai. Tai galima padaryti be vargo prieinamomis priemonėmis internete. Jei kas nors turi gudresnę programinę įrangą ar priėjimą prie duomenų bazių, saugančių interneto tiekėjų duomenis, prisikapstys ir prie tikslaus namų adreso. Taip pat yra ne vienas būdas kitų žmonių IP adresams sužinoti ir kiekvienas galime juos neblogai išmanyti.

Kitas dalykas – serveriai beveik visais atvejais, kai norime pasinaudoti jų paslaugomis, o mūsų kompiuteriai beldžiasi jiems į duris, renka informaciją apie mus ir fiksuoja veiklą internete. Dažniausiai tai daroma dėl dviejų priežasčių – technologinių (kai siekiama pagreitinti interneto ryšį) ir komercinių (kuo pardavėjas daugiau žino apie pirkėją, tuo sėkmingesni pardavimai, nes laiku gali pasiūlyti trūkstamą produktą). Tačiau gali būti ir kitokių motyvų – pavyzdžiui, duomenys renkami, kai persekiojama dėl asmeninių priežasčių ar siekiama įvykdyti nusikaltimą, norima pajungti jūsų kompiuterio resursus internetinėms atakoms, teisėsaugos organų vykdomo sekimo atvejais ir panašiai.

Vadinasi, kiekvienam interneto vartotojui kyla dvi problemos – saugumo ir privatumo. Apie pirmąją svarbu pasakyti, kad būti visiškai saugiam neįmanoma, tačiau yra nemažai būdų labiausiai sumažinti riziką. Šiuolaikinės technologijos rizikingos tiek pat, kiek rizikinga mūsų senai gerai nevirtualiai tvirtovei nukentėti nuo savo bičiulio. Kai XIX a. vyko industrializacija, žmonės masiškai iš kaimų kraustėsi į miestus, nusikaltimų juose netrūko – niekas gerai nežinojo, kaip užtikrinti saugumą pasikeitusioje aplinkoje. Bet ilgainiui mums pavyko išmokti valdyti ir gerokai sumažinti riziką – apšvietėme gatves, pradėjome rakinti būstų duris, mūsų saugumui užtikrinti pradėjo patruliuoti policija, išmokome esminių savisaugos principų. Kraustantis į interneto miestus teks iš naujo mokytis, kaip gyventi saugiai.

Panašiai ir dėl privatumo. Kiekvienas žmogus turi teisę į privatų gyvenimą. Privatumas reikalingas, kai norime apsaugoti intymius gyvenimo aspektus: juk miegamajame užtraukiame užuolaidas, maudydamiesi užsirakiname vonios kambario duris, svečių savo namų svetainėje taip pat nepasitinkame nuogi ar vilkėdami vien apatiniais, o į uždarus vakarėlius kviečiame tik artimus žmones. Viskas atrodo savaime suprantama, tačiau interneto miestuose neįtikėtinai didelė žmonių dalis tuo, kas privatu ir intymu (todėl nesidalytina), dalijasi stebimi svetimų akių. Ir, deja, apie tai nenutuokia.

Svarbu susirūpinti privatumu ir dėl profesinės veiklos ir karjeros perspektyvų. Ieškodami darbo, keisdami jį, siekdami paaukštinimo norime būti matomi kaip patikimi ir lojalūs profesionalai, turintys nepriekaištingą darbo kultūrą, o ne atrodyti, pavyzdžiui, kaip vakarėlių liūtai (nebent reikėtų organizuoti vakarėlius ar būti liūtais). Be to, apie visas mūsų sveikatos problemas tikrai nebūtina žinoti kolegoms, darbdaviams, vis dėlto jei mūsų internetinės paieškos rezultatai taptų prieinami, gali atrodyti labai iškalbingi.

Trečia, gyvename bendruomenėje, esame politiniai gyvūnai. Linkstame susidaryti nuomonę apie įvairius reikalus, o gavus daugiau informacijos galbūt teks ją keisti. Kasdien priimame įvairiausius sprendimus, formuluojame tikslus, jų siekiame, tobulėjame, šviečiame kitus, organizuojame ir ieškome geresnių bendrabūvio formų. Aktyviais dalyviais visuomenėje tapti sudėtinga ir daugelis mūsų turbūt nerizikuotų to daryti, jei būtume nuolat stebimi: apie organizuojamas veiklas galėtų lengvai išsiaiškinti ir mūsų veiksmus sabotuoti piktavaliai, konkurentai ar nedemokratiškos institucijos. Būtent dėl privatumo pažeidimų labai sunku dirbti aktyvistams nedemokratinėse pasaulio valstybėse – ne vieno veikla internete buvo stebėta, ne vienas dėl to, ką mąstė ir veikė, buvo apkaltintas, įkalintas ar net nužudytas, o jų artimieji iki šiol gyvena baimėje. Kitaip tariant, privatumas itin susijęs su mūsų galimybėmis būti aktyviais piliečiais, kovoti su priespauda, žmogaus teisių pažeidimais, kalbėti apie nusikaltimus.

Tačiau gerai, kad visi interneto vartotojai yra savotiški raganiai – tokie kaip Haris Poteris ir jo draugai. Turime priemonių savo privatumo ir saugumo parametrams valdyti. Tam, kad galėtume internete išnaudoti savo prietaisų galias, mums pats laikas išeiti (Hogvartso) mokslus, išmokti atpažinti ir užkardyti juodąją magiją, trukdančią visuomenei ramiai ir saugiai gyventi stebuklingame interneto mieste.

Tikimės, kad šis metodologinis leidinys mokykloje taps geru įvadu į interneto infrastruktūros pasaulį, apie kurį savo moksleiviams, integruodami į pamokas pateiktą informaciją, galės papasakoti įvairių dalykų mokytojai.

UŽDUOTYS

I. Reakcijos ir tinklo veikimo vizualizacijos žaidimas „Kaip veikia tinklas“.

1) Papasakokite moksleiviams, kad tinkle esantys prietaisai vienas kitą pastebi, todėl neįmanoma visiškai pasislėpti, kai naudojantis tinklu norima komunikuoti. Geras pavyzdys – mobilusis ryšys ir internetas, atkeliaujantis per mobiliojo ryšio bokštus. Kad ir kur keliautume, mūsų mobiliojo ryšio prietaisai prisijungia prie artimiausio bokšto. Jei aplinkui stovi keli bokštai – mūsų mobilusis prietaisas „pasisveikina“ su visais, kurie yra taip arti, kad pajėgia registruoti signalą ir paslaugiai asistuoti siųsdami pranešimus į kitus prietaisus.

2) Paprašykite moksleivių pasklisti po klasę – taip kaip Lietuvos žemėlapyje pasklidę mobiliojo ryšio bokštai, laukiantys, kol prie jų prisijungs netoliese atsidūręs mobilusis telefonas.

3) Vieną moksleivį išrinkite būti „mobiliuoju telefonu“, laisvai judančiu tarp „bokštų“ — po klasę pasklidusių bendraklasių. Paaiškinkite, kad vos „mobilusis telefonas“ sustoja, iš karto prisiregistruoja prie artimiausių bokštų ruošdamasis siųsti pranešimus kitiems telefonams ar prietaisams.

4) Paprašykite moksleivių reaguoti į sustojusį „mobilųjį telefoną“. Tai turėtų daryti trys arčiausiai „mobiliojo telefono“ esantys bokštai. Arčiausiai esantis bokštas turėtų reaguoti sakydamas: „Ping.“ Kiek toliau esantis: „Pong.“ O atokiausiai iš trijų esantis turėtų paklausti: „Kas gi čia vyksta?“ Taip pademonstruojama, kad prietaisai tinkle vienas kitą pastebi.
5) Kad būtų smagiau, moksleivį-„mobilųjį telefoną“ galima paprašyti judėti greičiau, o prietaisus – reaguoti operatyviau. Galima į žaidimą įtraukti du „mobiliuosius telefonus“. Nesureagavęs bokštas, kaip „sugedęs“, iškrenta iš žaidimo.

II. Diskusija apie privatumą.
Tikslas – suvokti privatumo problemą pasitelkus asmeninį pavyzdį ir paskatinti moksleivius diskusijoje patiems formuluoti argumentus, kodėl privatumas yra reikalingas.
1) Paklauskite moksleivių, ar jie naudojasi internetu ir ką naudodamiesi internetu dažniausiai veikia.
2) Paklauskite moksleivių, ar galėtų mokytojui parodyti ir detaliai papasakoti, ką veikia naršydami savo telefone, ar sutiktų visiems bendraklasiams atskleisti susirašinėjimus su artimiausiais draugais, taip pat internetinės paieškos istoriją. Užduokite klausimą, kokią informaciją sutiktų viešinti, kokios – ne ir kodėl.
3) Kai moksleiviai pasako argumentus, kodėl nenorėtų mokytojui atskleisti susirašinėjimų su draugais, o kokios informacijos viešinti neprieštarautų, iškelkite klausimą – kaip jie jautėsi išgirdę, kad mokytojas norėtų pamatyti jų telefono turinį. Paklauskite, kaip jie jaustųsi, jei mokykloje galiotų tokia taisyklė: moksleiviai, kas rytą atėję į mokyklą, pirmiausia turėtų atsiskaityti už praėjusios dienos naršymą ir susirašinėjimą internete. Ar moksleiviai, jei būtų tokia taisyklė, koreguotų savo elgesį ir kaip?
4) Apibendrinkite diskusiją išskirdami tris ankščiau tekste įvardytas priežastis, kodėl privatumas yra svarbus kiekvienam visuomenės nariui (intymios asmeninės priežastys, dalykinė reputacija, aktyvus dalyvavimas politinėje ir visuomeninėje veikloje).

III. Kūrybinė užduotis „Interneto miesto architektas“.
Papasakokite moksleiviams, kad internetą galima įsivaizduoti kaip miestą iš Hario Poterio knygų (filmų). Paaiškinkite, kad viskas, ką jie veikia internete, įmanoma tik todėl, kad kompiuteriai yra susijungę į bendrą interneto tinklą, kad egzistuoja du tipai kompiuterių – tai jų asmeniniai kompiuteriai (telefonai) ir serveriai, leidžiantys jiems naršyti „Instagram“, klausytis muzikos per „Spotify“, susirašinėti per „Facebook Messenger“ ar „Snapchat“. Kiekvienas kompiuteris šiame mieste ne tik turi savo unikalų adresą, bet ir stebuklingų galių – pavyzdžiui, tuo pat metu gali jungtis prie nutolusiuose pasaulio kampeliuose esančių serverių (t. y. tuo pat metu svečiuotis skirtingose vietose), suklaidinti tinklą sukurdamas virtualų antrininką, dėtis, kad šiuo metu yra visai kitoje vietoje negu iš tikrųjų.
Pakvieskite moksleivius įsivaizduoti, kad jie yra interneto architektai – kokį interneto miestą norėtų sukurti, nupiešti, nubraižyti? (Tokia užduotis tinka, pvz., dailės pamokose.)

IV. Namų darbai.
Ką apie mane gali pasakyti mano kompiuterio IP adresas? Užduotis reikalauja anglų k. žinių. Atliekama savarankiškai. Ką gali pasakyti IP adresas ir patį IP adresą sužinosite: https://www.ip-adress.com/what-is-my-ip-address.

ŠALTINIAI

1)Kaip veikia internetas? (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=7_LPdttKXPc

2)Kas yra IP adresas? (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=7_-qWIvQQtY
3)Duomenų centrai (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=XZmGGAbHqa0
4)Google duomenų centrai (anglų k.). Prieiga per internetą: https://www.google.com/about/datacenters/inside/locations/index.html
5)Ką Vilniuje skaičiuoja galingiausias kompiuteris Baltijos šalyse? // Mokslo sriuba (lietuvių k.). Prieiga per internetą: https://www.youtube.com/watch?v=rlAsHEU80Rk
6)Daiktų internetas ir privatumas// Mokslo sriuba (lietuvių k.). Prieiga per internetą: https://www.youtube.com/watch?v=mgAHrQjctZY
7)Neturiu ko slėpti – tikrai? Kodėl privatumas svarbus mums visiems// Privacy News Online (anglų k.) Prieiga per internetą: https://www.privateinternetaccess.com/blog/2017/09/nothing-hide-really-heres-privacy-matters-us/
8)Dalintis per daug. // Lietuvos vartotojų institutas (lietuvių k.) Prieiga per internetą: https://www.youtube.com/watch?v=5TxCgC-Audo
9)Duomenų apsauga ir privatumas internete// Jūsų Europa. Europos Sąjunga (lietuvių k.). Prieiga: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_lt.htm

2. Duomenų rinkimas internete

Apie kiekvieną iš mūsų šiandien renkama ir saugoma begalė duomenų. Taip yra ne tik todėl, kad internetas labai palengvino asmeninių duomenų rinkimą – padarė jį pigesnį ir lengviau panaudojamą, bet ir todėl, kad mes patys, net nesusimąstydami, skaitmeninėje erdvėje paliekame vis daugiau duomenų. Net jei nesinaudojame internetu, nuolat esame stebimi – kiekvienas mokėjimo pavedimas banke, kiekvienas mobilusis telefonas generuoja didelius srautus duomenų. Net jeigu nesame prisiregistravę socialiniame tinkle „Facebook“, jis šį bei tą žino ir apie mus – pavyzdžiui, per mūsų draugų, besinaudojančių socialiniu tinklu, adresų knygas telefonuose ar jų žaidžiamus žaidimus internete ir kvietimus pasijungti bendroms veikloms kituose socialiniuose tinkluose.

Šiuos internete paliekamus duomenis galima įsivaizduoti kaip sniege paliekamus, įšalusius pėdsakus. Kol vėl nepasnigo arba jei nepasirūpinome savo privatumo apsauga (nepaslėpėme pėdsakų), jie matomi ir pasitarnauja kitiems įvairiausiais tikslais. Šiame skyriuje paaiškinsime, kam ir kokiais tikslais gali būti naudinga masiškai stebėti interneto vartotojus ir apie juos kaupti duomenis.

2.1 Didieji duomenys

Dabar mažai kas rašo dienoraštį, užtat vis dažniau slapčiausias mintis, nuogąstavimus ir viltis patiki interneto paieškos programoms. O šios nėra nebylus popieriaus lapas. Paieškos programos – tai didžiulės duomenų rinkimo mašinos. Terminas didieji duomenys (angl. big data) apibūdina didžiulius kiekius tiek struktūruotų, tiek nestruktūruotų duomenų, kuriuos daugybė žmonių palieka apie save naudodami modernias technologijas ir paslaugas – pradedant išmaniaisiais telefonais ir baigiant išmaniuoju šaldytuvu. Didžiulis serveriuose saugomas duomenų

kiekis tapo priežastimi sukurti tokius įrankius kaip „Google Maps“, kuriais tokie kiekiai duomenų galėtų būti apdorojami, net jei yra nestruktūruoti.

Didieji duomenys dėl savo vertės pradėti vadinti naująja nafta, kuriai „kasti“ turtuoliai naudoja vis galingesnius kompiuterius. Duomenys ne visiems prieinami, bet tie, kurie gauna prieigą juos „kasti“, t. y. nagrinėti, gali rasti daug vertingų įžvalgų ir jas dažniausiai panaudoja siekdami didesnio pelno ar galios. Taip didžiosios interneto milžinės (pagrindinės keturios: „Amazon“, „Apple“, „Google“, „Facebook“) tampa turtingos lyg naftos magnatai.

Šių duomenų analizė leidžia įžvelgti statistines tendencijas, elgesio modelius ir atpažinti koreliaciją tarp skirtingų charakteristikų, tai atlieka mokslo šaka vadinama duomenų kasimu (angl. data mining). Remiantis gaunamomis įžvalgomis galima prognozuoti netgi ateitį – tokios prognozės naudingos įmonėms, organizacijoms ir valstybėms: leidžia anksti pastebėti pavojus, sumažinti riziką, taupyti laiką ir gauti pelno. Tačiau jos gali būti panaudotos žmonėms kontroliuoti ir duomenų valdytojų galiai įtvirtinti. Mat dažnai duomenys yra renkami vienais tikslais, o paskui, panaudojus analizę, susiejimą su kitais duomenimis, reorganizaciją, gali būti panaudoti visai kitais tikslais.

Šiandien panaudojama dar labai maža dalis duomenų. Vis didėjant kaupiamų duomenų kiekiui, vis mažėja išanalizuotų ir struktūruotų duomenų kiekis. Pasiekėme skaitmeninės ekonomikos „Pramonė 4.0“ pradžią. Tad kas atsitiks, kai bus prisikasta prie likusių duomenų? Žinome, kad naudojama nafta kartu su kitais industrializacijos aspektais sukėlė žmonijai pavojingą klimato kaitą, o ką ateityje sukels kasami duomenys? Kol kas prognozuoti sunku.

2.2 Ką galima daryti su duomenimis?

Tas, kuris žino apie mūsų viltis, baimes, taip pat amžių, pomėgius, gyvenimo būdą ir kitus asmenybės aspektus, turi daug galios. Anot virtualios realybės kūrėjo Jarono Laniero, didžiausią galią turi tie, kam priklauso didžiausi kompiuterių duomenų centrai su galingiausiais skaičiavimo pajėgumais. Jie gali šią informaciją panaudoti įvairiausiems tikslams: nuo produktų pardavimo iki įvairių žmogaus teisių ir laisvių suvaržymo ar išplėtimo.

Dideli duomenų kiekiai leidžia matematiniams algoritmams prognozuoti, ką greitai pirksime, kokios bus mūsų problemos, ką darysime ateityje. Remdamiesi šiomis prognozėmis algoritmai mums siūlo tam tikrą turinį ar reklamą. Dažnai įvertinama ne tik informacija, kurią galima pasiekti internetu, bet ir kasdien atliekamų veiksmų informacija (jei tik ji prieinama), pavyzdžiui, kreditinių kortelių, klientų lojalumo programų arba „išmanių namų“ prietaisų ir išmanių sporto apyrankių ar kitų stebėjimo prietaisų (angl. Self-tracking devices) informacija. Pavyzdžiui, draudimo kompanija „Axa Global Direct“, siekdama nustatyti individualią kainą, sakosi įvertinanti 50 skirtingų kintamųjų, įskaitant naršyklės sausainėlius, vartoseną ir net įrašus apie vakarėlius „Facebook“. Šis pavyzdys parodo, kaip masiškai sekdamos firmos gali suskirstyti žmones į gerus ir blogus klientus, į vertus kredito ar nevertus, pasiūlyti skirtingas kainas tam pačiam produktui, suteikti ar atsisakyti suteikti draudimą, pigiau ar brangiau parduoti lėktuvo bilietus ar nakvynę viešbutyje. Remiantis surinktais duomenimis galima daryti prognozes apie mūsų poreikius ir elgesį, spręsti apie politinius ir religinius įsitikinimus, sveikatos būklę, seksualinę orientaciją, netgi apie jausmus ir nuotaiką. Tokia mūsų duomenų gausa įmonėms ir organizacijoms suteikia labai daug galimybių mumis manipuliuoti, diskriminuoti, taikyti socialinę kontrolę ir sekti. Mums tai reiškia sprendimų priėmimo ir veiksmų laisvės ribojimą, netgi statistinę diskriminaciją (kuomet kasdieniai sprendimai, pavyzdžiui, dėl draudimo, paskolos, darbo suteikimo priimami pagal statistinius demografinės grupės duomenis).

2.3 Sekimas komerciniais tikslais

Jeigu internetinės paieškos lauke suvedėte „pratybų sąsiuvinis“, o naujienų tinklalapis, kuriame ieškote jau ne pratybų sąsiuvinių naujienų, bet naujienų apie mokytojų streiką, po kelių minučių pateikia pratybų sąsiuvinių reklamą, natūralu, kad jaučiatės sekamas. Mūsų kasdieniais įpročiais, paslaptimis, kurias patikėtume tik dienoraščiui, yra suinteresuoti daugelis verslininkų, įmonių, korporacijų.

Kad jus domina pratybų sąsiuviniai, keliais paspaudimais pasakėte ne tik paieškos programai, bet ir pratybų sąsiuvinius leidžiančiai leidyklai (apsilankėte jos tinklalapyje) bei porai dešimčių reklamos įmonių, kadangi įgalinote slapukus (juos plačiau aptarsime skyriuje apie duomenų šaltinius). Užtenka apsilankyti viename tinklalapyje, kad būtų atlikti 56 sekimo veiksmai, iš kurių 40 proc. atlieka stambūs reklamos tinklai. Tokio sekimo tikslas – iš karto po apsilankymo tinklalapyje pasiūlyti būtent apsilankiusiam vartotojui pritaikytą reklamą, kaip pavyzdyje su pratybos sąsiuviniu.

Kai kam „asmeninė“ reklama galbūt neatrodo grėsminga, tačiau mūsų naršymo elgesys apie mus pasako labai daug: mūsų interesus, rūpesčius, mintis ir pomėgius. Net ir panaudojus anonimizuotus duomenis galima atsekti, kuriam žmogui tie duomenys priklauso. Kitaip tariant, „parodyk, kur spaudi, ir aš pasakysiu, kas tu esi“. Tačiau ar apskritai internete įmanoma išlikti anonimu? Vienoje prancūzų studijoje buvo išanalizuota beveik 370 tūkst. interneto vartotojų naršymo įpročiai. Rezultatai parodė: specialiai programinei įrangai labai dažnai užtenka žinoti, kuriuos keturis tinklalapius vartotojas aplankė, kad galėtų jį automatiškai identifikuoti. Ta pati studija parodė, kad 69 proc. mūsų turi unikalią naršymo istoriją, ir jos negalima supainioti su niekieno kito – panašiai kaip pirštų antspaudo. Vadinasi, jei nesisaugome sekimo, anonimiškai naršyti internete neįmanoma.

Didieji duomenys kurį laiką naudojami reklamos tikslais. Verta prisiminti klasikinį pavyzdį iš JAV, kai tėvas pasipiktino, kodėl prekybos centras jo šešiolikmetei dukrai siunčia kūdikių prekių reklamą, nors ji tebesimoko mokykloje, Tačiau vėliau paaiškėjo, kad dukra iš tikrųjų laukėsi. Prekybos centras sužinojo tai anksčiau negu tėvas. Tad, galima sakyti, duomenų rinkėjai deda duomenis į krūvą ir duomenų pirkėjams palengvina vartotojų „medžioklę“.

2.4 Valstybių institucijų vykdomas sekimas

Interneto analogija su miestais tampa ypač akivaizdi, kai kalbame apie valstybes: miesto valdytojas ar policija seka gyventojus, stebi eismą, gatves, kad užkirstų kelią nusikaltimams. Problema atsiranda tada, kai miesto valdytojas ar policija dedasi turintys teisę stebėti gyventojų mintis (kaip minčių policija George’o Orwello romane „1984“).

Valstybės institucijos seka mūsų internetinius pėdsakas daugeliu atvejų pasitelkdamos kasdien naudojamas komercines paslaugas internete, pavyzdžiui, elektroninį paštą. Komerciniais tikslais vykdomas sekimas dažnai padaro įmanomą ir valstybinio masto sekimą. Tačiau valstybės naudoja ir specialias technologijas, tokias kaip išsami duomenų srauto turinio analizė (angl. Deep packet inspection), ji naudojama ir Lietuvoje.

Sekimas valstybės institucijų lygiu internete ypač suintensyvėjo po 2001 metų teroristinių išpuolių JAV – žmonėms buvo pasakyta, kad specialiosios tarnybos, siekdamos apsaugoti nuo terorizmo, turi sekti (patikrinti) kiekvieną. Jei žvelgsime istoriškai, valstybinio masto sekimas nėra naujiena: Sovietų Sąjungos okupuotoje Lietuvoje veikė KGB, Rytų Vokietijoje – slaptoji policija „Stasi“, akylai sekusi savo piliečius dar prieš interneto esą. Maždaug penkiasdešimčiai piliečių teko vienas „Stasi“ pareigūnas, sekdavęs, ar kuris nors nėra nusiteikęs

prieš režimą. Kartais juokaujama, kad šiandienos techninės galimybės, kai galima lengvai patikrinti savo duomenų atidžiai nesaugančio asmens pomėgius, draugų sąrašą, būtų buvusi „Stasi“ svajonė.

Valstybės renka duomenis apie savo piliečius ir statistikos tikslais ar suteikdamos tam tikras paslaugas. Tačiau surinkti duomenys, jei nesaugomi tinkamai (o Lietuvoje, anot 2016 m. duomenų, tik vienetai valstybės institucijų juos saugo tinkamai), gali kelti įvairios rizikos – pradedant kibernetinėmis atakomis prieš pavienius asmenis ir baigiant grėsme pačiai valstybei. Kai duomenys renkami be žmogaus sutikimo – tada duomenų rinkimas pradeda kirstis su teise į privatumą. Pilietis, žinodamas, kad yra sekamas, taip pat gali būti nusiteikęs mažiau priešintis valdžios sprendimams, kuriems nepritaria ir pan.

Valstybė seka siekdama apsaugoti gyventojus nuo terorizmo grėsmės bei kitų grėsmių nacionaliniam saugumui. Kitas valstybės tikslas, apie kurį retai užsimenama, – žmonės sekami, kad būtų užtikrintas valstybinės santvarkos tęstinumas ir numalšinti protestai, jiems neišplitus (todėl Egipto vadovybė bandė kontroliuoti „Facebook“, kitos arabų valstybės pasekė šiuo pavyzdžiu ir kontroliuoja visą internetą savo šalyse). Valdžia siekia kontroliuoti tas priemones, kuriomis naudojasi didžioji žmonių dalis, anksčiau tai buvo televizija, dabar – internetas ir telefono ryšys (Arabų pavasario pavyzdys).

Kitas pavyzdys – Kinija. Joje dabar testuojama socialinių kreditų sistema, grįsta masiniu piliečių sekimu – piliečiai sekami vaizdo kamerų gatvėse, kaimynų, internete. Kinija garsėja kaip valstybė, sekanti ir žinanti kiekvieną savo piliečių žingsnį, – dar 2013 metais ji organizacijos „Reporteriai be sienų“ paminėta tarp valstybių, kurios yra „Interneto priešai”, kadangi visas internetas Kinijoje priklauso valstybei, komunistų partijai ir yra jos kontroliuojamas. Todėl ji yra prasčiausia ir interneto laisvės reitinguose („Freedom House“). Valstybės atliekamas sekimas yra glaudžiai susijęs su cenzūra, o sekimas internete kombinuojamas su sekimu vaizdo kameromis, kuriose įtaisyta veido atpažinimo programa.

Lietuvos Respublikos Konstitucijos 22 straipsnyje teigiama: „Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą.“ Tačiau Kibernetinio saugumo įstatymu nėra tiksliai apibrėžta, kada galima rinkti asmens duomenis, o kada to daryti negalima.

Iš esmės negalima konkrečiai pasakyti, kiek plačiai Lietuvos valstybė vykdo savo piliečių sekimą. Lietuvos įstatymai leidžia kaupti pavienių asmenų duomenis ir tokius asmenis sekti, taip pat ir per elektroninio susirašinėjimo priemones.

Lietuvos gyventojus sekti gali:
1. Valstybės saugumo departamentas, Antrasis operatyvinių tarnybų departamentas, žvalgybos institucijos – žvalgybos tikslais, siekdamos nustatyti, ar nėra pavojaus valstybės saugumui.
2. Teisėsaugos institucijos – siekdamos užkirsti kelią nusikaltimui įvykdyti ar nusikaltimui ištirti.
3. Policija (be teismo sprendimo) – siekdama užkirsti kelią pažeidimams kibernetinėje erdvėje pagal Kibernetinio saugumo įstatymą.
4. Ryšių reguliavimo tarnyba (netiesiogiai) (įpareigojo elektroninio ryšio tiekėjus teikti metaduomenis, vėliau to atsisakė ir ieškojo kito sprendimo).

Lietuvoje kriminalinę žvalgybą vykdo šios institucijos: Finansinių nusikaltimų tyrimo tarnyba, Muitinės departamentas, Policijos departamentas, Kriminalinės policijos biuro ir teritorinės policijos įstaigos, Specialiųjų tyrimų tarnyba, Vadovybės apsaugos departamentas, Valstybės sienos apsaugos tarnyba, Kalėjimų departamentas ir laisvės atėmimo vietos. Taip pat Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos ir Valstybės saugumo departamentas, kai jų padaliniai atliks kriminalinės žvalgybos veiklas.

2.5 Sekimas nusikalstamais tikslais

Lygiai taip pat, kaip įsilaužiama į fizinius pastatus, įsilaužiama ir į skaitmenines duomenų saugyklas. Kuo daugiau duomenų saugoma elektronine forma, tuo dažniau pasitaiko ir jų vagysčių. Debesijos ir įmonių tinklai dėl praktinių priežasčių yra pasiekiami iš viso pasaulio, tai sudaro sąlygas nusikaltėliams iš bet kurios pasaulio vietos į juos įsilaužti. Informacinių technologijų sistemos beveik visada turi saugumo spragų arba netinkamai naudojamos, todėl gana dažnai įsilaužimai būna sėkmingi. Duomenis internete jungdamiesi prie valstybinių paslaugų ar apsipirkinėdami elektroninėse parduotuvėse perduodame per autentifikavimo sistemas – tarpininkus, kurių kompetencija turime pasitikėti, o nusikaltėliai šiose sistemose nuolat ieško landų. Dažniausiai jie siekia išvilioti pinigų, pasisavindami tapatybę arba šantažuodami, tačiau kai kurių informacijos vagių tikslai yra politiniai, kaip kandidatės į Jungtinių Amerikos Valstijų (JAV) prezidentus Hillary Clinton atveju, kai karščiausiu rinkimų kampanijos momentu buvo paviešinti slapti jos susirašinėjimai elektroniniu paštu.

Net kas penktas Lietuvos gyventojas 2014 metais pats ar per draugus, giminaičius, pažįstamus susidūrė su tapatybės vagystėmis. Tapatybės vagystė reiškia, kad pasisavinami žmogų identifikuojantys duomenys, pavyzdžiui, paso duomenys, adresas, pavagiama „Facebook“ ar „Gmail“ paskyra. Apsimetę kitu žmogumi nusikaltėliai gali pasiimti greitųjų kreditų, turėdami prisijungimo prie internetinio banko duomenis pavogti pinigų. Vis dažniau nusikaltėlių grupės socialiniuose tinkluose susikuria netikrų paauglių profilių, iš šių profilių kontaktuoja su jų bendraamžiais, ketindami išvilioti apsinuoginusių ar nuogų jų nuotraukų, filmukų ir vėliau juos šantažuoti, kad susimokėtų už informacijos neviešinimą.

Nusikaltėliai, tikėdamiesi praturtėti iš šantažo, dažnai siekia gauti jautrių duomenų, kurių žmonės nenorėtų pamatyti paskelbtų viešai (tarkim, sveikatos duomenų). Pasinaudojama ne tik valstybių ar interneto milžinių, bet ir nedidelių įmonių sukauptais duomenimis. Kartais prie duomenų prieinama palyginti lengvai. Tai įrodo atvejis, kai vienos Lietuvos plastinės chirurgijos klinikos klientų duomenys buvo nutekinti pasinaudojus buvusio klinikos darbuotojo prisijungimo duomenimis. Nusikaltėliai pavogė daugiau nei 22 tūkst. plastinės chirurgijos klinikos klientų duomenų (vardus, pavardes, asmens kodus, adresus, fotografijas prieš ir po operacijų) ir, paviešinę asmeninius duomenis tamsiajame internete (angl. Darknet), pačių klientų bei plastinės chirurgijos klinikos reikalavo susimokėti už fotografijų neskelbimą. Įsilaužėliai buvo sučiupti, šiuo metu vyksta teisminis procesas, tačiau juos pagauti pavyksta ne visada.

Žinoma daug atvejų, kai internete įsilaužiama į elektroninės prekybos svetaines, pavagiami pirkėjų asmeniniai duomenys, kreditinių kortelių numeriai, kurie vėliau naudojami vykdant kitus kriminalinius nusikaltimus. Įsilaužėliai stengiasi rasti saugumo spragų tose platformose, kurias naudoja daugiausia žmonių, tačiau tai nereiškia, jog alternatyvios platformos visiškai saugios. Jei nusikaltėlis ketina įsilaužti į konkretaus žmogaus (dažniausiai žinomo) internetinę erdvę ir yra pasiryžęs skirti daug laiko, kad sulauktų lemtingos klaidos, įsilaužimo išvengti nelengva. Be to, tobulėjant technologijoms tobulėja ir apgavysčių būdai. Kai gaunate laišką iš visiškai nepažįstamo žmogaus ir jis netaisyklinga anglų kalba prašo pinigų, suprantate, kad tai apgaulė, ir laišką ištrinate. O kai programišius įsilaužia į jūsų draugo elektroninį paštą ir atsiunčią laišką pamėgdžiodamas jo rašymo manierą, perprasti apgaulę gali būti sunkiau. Taip atsitiko vienai universiteto dėstytojai iš Lietuvos: nusikaltėlis užgrobė jos kolegos iš Italijos elektroninio pašto dėžutę, apsimesdamas kolega paprašė pervesti pinigų ir jų gavo.

Kitas įsilaužėlių „verslo modelis“ – paimti duomenis lyg įkaitus ir už jų „išlaisvinimą“ reikalauti išpirkos. Pavyzdžiui, ransomware tipo viruso, žinomo kaip „WannaCry“, paleidėjai atakavo apie 300 tūkst. kompiuterių visame pasaulyje, užšifruodami kompiuteriuose ir serveriuose esamą informaciją, kurios nebebuvo įmanoma atstatyti, ir padarė žalos už 10 mlrd. dolerių.

UŽDUOTYS

Tema: Duomenų rinkimas internete „Dideli duomenys – didelės problemos?“

I. „Duomenų prekybininkas“

1. Prieš pradėdami, parodykite videožaidimo „Data dealer“ (Duomenų prekybininkas) anonsą iki apytiksliai 1:32 minutės. Jį rasite čia: https://datadealer.com (yra versijos anglų ir vokiečių kalbomis). Žaidimas kritiškai vertina prekybą bei piktnaudžiavimą duomenimis.
2. Suskirstykite moksleivius į grupes po 5: vienas moksleivis tegu būna duomenų prekybininkas, kiti 4 – jo klientai (sekimo valstybės diktatorius, elektroninė parduotuvė, bankas, kelionių sveikatos draudimas). Išdalykite moksleiviams vaidmenų korteles (jas rasite kitame puslapyje). Duomenų prekybininko užduotis – apklausti savo klientus, kokių duomenų jie norėtų gauti, ir juos užsirašyti. Kiekvienas duomenų prekybininkas žaidimo pabaigoje pristato, kokių duomenų kiekvienas klientas pageidavo. Duomenų vertę kartu su moksleiviais galite reitinguoti („Kokia informacija galimai vertingesnė?“).

Galimi atsakymai:

Bankas	Elektroninė parduotuvė	Kelionių sveikatos draudimas	Sekimo valstybė
Skolos, turtas, profesija, amžius, pajamos	Interesai / mėgstami dalykai, vartojimo įpročiai, mokėjimo įpročiai (ar greitai apmoka sąskaitas), amžius, gyvenimo būdas, mėgstama muzika	Ligos, hobiai, maitinimosi įpročiai, svoris, alkoholio vartojimas, seksualinė orientacija, DNR profilis	Politinės nuostatos, turtas, komunikacijos įpročiai, draugų ratas, judėjimo profilis

3. Pabaigoje trumpai aptarkite prekybos duomenimis temą. Kas yra duomenų prekybininkai? Kaip duomenų prekybininkai renka informaciją? Apie kokius duomenų prekybos skandalus moksleiviai jau girdėjo (jei nežino, papasakokite apie Cambridge Analytica skandalą)? Paklauskite moksleivių, ar atiduotų savo duomenis, žinodami, kad šie gali būti panaudoti nesąžiningiems rinkimams, kam nors pasipelnyti arba, pavyzdžiui, skiriant jiems didesnę kainą, kai perka tam tikros paslaugos. Kitos pamokos tema arba namų darbų užduotis galėtų būti: „Kaip asmeniškai galima apsisaugoti nuo manipuliavimo duomenimis?“

II. Didžiųjų duomenų teikiamos galimybės ir rizika

1. Šią užduotį paranku atlikti, kai moksleiviai jau supažindinti, kokie duomenys gali būti įdomūs įvairiems „duomenų pirkėjams“ (pavyzdžiui, atlikus pirmąją užduotį „Duomenų prekybininkas“). Užduoties pradžioje galite parodyti įvairių vaizdo įrašų fragmentų arba duoti perskaityti tekstų apie didžiuosius duomenis.

Video didžiųjų duomenų tema:

„Mokslo ekspresas“. Didžiųjų duomenų era: archeologija. https://www.youtube.com/watch?v=8YzC5--_HQc (pakeisti į bit.ly) (taupant laiką galima rodyti iki maždaug 2:40 minutės)
Vokiečių kalba: https://www.youtube.com/watch?v=DusV8hfDXSg

Tekstai didžiųjų duomenų temomis:

Lukrecijus Tubys. Ar jau atsisveikinote su teise į privatumą? E. Snowdeno dokumentai ir Lietuva. (galima duoti skaityti ištrauką) http://www.universitetozurnalistas.kf.vu.lt/2015/01/ar-jau-atsisveikinote-su-teise-i-privatuma-e-snowdeno-dokumentai-ir-lietuva/

2. Suskirstykite moksleivius į grupes po 5. Duokite jiems šią užduotį: „Minčių žemėlapyje surašykite, kas šiandien įmanoma pasitelkus didžiuosius duomenis. Suskirstykite surašytus teiginius į didžiųjų duomenų teikiamas galimybes ir rizikas. Suskirstyti naudokite +/- ženklus arba žalią ir raudoną spalvas.“
Galimi atsakymai:

Galimybės: individualiam vartotojui pritaikytas medijų ir vartojimo pasaulis (paieškos sistemos, naujienų tinklalapiai, elektroninės parduotuvės); nauji verslo modeliai; naujos transporto analizės priemonės (išvengiama transporto spūsčių ir avarijų); tikslesnė informacija ir / ar jos analizė (partnerių paieškoje, mokykloje); įmonės gali dirbti skaidriau ir efektyviau; naujos darbo vietos; priemonės skurdui mažinti ir užkirsti kelią ligoms išplisti (atpažinti, kaip plinta ligos, pavyzdžiui, su „Google Flu Trends“); apskaičiuojama nusikaltimų tikimybė (angl. predictive policing) – išaugęs saugumas.

Rizikos: įtarimai pareiškiami arba įkalinima remiantis prognozėmis, kad vienas ar kitas žmogus ateityje padarys nusikaltimą, o ne nusikaltimais; apskaičiavus finansinį patikimumą, siūlomos skirtingos kainos ar nuolaidos (angl. dynamic pricing); sekimas (visa apimančios žinios apie mus); kainų didėjimas (draudimui); žmogus tampa klientu, nebe piliečiu; nebėra galimybės būti pamirštam (jaunystės nuodėmės); manipuliacija („efektyvi, klientui pritaikyta kalba“).

3. Pabaigoje kartu su moksleiviais ant lentos nubrėžkite bendrą minčių žemėlapį ir pagal jį tose pačiose grupėse kaip ir pirmoje užduotyje pakvieskite užrašyti minčių lietų (galimybės ir rizikos, kylančios iš didžiųjų duomenų).

ŠALTINIAI

1)Lukasz Olejnik, Claude Castelluccia, Artur Janc. Why Johnny Can’t Browse in Peace: On the Uniqueness of Web Browsing History Patterns. 5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2012), Jul 2012, Vigo, Spain. 2012. Priega per internetą: https://hal.inria.fr/hal-00747841/document
2)Big Data for Social Innovation // SSIR (anglų k.). Prieiga per internetą: https://ssir.org/articles/entry/big_data_for_social_innovation
3)Didieji duomenys: aukso gysla, į kurią krypsta verslo žvilgsnis // TV3 (lietuvių k.). Prieiga per internetą: https://www.tv3.lt/naujiena/791743/didieji-duomenys-aukso-gysla-i-kuria-krypsta-verslo-zvilgsnis
4)EU Surveillance. The EDRi papers. Edition 02, 2012. Prieiga per internetą: https://edri.org/wp-content/uploads/2013/10/paper02_web_20120123.pdf

5)Lietuvoje kas penktas susiduria su tapatybės vagystėmis// Delfi (lietuvių k.). Prieiga per internetą:https://www.delfi.lt/mokslas/technologijos/lietuvoje-kas-penktas-susiduria-su-tapatybes-vagystemis.d?id=65198847
6)Technologijų ekspertas: duomenų nutekinimo atvejų tik daugės// LRT (lietuvių k.). Prieiga per internetą: https://www.lrt.lt/naujienos/kalba-vilnius/32/177842/technologiju-ekspertas-duomenu-nutekinimo-atveju-tik-dauges
7)Pacientai iš grožio chirurgijos prisiteisė tūkstančius eutų neturtinės žalos// Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/news/daily/law/pacientai-is-grozio-chirurgijos-prisiteise-tukstancius-euru-neturtines-zalos.d?id=80029099
8)Grožio chirurgijos klinika klimpsta vis giliau: internete nuogas elitas// Tv3 (lietuvių k.). Prieiga per internetą: https://www.tv3.lt/naujiena/909433/grozio-chirurgijos-klinika-klimpsta-vis-giliau-internete-nuogas-elitas
9)Šantažuojami grožio klinikos pacientai priėmė sprendimus// Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/santazuojami-grozio-klinikos-pacientai-prieme-sprendimus.d?id=74601352
10)Paviešinti grožio klinikos duomenys: už siuntimąsi gresia baudžiamoji atsakomybė// 15min (lietuvių k.). Prieiga per internetą: https://www.15min.lt/verslas/naujiena/bendroves/paviesinti-grozio-klinikos-duomenys-uz-siuntimasi-gresia-baudziamoji-atsakomybe-663-804882
11)https://www.lrt.lt/naujienos/ekonomika/4/200171/bukite-atsargus-cekius-registruoti-kviecia-ne-tik-vmi
12)Katrin Eggert (BvD e. V.), Ralf Heimburger (Mitglied im AK Schule, BvD e. V.), Rudi Kramer (Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.), Riko Pieper (stellv. Sprecher der Initiative „Datenschutz geht zur Schule, BvD e. V.), Frank Spaeing (stellv. Sprecher der Initiative „Datenschutz geht zur Schule, BvD e. V.) [Hrsg. (atsakingi redaktoriai)]. Datenschutz geht zur Schule: Sensibler Umgang mit persönlichen Daten. Arbeitsblätter. [Duomenų apsauga ateina į mokyklą. Apgalvotas elgesys su asmeniniais duomenimis. Užduočių ruošiniai]. 2018 m. lapkritis. Prieiga per internetą: https://www.klicksafe.de/service/materialien/broschueren-ratgeber/datenschutz-geht-zur-schule/#s
13)Rekordiniai kibernetinių nusikaltimų metai: 5 pavojingiausios atakos// Delfi (lietuvių k.). Prieiga per internetą:https://www.delfi.lt/mokslas/technologijos/rekordiniai-kibernetiniu-nusikaltimu-metai-5-pavojingiausios-atakos.d?id=76824157

3. Duomenų šaltiniai

Turbūt ne vienam kyla klausimas, kaip surenkami į didžiųjų duomenų aruodus patenkantys duomenys – kas yra duomenų apie mus šaltiniai, iš kurių semia ir analizuoja visi, mumis suinteresuotieji.

3.1 Metaduomenys

Bene lengviausiai prieinami duomenys apie mus yra metaduomenys. Edwardas Snowdenas, buvęs JAV saugumo struktūrų samdinys, atskleisdamas informaciją apie valstybės mastu be piliečių žinios vykdytą kibernetinį sekimą, parodė, kad saugumo agentūros visame pasaulyje renka arba stebi didžiulį kiekį metaduomenų. Metaduomenys – tai elektroninę informaciją

apibūdinantys duomenys. Kad geriau suprastume, šiuos duomenis galime palyginti su knygos aprašu bibliotekoje: tai informacija, kuria apibūdinama knygos vieta, identifikuojamas autorius, leidykla, turinys, apimtis, fiksuojama, kas ir kada ją skolinosi. Kompiuteriuose taip pat saugoma informacija apie jame sukuriamus, į jį gaunamus ar iš jo siunčiamus dokumentus. Pavyzdžiui, turime išsaugotą „Microsoft Word“ programos dokumentą. Dar jo neatidarę galime matyti pavadinimą, sukūrimo datą, dydį, kada paskutinį kartą dokumentas buvo pakeistas ir panašias detales. Ši informacija saugoma, kad dokumentas galėtų būti rūšiuojamas, lengvai randamas kompiuteryje ar būtų galima tobulinti programą.

Metaduomenims priskiriamas kiekvieno, į tinklą prisijungiančio prietaiso adresas – t. y. IP adresas – informacija apie prietaisą, išreikšta kodu. Kiekvieną kartą, atvėrus interneto svetainę, kompiuteris su serveriu, kuriame veikia interneto svetainė, dalijasi IP adresu (kad serveris žinotų, kokiu adresu siųsti prašomos svetainės atvaizdą). Paieškos sistema „Google“ gali parodyti IP adresą, jei to klausiame paieškos lange įrašydami „My IP address“. Interneto tiekėjas paskiria IP adresą kiekvienam vartotojui, todėl jis susiejamas ir su vartotojo interneto maršruto parinktuvu. Visi namuose esantys įrenginiai per tą patį maršruto parinktuvą pasirodo tinkle tuo pačiu išoriniu IP adresu, tačiau egzistuoja ir lokalus IP adresas, kad maršruto parinktuvas žinotų, kuris prietaisas ir prie kurios svetainės prašė prisijungimo, ir svetainės failus siųstų būtent jam. Tad prisijungus prie interneto tinklo privatumas savaime nėra galimas, nes kompiuteriai vienas kitą tinkle turi pažinti, o tam pasitarnauja IP adresai. Geriausias būdas apsaugoti savo interneto prisijungimą ir IP adresą yra žinoti, kam suteiki WiFi (belaidžio vietinio tinklo) slaptažodį ir jį nuolat keisti, kad prie tinklo negalėtų jungtis nepageidaujami asmenys. Taip pat savo IP adresą galima pakeisti naudojant VPN (angl. Virtual Private Network) – tai speciali programinė įranga, kuria kompiuteris prie interneto prijungiamas per tarpinį serverį, suteikiantį prietaisui visai kitą IP adresą, o kartu su juo ir kitą lokaciją bei susijusius metaduomenis. Verta pridurti, kad naudojimasis VPN kelia daug legalumo klausimų – pats VPN yra legalus, tačiau jo panaudojimas kai kuriems veiksmams, pavyzdžiui, piratavimui yra nelegalu.

Kitas populiarus metaduomenų šaltinis – tai EXIF duomenys, apibūdinantys skaitmeninio formato nuotraukas. Peržiūrėjus nuotraukos metaduomenis, galima sužinoti kameros, kuria fotografuota, pavadinimą, fotoaparato užrakto greitį, nuotraukos ekspoziciją, o kartais net detalias GPS koordinates, kur nuotrauka buvo padaryta. Jeigu kompiuteryje naudojame „Windows“ operacinę sistemą, galime išsiaiškinti savo saugomų nuotraukų metaduomenis paspaudę dešiniu pelės klavišu ant dominančios nuotraukos, lentelėje spustelėję „Ypatybės“ (angl. Properties) ir atvertę skyrelį „Išsami informacija“ (angl. Details). Toje pačioje lentelėje galime pasirinkti, kokius duomenis norime pašalinti, ir juos pašalinti. Jei EXIF duomenys liks nepašalinti, o nuotrauka dažnai dalijamasi, pavyzdžiui, per elektroninį paštą ar susirašinėjimo programėlės, gavėjai galės tikrai daug pasakyti apie fotografavusį ar nuotraukoje užfiksuotą asmenį.

2012-aisiais dėl to, kad žurnalistai neištrynė EXIF duomenų, specialiosios tarnybos susekė bėglį – nužudymo užsakymu įtartą garsų programuotoją, antivirusų kūrėją Johną McAfee. JAV žurnalas „Vice“ paskelbė interviu su J. McAfee’u ir iliustravo jį bėglio nuotrauka neištrynęs EXIF duomenų. Greitai teisėsaugai paaiškėjo, kad įtariamasis slapstosi Gvatemaloje.

Geras dalykas, kad dauguma socialinių tinklų, tokių kaip „Twitter“ arba „Facebook“, daugeliu atvejų pašalina EXIF duomenis iš skelbiamų nuotraukų. Vis dėlto, perkeliant nuotraukas iš telefono ar fotoaparato į kitus prietaisus, EXIF duomenys išlieka, vadinasi, jei šia nuotrauka bus pasidalyta elektroniniu paštu, kiekvienas gavėjas galės tuos duomenis matyti.

3.2 Naršyklės kaip duomenų šaltinis

Naršymo istorija. Naudodamiesi naršyklėmis paliekame savo naršymo istorijos pėdsakus – sąrašą visų internetinių svetainių, kuriose lankėmės. Pavyzdžiui, jei orų prognozių svetainėje patikrinome, koks bus rytoj oras, tai ši svetainė bus naršymo istorijos dalis. Kai kurios bendrovės apie lankytojus renka tokius duomenis– kartais jie yra sugrupuojami, kad vėliau naršant (pvz., ieškant per „Google“ paiešką) pagal atitinkamus reikšminius žodžius būtų siūlomi tie patys ir panašūs (į jau aplankytus) tinklalapiai. Nors naršymo veikla ir gali atrodyti lyg dėlionės detalės, kartais jų užtenka susidaryti bendram vaizdui – identifikuoti, koks asmuo esame. Be to, jeigu savo prietaise saugome naršymo istoriją, prietaisą praradus ar „nulaužus“, nepažįstami asmenys gali peržiūrėti visą mūsų interneto naršymo istoriją.

Jeigu naršome „Google“ prisijungę prie savo paskyros, visa istorija nukeliauja į mūsų profilį (o ištrynus verta patikrinti, ar ji ištrinta tik iš vieno įrenginio, ar ir kitų įrenginių, kuriais naudojomės). Pagal naršymo istoriją „Google“ sukuria asmeninį reklamos profilį (savąjį pasitikrinti galima čia: https://www.google.com/settings/ads/).

Norėdami apsaugoti savo naršymo istoriją, galime rinktis kelis variantus: dauguma naršyklių turi nematomo režimo parinktį, tai apsaugo ir nuo slapukų išsaugojimo, kitas būdas – nuolat trinti naršymo istoriją. Be to, patartina nesaugoti slaptažodžių kompiuteryje: jeigu sunku juos prisiminti, geriau pamąstyti apie tam skirtą programėlę – slaptažodžių valyklę. Slaptažodžių saugiam saugojimui naudojamos specializuotos programos, kurios kuria ilgus slaptažodžius ir juos išsaugo taip, kad niekas kitas išskyrus jus pačius jų nepamatytu ir nepanaudotu, kaip pavyzdys programa „RoboForm“.

3.3 Slapukai

Duomenis apie tai, kas mums rūpi, mūsų svajones ir rūpesčius gauna praktiškai kiekvienas interneto tinklalapis, kuriame lankomės, jei tik leidžiame jam mūsų naršyklėje įdiegti slapukus (angl. Cookies). Tai maži duomenų vienetai / failai, kurie, jei tik leidžiame, apsigyvena naršyklėje (ją galima pavadinti mūsų interneto virtuve). Kai, panaršę tinklalapyje, po kurio laiko į jį grįžtame, slapukai, jei tik neištrynėme, laukia mūsų, jų siuntėjai automatiškai jau yra išanalizavę mūsų elgseną tame tinklalapyje ir stengiasi pasiūlyti tai, ko galbūt pageidautume. Norėdami naršyti tam tikrame tinklalapyje dažnai neturime kitos išeities, kaip tik leisti slapukams kaupti mūsų informaciją.

Kai kurie slapukai yra būtini, tarkim, padeda pasirinktas prekes sudėti į „krepšelį“ ir po keliasdešimties minučių susinaikina patys. Neleidę jiems veikti, nebegalėsime visavertiškai naudotis tinklalapiu – elektroninėje parduotuvėje nebegalėsime ko nors nusipirkti ir panašiai.

Kita slapukų rūšis – nuolatiniai slapukai. Jie prisimena mus, kai vėl apsilankome tinklalapyje, ir gali sekti, pavyzdžiui, kiek laiko praleidome skaitydami vieną ar kitą straipsnį arba apžiūrinėdami kokią nors prekę. Tokie slapukai gali būti ir naudingi – grįžus į svetainę nebereikia iš naujo nustatinėti pasirinktos kalbos, šrifto dydžio ir kitų parametrų, o tai daro naudojimąsi tinklapiu patogesnį. Slapukai taip pat padeda tinklalapio administratoriui sužinoti, kiek žmonių ir iš kokių šalių apsilankė tinklalapyje.

Europos Sąjungoje įsigaliojus Bendrajam duomenų apsaugos reglamentui, dauguma tinklalapių, pirmą kartą juose lankantis, siūlo pasirinkti, kokius slapukus leidžiate suinstaliuoti savo įrenginyje, pavyzdžiui, būtinuosius, reklamavimo slapukus ir kitus („15min.lt“ yra geras pavyzdys, kaip galėtų būti tvarkomi slapukai).

Svarbu pastebėti, kad slapukai nesaugo konkretaus tinklalapio vartotojo asmens duomenų – kiekvienam vartotojui priskiriama tam tikra raidžių, skaičių ir ženklų kombinacija, pagal kurią naršytojas atpažįstamas jam vėl apsilankius tinklalapyje.

3.4 Nešifruotos svetainės

Dauguma svetainių ir programėlių šiandien naudoja HTTPS saugų prisijungimą prie puslapio – taip visa komunikacija tarp naršyklės ir svetainės yra šifruojama. Jeigu mes jungiamės prie svetainės HTTP (nešifruotu būdu), visą informaciją gali lengvai nuskaityti pašaliniai asmenys. Pavyzdžiui, vartotojui jungiantis per WiFi ryšį, pasisavinti jo konfidencialią informaciją užtektų tam tikros, signalą skaitančios radijo ryšio įrangos arba tame pačiame tinkle esančio piktavalio su sekimui paruošta programine įranga. HTTPS atveju informacija, siunčiama svetainei, yra šifruojama, o paskui dešifruojama, todėl prisijungęs pašalinis asmuo negali taip lengvai matyti konfidencialių duomenų. Norintiesiems savo tinklalapį apsaugoti šiuo SSL protokolu, reikia gauti sertifikatą, todėl naršyklėje esantis HTTPS prierašas padeda įsitikinti serverio, su kuriuo ruošiamasi bendrauti, tikrumu ir garantuoja, kad siunčiamą informaciją matys tik siuntėjo serveris ir vartotojas, kuris naršo svetainėje.

Naršyklės HTTPS puslapius pažymi spynos piktograma, ant jos paspaudus galima sužinoti sertifikato savininką, jo galiojimo periodą, išdavusios institucijos pavadinimą bei kitą svarbią informaciją. Jeigu interneto naršyklė nustato, kad sujungimas nėra saugus, rodomas raudonai perbrauktas HTTPS arba parašoma, kad svetainė nesaugi. „Google Chrome“ naršyklė pastaruoju metu vartotojus įspėja, jei svetainės duomenys nešifruoti, taip pat baudžia nesaugias svetaines, klausia, ar tikrai norite eiti į jas ir panašiai.

Vis dėlto daug svetainių dėl didesnės veikimo spartos vis dar naudoja HTTP, HTTPS protokolas nebūtinas, kai interneto puslapis yra informacinis, jame nereikia įvesti jokių vartotojo duomenų, neviešos informacijos.

3.5 Mobiliosios programėlės

Prieiga. Kiekvienas išmanusis telefonas turi daugybę informaciją fiksuojančių daviklių – kur esame, kaip greitai judame, kaip laikome telefoną (gulsčiai ar vertikaliai). Kadangi programėlės bendrauja siųsdamos duomenis – tam tikrą informaciją įveda vartotojas, tam tikrus rodiklius davikliai surenka, siunčiantis programėles iš neoficialių programėlių platintojų mūsų įvedami duomenys gali būti lengvai pasiekiami trečiųjų asmenų. Oficialių operacinių sistemų parduotuvės „App Store“, „Google Play“ ar „Amazon“ imasi papildomų saugumo priemonių ir blokuoja programėles, kurios bendrauja su savo serveriais nesaugiu ryšiu, t. y. ne HTTPS.

Kita vertus, sujungus paskyras didėja duomenų kaupimo galimybės. Tuo pasižymi „Android“ operacinės sistemos – vos tik susiejame savo telefoną su „Google“ paskyra, „Google“ pradeda registruoti duomenis, pvz.: skambučių trukmę, dažnį, kokį prietaisą naudojate, kaip dažnai ir kita (tai leidžia „Google“ privatumo politika). Kol kas „Apple“ privatumo politika kiek kitokia – daugelis telefono kaupiamų duomenų yra laikomi tik pačiame „iPhone“ (ir nesiunčiami atgal į „Apple“), pavyzdžiui, buvimo vieta gali būti stebima mūsų programinės įrangos „iOS“, bet pati „Apple“ bendrovė nežino, kur esame.

Svarbu atkreipti dėmesį, kokioms funkcijoms prieigos prašo programėlė, tai būna nurodyta siunčiantis iš oficialių parduotuvių. Racionalu, kai, pavyzdžiui, orų programėlė prašo mūsų

vietovės nustatymo, bet jau turėtų kilti įtarimų, jei tokia programėlės norės prieigos prie mikrofono. Prieigas patikrinti ir keisti nustatymus galima: „Android“ atveju reikia eiti į „Settings“ (Nustatymus), tuomet pasirinkti „Apps&Notifications“ (Programėlės ir įspėjimai) ir „Permissions“ (Leidimai); „iOS“ atveju „Settings“ aplanke pasirinkus programėlę iškart matysite, kam ji turi prieigą.

Buvimo vietos sekimas. Net jei ir kontroliuojame prieigą, visus atvejus numatyti painu. Pavyzdžiui, nors neleidžiame programėlei sekti mūsų vietovės, bet suteikiame prieigą prie nuotraukų, programa taip pat (jeigu norėtų) galėtų matyti, kur buvome, nustatyti namų adresą, atostogų vietas, kadangi nuotraukų duomenys žymisi geografinius metaduomenis. Žinoma, dažniausiai programėlės gauna informaciją, nepavadintą mūsų vardu, o priskyrus unikalų ID, tačiau dėl renkamo didžiulio kiekio duomenų, lengvai galima identifikuoti asmenį (pvz., pagal namų, kur asmuo praleidžia naktį, ir darbo adresus).

Jei „Google“ leidžiame sekti savo buvimo vietą, pagal judėjimo greitį ji gali nustatyti, ar keliavome pėsčiomis, dviračiu ar automobiliu. Sekantys buvimo vietą gali atpažinti net šunų savininkus, kadangi jie dažnai juda netolygia trajektorija. Taip „Google“ atpažįsta ir žmones, važiuojančius automobiliais, kad apskaičiuotų apytikrį maršruto laiką ir sektų eismo sąlygas.

3.6 Elektroninis paštas

„Gmail“ el. pašto sistema neslepia, kad siekdama pastebėti šlamštą, internetinius sukčius, skenuoja elektroninius laiškus ir ieško juose tam tikrų žymių, raktinių žodžių (angl. keywords). Taip pat tai panaudoja ir savo kuriamai dirbtinio intelekto įrangai tobulinti, pvz., neseniai pradėjusiai veikti „Smart Response“ (daugiau: https://www.cnbc.com/2018/05/08/google-launches-smart-compose-for-gmail.html).

Vis dėlto 2018 m. liepą „Google“ patvirtino, kad kartais „Gmail“ laiškai gali būti skaitomi ne tik mašinų, bet ir žmonių (programuotojų), net neprašius atskiro leidimo, kadangi tai nurodyta privatumo politikoje, kurios, kaip žinia, dauguma neskaito.

3.7 Dirbtinis intelektas

Dirbtinis intelektas – kompiuterinės sistemos gebėjimas, analizuojant duomenis, veikti taip, kaip veikia žmogaus intelektas (mokytis pačiai, vykdyti užduotis, daryti sprendimus, prognozuoti). Jam kurti ne tik pasitelkiami psichologijos ir neurologijos, matematikos ir logikos, komunikacijos teorijos, filosofijos ir lingvistikos mokslų duomenys, pats intelektas tobulėja analizuodamas didelius informacijos kiekius. Kadangi dirbtinio intelekto sistemos gali apdoroti didelius duomenų kiekius, o sistemų tikslumas didėja kartu su duomenų kiekiu, duomenų paklausa vis labiau auga, o apdoroti naudojami modeliai tik dar labiau didina duomenų kasybos mastus. Algoritmais grįsta sistema sukurta taip, kad programos mokosi pačios – joms priimant sprendimus, nurodoma, ar jie teisingi, ar klaidingi.

Vienas gerai žinomų dirbtinio intelekto panaudojimo pavyzdžių – autonominiai automobiliai. Kompanija „Tesla“ jiems kurti renka duomenis iš visų savo transporto priemonių, kuriose įmontuoti įvairiausi davikliai, analizuojantys, kokius veiksmus daro vairuotojas, kaip valdo automobilį, ant kurių prietaisų ir kuriuo metu deda rankas ir kita.

Svarbus aspektas, kad duomenų tiekimas dirbtiniam intelektui negali sustoti – jis yra nuolat alkanas. Be naujų duomenų dirbtinio intelekto formuojami modeliai gali keistis nenuspėjamu būdu. Nauji duomenys reikalingi dar ir todėl, kad laikui bėgant pačių duomenų tendencijos gali kisti. Čia susiduriama su daugybe etikos bei privatumo problemų, ypač medicinos srityje. Tikima, kad

dirbtinis intelektas būtų ypač naudingas sveikatos priežiūros srityje (pateikti įžvalgas, kurios nėra akivaizdžios žmonėms), tačiau tam reikia daugybės asmenų ligos istorijų duomenų, o to žmonės nenori taip lengvai atskleisti. Europos Sąjungoje tam tikrus saugiklius įtvirtino Bendrasis duomenų apsaugos reglamentas (BDAR), pavyzdžiui, vartotojas turi būti informuojamas apie sprendimus, kuriuos priima automatizuotos arba dirbtinio intelekto algoritmų sistemos, ir turi teisę atsisakyti automatizuoto apdorojimo arba dirbtinio intelekto sprendimo.

UŽDUOTYS

I. Perskaitykite straipsnį https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy ir patikrinkite, kokią informaciją per pastarąją parą apie jus surinko „Google“ ir „Facebook“? (Kur buvote? Ko ieškojote? Kokie jūsų pomėgiai?)
II. Išsirinkite 5 kasdien aplankomus tinklalapius ir patikrinkite, ar jie naudoja saugų prisijungimą. Kas išdavė jų sertifikatus, koks jų galiojimo laikas? Kokių grėsmių galima tikėtis, jei šios svetainės naudoja nesaugų prisijungimą?
III. Darbas grupėmis.
1) Moksleiviai padalijami į grupes ir kiekvienai grupei parenkama po vieną populiariausių programų („Facebook“, „Google“, „Snapchat“, „Twitter“, „Instagram“, „Spotify“ t. t.).
2) Moksleiviai turi perskaityti parinktos programos privatumo politiką ir parengti apibendrinimą: kokius duomenis apie juos renka programa, koks saugumas užtikrinimas, kokias rizikas pastebi; ir pristatyti klasei.

ŠALTINIAI

1)Dirbtinis intelektas Google veikloje (anglų k.). Priega per internetą: https://www.youtube.com/watch?v=BRUvbiWLwFI
2)HTTPS paaiškinimas (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=rROgWTfA5qE
3)HTTPS paaiškinimas (anglų k.). Prieiga per internetą: https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/
4)Programėlės ir vietų nustatymas (anglų k.). Prieiga per internetą: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html
5)Visa Google ir Facebook kaupiama informacija (anglų k.). Prieiga per internetą: https://twitter.com/iamdylancurran/status/977559925680467968?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E977559925680467968&ref_url=https%3A%2F%2Fwww.nbcnews.com%2Ftech%2Ftech-news%2Fgoogle-sells-future-powered-your-personal-data-n870501
6)Apple privatumo politika (anglų k.). Prieiga per internetą: https://www.apple.com/legal/privacy/en-ww/
7)Google privatumo politika (anglų k.). Prieiga per internetą: https://policies.google.com/privacy
8)Duomenų kaupimas kompiuterio kamera (anglų k.). Prieiga per internetą: https://nordvpn.com/blog/tell-if-laptop-camera-hacked/
9)Gmail laiškų skaitymas// BBC (anglų k.). Prieiga per internetą: https://www.bbc.com/news/technology-44699263

4. Didesnį privatumą užtikrinančios paslaugų internete alternatyvos

Ankstesniuose skyriuose supratome, kas gali norėti mūsų duomenų, kaip tie duomenys gali būti prieinami. Kilo noras sustiprinti spynas? Šiame skyriuje aptarsime, kaip galima stiprinti savo internetinę privatumo gynybą.

Šimtaprocentinės apsaugos garantuoti negali jokia programa, joks internetinis įrankis, tad visada reikėtų apsvarstyti, ar tikrai verta naudotis tam tikra programa ar įrankiu, ar tikrai informacija, kurią pateikiate programų kūrėjams, turėtų laisvai tekėti interneto tinklais. Jei tai tikrai reikalinga, pravartu naudotis privatumą saugančiomis priemonėmis; jas galima palyginti su spynomis į rūsį ar kitus kambarius, į kuriuos nebūtinai net kiekvieną draugą kviečiame. EFF (angl. Electronic Frontier Foundation) rekomenduoja sudaryti sąrašą (kaip tai darytume ir su kitu savo turtu), kokius duomenis saugome nuo svetimų akių, kam jie gali būti įdomūs.

Niekas nenorėtų, kad po miestą klajotų asmuo, turintis raktą nuo daugumos miesto gyventojų spynų. Tai būtų nesaugu ir visi skubiai pultų keistis spynų. Interneto mieste didieji paslaugų tiekėjai tokius raktus turi, kai nešifruota informacija keliauja per jų serverius. Tokius raktus turi ir žinomos kompanijos, tokios kaip „Google“, „Facebook“. Jos netgi gali pasiūlyti reklamą pasiremdamos mūsų laiškuose esančiu turiniu.

Jei buvote įpratę savo duomenimis švaistytis į kairę ir į dešinę, bet nusprendėte keisti įpročius, privatumui apsaugoti reikalingų veiksmų gausa iš pradžių gali būti gąsdinanti. Kur pradėti: nuo stipresnės spynos durims (kompiuterio apsaugos) susikūrimo ar nuo geros spynos savo dienoraščiui (laiškų šifravimo) sukūrimo? Vieno visiems tinkančio atsakymo nėra. Pradėti galima ten, kur įdomiausia, lengviausia. Privatumą geriau saugančių įpročių ugdymas primena naujo raumens treniruotę – iš pradžių sunku, bet nuosekliai mankštinantis rezultatai pastebimi.

Galite pradėti nuo lengviausių žingsnių, pavyzdžiui, ištrinkite naršymo istoriją ir sausainėlius, belaidžio namų tinklo gamyklinį slaptažodį pakeiskite į saugesnį (darykite tai bent kartą per pusmetį), blokuokite reklamą svetainėse (pvz., su nemokamu „Adblock Plus“), instaliuokite naršyklės priedą „PrivacyBadger“. Tada galite peržiūrėti, kokie privatumo nustatymus pasirinkti naudojamuose socialiniuose tinkluose ir juos pakeisti į geriau privatumą saugančius.

Netgi tiems, kurie jau įsisąmonino privatumo svarbą internete, gali būti nelengva keisti savo įpročius ir pradėti labiau rūpintis duomenų apsauga. Šis neatitikimas tarp mūsų supratimo, kokia svarbi duomenų apsauga, ir mūsų veiksmų, skirtų duomenims apsaugoti, yra vadinamas privatumo paradoksu.

4.1 Techninis saugumas vs. privatumas

Techninis saugumas ir privatumas nėra tapatūs. Techninis saugumas reiškia, kad, pavyzdžiui, jūsų elektroninio pašto tiekėjas naudoja daugiapakopes apsaugos priemones norėdamas apsaugotų elektroninio pašto dėžutę nuo įsilaužėlių. Privatumas reiškia, kad priėjimo prie elektroninio pašto ar kitų duomenų neturi net paslaugos ar interneto tiekėjas.

„Google“ paieškos programa – geras pavyzdys, kuo techninis saugumas skiriasi nuo privatumo: kai suvedate norimą ieškoti frazę į „Google“, paieškos gigantas jos ieškos naudodamas saugų HTTPS ryšį, tačiau jūsų paieškos frazė bus prieinama pačiam „Google“ ir saugoma jo serveriuose. Tad saugiai prisijungę prie interneto negalite būti tikri, kad jūsų duomenys nėra niekam prieinami.

Kaip keisti savo internetinį gyvenimą, kad jame atsirastų daugiau privatumo? Visiems pagrindiniams paslaugų tiekėjams internete yra alternatyvų. Jos dažnai orientuotos į tokių paslaugų siūlymą, kokių nesiūlo didžiosios interneto korporacijos; alternatyvos dažnai būna grįstos decentralizacija ir interneto bendruomenės įsitraukimu kuriant paslaugą atviru ir visiems prieinamu kodu (kur kiekvienas gali pasitikrinti, kaip programa sukurta, ar programos kodas neturi spragų ir ar paslaugos tiekėjas nekaupia perteklinių asmeninių duomenų). Kokios alternatyvos egzistuoja populiariems, bet mūsų privatumo taip akylai nesaugantiems internetinių paslaugų tiekėjams?

Keletą alternatyvų pateikiame lentelėje.

Lentelė. Privatumą labiau saugančios alternatyvos

Paslaugos rūšis	Populiarūs paslaugų tiekėjai, renkantys daug duomenų	Alternatyvos, privatumą saugančios labiau
Susirašinėjimų / pokalbių kambarių programėlės	„WhatsApp“, „Messenger“	„Signal“. Dar didesniam privatumui: „Pidgin“, „Off-the-Record“ (OTR), „Jabber“, „Conversations“
Socialiniai tinklai	„Facebook“	„Mastodon“, „Diaspora“
Paieškos varikliai	„Google“	„Startpage“, „DuckDuckGo“, „Ecosia“
Naršyklės	„Google Chrome“, „Microsoft Explorer“, „Safari“	„Firefox“ yra pripažįstama kaip labiausiai privatumą sauganti + taikyti privatų režimą; „Orweb“; „Firefox“ + „Mailvelope.com“. Anonimiškumui: „Tor“, „Richochet“
Elektroninis paštas	„Gmail“	„Thunderbird“ + PGP (naudotis „Gmail“ taip, kad laiškų nebūtų galima skaityti), „Thunderbird“ + „Enigmail“, „Open PGP“; kiti el. pašto paslaugos teikėjai, taip pat mokami
Programėlėms parsisiųsti	„Google Play“	„Fdroid“ (gali neturėti visų aplikacijų, bet turės tokių aplikacijų, kurių neturi „Google Play“)

4.2 Naršyklių nustatymai ir alternatyvos

Privatus naršymo režimas. Interneto naršyklėse prieinamas privatus naršymo režimas (angl. private mode) – dar vienas būdas, padedantis saugoti jūsų privatumą. Tačiau jis apsaugo privatumą tik nuo žmonių, besinaudojančių tuo pačiu kompiuteriu ar kitu įrenginiu, kadangi nesaugo jūsų paieškos istorijos, nesiunčia sausainėlių, laikinųjų rinkmenų ar tinklalapių, kuriuose

apsilankėte, sąrašo. Tačiau naršant incognito režimu jūsų interneto tiekėjas, mokykla ar tinklalapiai, kuriuose apsilankėte, gali registruoti apsilankymą[1]. Pasinaudojus privačiu naršymo režimu patartina išjungti naršyklę ar pakeisti langą, kad būtų mažiau galimybių susekti. „Firefox“ naršyklėje galima pasirinkti nuolatinį naršymą privačiu režimu.

Anonimiškumas kaip kare: „Tor“, VPN. Nors ir naršote privačiu režimu, naudojate ištisinį šifravimą, voką voke (žr. Saugumas el. pašte) ar vieną iš alternatyvių naršymo variklių, metaduomenų neįmanoma šifruoti. Jei internete norite naršyti anonimiškiau, galima naudoti naršykles, tokias kaip „Tor“ arba eksperimentinę „Richochet“. Žodis „anonimiškiau“ vartojamas specialiai, nes šimtaprocentinio saugumo ar privatumo internete nebūna. Pasitaiko, kad ir „Tor“ naudotojai būna susekami – tai atsitinka dažniausiai ne dėl pačios „Tor“, kaip programos, saugumo skylių, bet dėl naudotojo klaidų, pavyzdžiui, per šią naršyklę buvo prisijungta prie nešifruojamo elektroninio pašto dėžutės. Ši naršyklė tokia saugi / pažengusi, kad atitikmenį jai analoginiame pašto paslaugų pasaulyje sunku rasti. „Tor“ lyginama su svogūnu: žinutė yra svogūno viduje, ir reikia nulupti labai daug sluoksnių, kad prie jos būtų galima prisikasti.

Sakoma, „Tor“, kurio simbolis – svogūnas, priverčia „verkti“ saugumo tarnybas, nes pats naršyklės mechanizmas yra toks, kad saugumo tarnybos, net ir nusipirkusios „Tor“ serverių, retai gali sužinoti, kas iš tikrųjų „Tor“ naudojasi. Jei būna išsiaiškinama „Tor“ naudotojas, tai paprastai įvyksta dėl žmogiškų klaidų, o ne dėl klaidų „Tor“ sistemoje.

Paslėpti savo naršymą naudojant blokuojamą serverį nuo paslaugų teikėjo gali padėti VPN galimybė, tiksliau – VPN gali pakeisti esamą serverį kitu, kuris nebus blokuojamas ar sekamas. Tai ypač pravartu, kai esamoje šalyje tam tikri paslaugų teikėjai blokuojami. Pavyzdžiui, Kinija blokuoja „Gmail“, „Facebook“ bei kitas svetaines, ir norintieji apeiti šią cenzūrą gali naudotis VPN.

4.3 Paieškos sistemos

Internetiniame mieste, kaip ir fiziniame, galima patirti daug nuotykių, rasti įdomių kampelių, sužinoti daug nauja muziejuose, bibliotekose, kepyklose. Kaip ir fiziniame mieste, internete mums reikalingas žemėlapis. Tokiu žemėlapiu dažniausiai tampa paieškos variklis. Esama įvairių interneto žemėlapių: įvairaus detalumo, įvairaus mastelio.

„Google“ paieškos sistema primena mus sekantį žemėlapį. Jis padeda orientuotis, rasti, ko norime, bet taip pat labai daug žino apie mus ir, naudodamas tą informaciją, gali pradėti siūlyti keliavimo interneto mieste „maršrutus“(angl. search bubble), kurių nebūtinai norime, bet paieškos sistema mano, kad mums ten patiks, todėl siūlo alternatyvas remiantis mūsų naršymo ar paieškų istorija.

Kaip saugoti savo privatumą naudojantis netradiciniais internetinės paieškos varikliais? Alternatyvi paieškos sistema „DuckDuckGo“ sakosi esanti „paieškos variklis, kuris neseka tavęs“. Kitaip nei „Google“, „DuckDuckGo“ nerenka informacijos apie žmones, besinaudojančius šia sistema, tačiau jie vis dėlto žino, kokius paieškos žodžius žmonės šioje sistemoje naudoja – tiesiog nesusieja paieškos istorijų su konkrečiu vartotoju. „DuckDuckGo“ taip pat sako rodanti vartotojams tai, ko yra internete nenaudodama algoritmų, pasakančių, kokie rezultatai konkrečiam žmogui būtų įdomesni.

Kitas variantas – Nyderlanduose įsikūrusi bendrovė „Startpage“. Ji siūlo „Google“ paiešką, bet be „Google“ įprasto sekimo. Jie nusipirko „Google“ duomenis ir sakosi esantys diskretiškiausia ir geriausia interneto paieškos sistema. „Startpage“, kitaip nei „Google“, negali perduoti jokių duomenų net valstybės institucijoms, nes jų paprasčiausiai nekaupia. Svarbu suprati: kai atlikę paiešką paliekame paieškos variklį ir nueiname į kokį nors kitą tinklalapį, paieškos variklio siūloma privatumo apsauga nebeveikia. Kaip saugomas mūsų privatumas, kokie duomenys apie

mus renkami, priklauso jau nuo to, kokius tos svetainės sausainėlius nusprendėme leisti veikti, kokia naršykle jungiatės ir panašiai. Šiai spragai ištaisyti „Startpage“ turi duomenų apsaugos funkciją – anoniminę peržiūrą (tinklalapius, kuriuos radote naudodamiesi anonimine paieškos sistema „Startpage“, galite peržiūrėti taip pat anonimiškai). Lietuviškuose interneto tinklalapiuose dažnai kalbama apie „Startpage“ virusą – vis dėlto „Startpage.com“ nėra virusas, tačiau egzistuoja tokio pat vardo „Trojan“ virusas[1].

Žmonės ieško ne tik alternatyvų, kurios saugo jų privatumą, bet ir prisideda prie bendro gėrio visuomenėje. Tokia alternatyva tarp interneto paieškos sistemų yra „Ecosia“ – jie uždirba pinigų iš reklamos ir didžiąją dalį pelno skiria įvairiems aplinkosauginiams projektams, pavyzdžiui, miškams išsaugoti. „Ecosia“ savo tinklalapyje skelbia: „Kad pasodintum medį, reikia atlikti maždaug 45 paieškas.“ Paieškos variklio įkūrėjai yra įsipareigoję patys nieko neuždirbti. Todėl besirūpinantiems mūsų planetos likimu, klimato kaita, „Ecosia“ gali būti geras pasirinkimas. O privatumas? Asmeninius duomenis iš savo serverių „Ecosia“ ištrina po savaitės[2].

4.4 Elektroninio pašto duomenų šifravimas

Norėdami pasirinkti geriausią variantą saugoti savo privatumui internete, pirmiausia turime suprasti, kokie privatumo modeliai egzistuoja internete (žr. lentelę „Privatumo modelių internete palyginimas su pašto paslaugomis“). Kitaip tariant, kokio stiprumo spynų būna. Jei siunčiame žinutę interneto tinklais taip, kaip ir paprastu paštu, norime būti tikri, kad niekas kitas jos nematė. Nebent žinutėje nėra nieko, ką norėtume slėpti voke, pavyzdžiui, draugams iš Vilniaus atviruke siunčiame saulėtus linkėjimus iš Palangos. Žinome, kad paštininkas gali perskaityti šią žinutę, bet dėl to nesijaudiname. Laiškų siuntimas naudojantis „Gmail“ elektroninio pašto paslauga prilygsta linkėjimams siunčiamiems atviruku. Kai išsiunčiame atviruką, pirmiausia, jį iš pašto dėžutės išima vietinis paštininkas (arba mūsų interneto paslaugos tiekėjas), tada jis keliauja į vietinį Palangos paštą (arba „Gmail“ serverį JAV), kuris nustato, kur toliau siųsti atviruką. Mūsų atveju į Vilniaus paštą („Gmail“ siunčiamo laiško atitikmuo – antrasis serveris JAV), jis perduoda mūsų atviruką Vilniaus paštininkui (arba mūsų draugo interneto paslaugos tiekėjui). Mūsų siunčiamą atviruką gali apžiūrėti mažiausiai keturi pašto darbuotojai. Dėl to neprieštaraujame – svarbu, kad siuntinys pasiektų draugą. O jeigu siunčiame labai asmenišką laišką draugui, jį įdedame į voką, kad pakeliui jo niekas neperskaitytų.

Problema ta, kad „Gmail“ su visais mūsų laiškais elgiasi taip, tarsi jie būtų atvirukai. Kartais pasitaiko nesąžiningų paštininkų: jie pirmiausia atidaro voką, peržiūri jo turinį ir tik tada persiunčia adresatui. Laiško įdėjimas į voką internete prilygtų TLS (angl. Transport Layer Security) – vokas žinutei transportuoti yra, bet neapsaugo nuo nesąžiningų paštininkų. Jeigu laišką įdėsime į du vokus, teoriškai paštininkas galės mūsų laišką pažiūrėti, bet mažai tikėtina, nestai jam kainuotų per daug laiko, o paštininkai, žinia, daug laiko neturi. Internete vokas voke būtų end-to-end šifravimas: interneto tiekėjas matytų tik išorinį voką, jį nusiųstų serveriui. Išorinį voką atidaręs serveris vidinį voką persiųstų adresatui. Šiuo principu veikia, pavyzdžiui, „Signal“ susirašinėjimų programėlė.

Lentelė. Privatumo modelių internete palyginimas su pašto paslaugomis

Pašto sistemos atitikmuo	Šifravimo būdas internete	Paslaugos, taikančios šį šifravimo būdą
Atvirukas	Jokio / „Detail Ansicht“	„Gmail“

Nesąžiningas paštininkas	Transport Layer Security (TLS)	Paštas, „Hangouts“, „Messenger“
Vokas voke	Ištisinis šifravimas	„WhatsApp“, „Signal“
Svogūnas lankosi pašte	Svogūninis šifravimas	„Tor“
Asmeniniai pašto balandžiai	Asmeninis serveris / serveris pas draugus, kuriais pasitikite	„Jabber“ / kt., pavyzdžiai, kai su draugais dalijatės serveriu

Kaip atviruką pakeisti voku voke? Tam yra keletas būdų: galima rinktis šifruojamo elektroninio pašto tiekėjo paslaugas arba šifruoti jau naudojamo pašto dėžutę. Pavyzdžiui, „Posteo“ ar „ProtonMail“ paštas nesaugo elektroninio pašto serveriuose, todėl net kam nors pareikalavus perduoti susirašinėjimus, tai būtų neįmanoma. Tai vadinama privatumo užtikrinimu projektuojant (angl. Privacy by Design).

4.5 Alternatyvios mobiliosios programėlės

Visų pirma, telefoną, kaip ir kompiuterį, reikėtų prižiūrėti ir įsidiegti antivirusinę programą. Išmaniojo telefono programėlės kaupia gerokai daugiau duomenų apie mus negu tos pačios paslaugos kompiuteryje. Nereikėtų duoti priėjimo nemokamoms išmaniosioms programėlėms prie savo duomenų, kai nebūtina (tai galima valdyti tiek „Android“, tiek iOS), pavyzdžiui, vargu, ar kalbos mokymosi programėlei tikrai reikia priėjimo prie nuotraukų ir adresatų sąrašo.

Kokie duomenys apie mus prieinami pokalbių programoms, priklauso nuo to, kokį susirašinėjimų šifravimo būdą jos naudoja. Kitaip tariant, kiek stiprios jų uždedamos spynos. Tarp nemokamų susirašinėjimų programėlių, kurios daugiau dėmesio skiria savo vartotojų privatumui, „Signal“ yra laikoma stipriausia. Ji šifruojama ištisiniu šifravimu (angl. End-to-end encryption). Yra ir mokamų programėlių! Kitaip nei interneto gigantai, uždirbantys iš reklamos, jos uždirba iš savo vartotojų privatumo saugojimo, viena tokių programų yra „Threema“.

Informacinių technologijų ekspertų teigimu, dėl didelės alternatyvų pasiūlos gali būti sunku susigaudyti, kuri alternatyva geresnė, ir kartais tenka tiesiog pasitikėti paslaugos tiekėjais. Žinoma, prieš tai patartina patikrinti, ar nėra kokių nors įtarimą keliančių aspektų.

4.6 Slaptažodžių kūrimo ypatumai

Įsivaizduokite: esate programišiai (hakeriai) ir prisėdę prie svetimo kompiuterio turite atspėti kieno nors slaptažodį. Žinoma tik tiek, kad slaptažodis sudarytas iš keturių skaitmenų ir tas žmogus nemėgsta sudėtingų slaptažodžių. Kokius variantus išbandytumėte pirmiausiai?

Angliškoje abėcėlėje yra 26 raidės, tad kiekvienas simbolis gali turėti ne 10 reikšmių, kaip iš skaitmenų sudarytame slaptažodyje, o 26 reikšmes. Štai formulė suskaičiuoti visiems galimiems variantams: 264 = 456 976. Raidinių variantų daugiau kaip 45 kartus daugiau nei vien iš skaitmenų. Tai atrodo daug, kol nesužinai, kokiu greičiu spėlioja kompiuteris. Dar 1998 metais buvo sukonstruotas įrenginys, galintis atlikti 90 mlrd. spėjimų per sekundę. Tokiu greičiu

spėliojančiam kompiuteriui įveikti mūsų keturių raidžių slaptažodį užtruktų ne ilgiau kaip 0,000005 sekundės

Tačiau tikriausiai žinote, kad dauguma svetainių stabdo prisijungimo procesą po kelių nesėkmingų bandymų (pavyzdžiui, liepia uždėti varnelę „Captcha“) arba siunčia nuorodą į el. paštą skatindami patvirtinti, kad tikrai bando prisijungti paskyros savininkas. Todėl slaptažodžiai spėliojami dažniausiai kitaip. Kad suprastumėte – kaip, pirmiausia reikia žinoti, kaip interneto paslaugų tiekėjai saugo slaptažodžius. Kai sukuriama paskyra, tarkime, elektroninio pašto dėžutė, šios paslaugos teikėjas įrašo sugalvotą slaptažodį savo duomenų bazėje, esančioje jo serveriuose. Kai bandoma prisijungti kitąkart ir suvedamas slaptažodis, sistema patikrina, ar tai, kas suvesta, atitinka tai, kas saugoma jos duomenų bazėje.

Bent jau taip elgtasi anksčiau, kol nesusidurta su problema, kad programišiai įsibrauna į pašto paslaugo tiekėjų sistemą ir, nusikopijavę duomenų bazę, turi visus vartotojų prisijungimo vardus su slaptažodžiais. Kad vartotojų slaptažodžiai būtų apsaugoti duomenų bazės vagystės atveju, paslaugų teikėjai į jas nebeįrašo slaptažodžių. Kai sugalvojate slaptažodį ir įvedate į slaptažodžio laukelį, sistema apdoroja jį tam tikru algoritmu, sugeneruojančiu unikalią skaičių ir simbolių seką, ir į duomenų bazę įrašo tik ją. Kai kitąkart bandoma prisijungti ir įvedamas slaptažodis, sistema vėl apdoroja jį tuo pačiu algoritmu ir palygina, ar gautas rezultatas yra toks pats, koks saugomas jos duomenų bazėje (angliškai tai vadinama hashu, o pats procesas – password hashing).

Jei duomenų bazė pavagiama, programišius gauna tik krūvas bereikšmių simbolių, kurių neįmanoma atversti į slaptažodį. Vienintelis būdas sužinoti, koks vartotojo slaptažodis, yra pasinaudojus tuo pačiu algoritmu versti visus iš eilės žodžius į hashus. Kai pamatoma, kad kuris nors sugeneruotas hashas atitinka jau esantį pavogtoje duomenų bazėje, tada pažiūrima, iš kokio žodžio jis sugeneruotas, ir programišius žino slaptažodį. Tai ir yra slaptažodžių spėliojimas. Nors šis procesas yra ilgas, bet pasaulyje egzistuoja duomenų bazės, kuriose saugomi hashai ir tikrieji slaptažodžiai, tad ir šis slaptažodžių saugojimo metodas tapo ne tokiu saugiu.

Jei naudojate „password123“ ar kurį nors kitą populiarų arba silpną slaptažodį, jį robotas spės pirmiausiai ir tam prireiks sekundės dalių ar daugiausiai kelių sekundžių. Populiariausi slaptažodžiai yra tokie:

123456789.
12345678.
12345.
111111.
1234567.
sunshine.
qwerty.
iloveyou.

Juos atspėti labai lengva net žmogui, o ir robotas spėlioti pradeda būtent nuo jų, vėliau pereina prie žodyno, dar vėliau – prie atsitiktinių simbolių sekų. Daugybė tradicinių gudrybių yra žinomos ir jos nepadės, nes robotas užprogramuotas jas visas patikrinti pirmiausiai.

Tad kaip susikurti saugų slaptažodį? Tai suprasite per kitas 10 minučių. Tarkime, pasigaminote kompiuterį specialiai spėlioti slaptažodžiams. Slaptažodžiai hashinti sudėtingu algoritmu ir šis kompiuteris sugeba patikrinti po 10 mln. slaptažodžių per sekundę. Apskaičiuokite, kiek laiko jis užtruktų, kol išmėgintų visas galimas kombinacijas tam tikro ilgio atsitiktiniuose slaptažodžiuose, kuriuos sudaro:

1. Šeši simboliai, vien skaičiai [106 = 1 000 000/10 000 000 -> 0,1 sek.].
2. Šeši simboliai, vien skaičiai ir mažosios lotyniškos raidės [10+26 -> 366 2 176 782 336/10 000 000/60 -> 217 sek. -> 3,5 minutės].

3. Šeši simboliai, vien skaičiai ir lotyniškos didžiosios bei mažosios raidės [10+26+26 -> 626 =56 800 235 584/10 000 000/60/60 -> 95 minutes]
4. Dvylika simbolių (skaitmenys, mažosios ir didžiosios lotyniškos raidės) [6212 = apytiksliai 322 600 000 000 000 000 000. Spėliojant 10 000 000 spėjimų per sekundę greičiu išmėginti visas įmanomas kombinacijas užtruktų 32 260 000 000 000/60/60/24/365 -> daugiau nei 10 000 000 metų].
5. Užduotis: suskaičiuoti savo slaptažodžio iš pagrindinės socialinio tinklo ar el. pašto paskyros gylį]

Kokia tendencija? Kuo ilgesnis slaptažodis, tuo ilgiau užtrunka jį atspėti. Atspėjimo laikas ilgėja efektyviau, jei slaptažodis yra ilginamas, o ne tuomet, kai tokio paties ilgio slaptažodyje pridedama daugiau atsitiktinių simbolių.

Reikia įsidėmėti, kad žmogus ir kompiuteris slaptažodžius spėlioja skirtingai: žmogui sunkiai įveikiamą slaptažodį kompiuteris gali sudoroti greičiau, nei spėsite mirktelėti, tad ir kurti slaptažodžius reikia ne tokius, kokie atrodo sudėtingesni, o kokie yra sunkiau nulaužiami kompiuteriu. Dabar jau žinome, kad slaptažodį saugesnį – sunkiai atspėjamą kompiuteriu – daro ne jo simbolių atsitiktinumas (pvz., gC^.8Gg), o ilgis (pvz., kaimynasnesurenkasunskakuciu – 28 simboliai, truputį juokinga, bet skaičiavimo laikas – astronomiškai ilgas).

Tad koks slaptažodis yra saugus? Standartas dabar – mažiausiai 12 simbolių, tarp kurių yra skaičių, didžiųjų ir mažųjų raidžių, specialiųjų ženklų (kablelių, šauktukų, grotelių ir t. t.), bet jei sugalvosite 20 simbolių slaptažodį vien iš mažųjų raidžių, jo taip pat nepajėgs atspėti per tokį laiką, kokį vertėtų skirti spėjimams. Ir, kaip matėte iš pavyzdžio apie neatsakingą kaimyną, įmanoma sugalvoti ilgą, unikalų ir lengvai atsimenamą slaptažodį.

Sugalvokite netikėtą frazę iš trijų ar keturių žodžių ir turėsite saugų slaptažodį. Geriau būtų ne populiarios dainos pavadinimas arba koks nors kitas itin populiarus posakis. Pamėginkite. Pavyzdžiui, „bulvemis lyja labai retai“, „dovanotiems dantims i arkli neziurima“. Voilà! Turite saugų ir atsimenamą slaptažodį.

Kodėl negalima naudoti vienodų slaptažodžių? Ką darysite žinodami, kaip sugalvoti saugų slaptažodį? Turbūt pasikeisite – ir pirmiausia tų paskyrų, kurias naudojate dažniausiai ir kurios jums svarbiausios. Bet paskyrų turime daug, ir jų kasmet tik daugės.

Anot kai kurių tyrimų, paaugliai turi maždaug aštuonias socialinių tinklų paskyras, neįskaitant elektroninio pašto. Skaičiuokime, ką jau turi daugelis jūsų draugų dabar: „Facebook“, „Instagram“, „Snapchat“, „WhatsApp“, „Gmail“, „Spotify“, „musical.ly“, galima paminėti „Goodreads“. Žaidimų svetainės ir daugybė kitų paslaugų internete reikalauja užsiregistruoti, net jei ten apsilankoma kartą per metus. Taip susikaupia iki vidutiniškai 27 paskyrų vienam interneto vartotojui, o atsiminti tiek daug saugių slaptažodžių žmogui neįmanoma.

Ar galima tą patį saugų slaptažodį naudoti visur? Jei norite, kad jis taptų nesaugus – tada taip. Įsivaizduokite: jūsų šeima visur naudojasi labai kokybiškomis, neišlaužiamomis spynomis – namuose, sodyboje, garaže, automobilyje, dviračio prirakinimo grandinėje, persirengti skirtoje baseino spintelėje ir taip toliau. Tačiau visos jos atrakinamos tuo pačiu raktu – jei jį neapdairiai paliksite ir kas nors pasidarys kopiją, gaus priėjimą iškart prie visų jums brangių daiktų. Panašiai yra ir internete: užtenka vieno neatsakingai jūsų duomenis saugančio interneto paslaugų teikėjo, ir visas jūsų duris atrakinantis slaptažodis atsiduris programišių rankose. Ne visi paslaugų teikėjai taiko šiuolaikinius reikalavimus atitinkančius saugumo standartus, pavyzdžiui, tebenaudoja senus hashinimo algoritmus, kurie lengvai įveikiami šiuolaikiniais kompiuteriais. Šie dalykai sudėtingi ir jų paprastam interneto vartotojui išmanyti nebūtina, be to, daugelis net neskelbia, kokius apsaugos įrankius naudoja. Be to, net jei įmonė stengiasi apsaugoti duomenis, jų turi tiek daug ir daugybėje serverių, kad kartais tiesiog įsivelia klaidų ir dalis duomenų lieka neapsaugoti. Prisiminkite pirmąją pamoką: internetas yra nuolat pertvarkomas ir chaotiškas, jame važinėjama visomis eismo

juostomis į visas puses, kalbamasi daugybe kalbų vienu metu, pastatai statomi vieni ant kitų. Palikę savo „saugų“ slaptažodį daugybėje vietų rizikuojate, kad kuri nors iš jų bus lengvai prieinama, nes kas nors tiesiog pamiršo įstatyti duris arba net sumūryti sieną.

Internete dabar platinama per keletą metų sukaupta pavogtų slaptažodžių duomenų bazė, kurioje yra keleto milijardų vartotojų prisijungimo duomenys. Galbūt bazėje yra ir jūsų arba artimųjų kadaise kur nors įvestas, bet tebenaudojamas, slaptažodis. Galite net pamiršti, kad kadaise registravotės kokiame nors nedideliame puslapyje, kurio duomenų bazė vėliau buvo nulaužta ir kuris nebuvo stipriai apsaugotas. Net jei pasikeitėte slaptažodį nulaužtajame puslapyje, kokia grėsmė išlieka? Kadangi žmonės naudoja vienodus slaptažodžius ir taip elgiasi ilgus metus, programišiai galbūt gali sėkmingai pasinaudoti prisijungimo duomenimis kitame puslapyje net po keleto metų.

Štai keli neseni pavyzdžiai, kad net ir didžiausios, turtingiausios korporacijos, investuojančios didžiules lėšas saugumui, negali jo užtikrinti 100 proc.: iš „Sony Playstation Network“ 2011 m. pavogta 77 mln. vartotojų duomenys, iš „Adobe“ – 2013 m. 152 mln. vartotojų duomenys, iš „Yahoo!“ – 2013 m. net 3 mlrd. vartotojų duomenų, o kadaise „Yahoo!“ buvo didžiausia interneto paslaugų kompanija, kaip dabar „Google“.

Todėl norėdami jaustis ramesni turite naudoti skirtingus slaptažodžius. Tik kaip juos visus atsiminti? Čia į pagalbą ateina slaptažodžių tvarkyklės (angl. password manager arba password locker). Dažniausiai tai naršyklės įskiepis asmeniniame kompiuteryje arba programėlė telefone ar planšetėje.

Slaptažodžių tvarkyklė:

- įsimena jūsų slaptažodžius už jus,
- kad nereikėtų galvoti slaptažodžio, sugeneruoja naujus saugius slaptažodžius už jus,
- sinchronizuoja slaptažodžius: jei pakeitėte juos kuriame nors įrenginyje – kitame naujus slaptažodžius įrašys automatiškai, kai bandysite prisijungti, reikalauja atsiminti vieną saugų slaptažodį (pavyzdžiui, keturių žodžių frazę) ir naudoja aukšto saugumo priemones jam apsaugoti.

Populiariausios ir geriausiai dabar pasaulyje vertinamos slaptažodžių tvarkyklės:

„1password“;
„Blur“;
„Keeper“;
„Dashlane“;
„EnPass“;
„LastPass“;
„LogMeOnce“;
„Password Boss“;
„RoboForm“;
„Sticky Password“;
„True Key“;
„Zoho Vault“.

Tikriausiai pastebėjote, kad naršyklės, tokios kaip „Firefox“, „Safari“, „Chrome“, turi labai panašią funkciją: įsimena slaptažodžius už jus ir juos įrašo. Tačiau saugumo specialistai nepataria šia funkcija naudotis, nes ji sukurta pirmiausia vartotojo patogumui, bet ne saugumui užtikrinti, tad gali būti lengviau pažeidžiama. Be to, ji patogi, jei naudojatės tik kompiuteriu, o jei

norite, kad saugūs slaptažodžiai būtų automatiškai tvarkomi ir telefone ar planšetėje, kur prisijungiate per programėles, užpildyti prisijungimo formų minėta funkcija jose negali.

Dar vienas svarbus žingsnis apsaugoti elektroninį paštą – naudoti dviejų žingsnių atpažinimo sistemą, kai ne tik įvedate saugų slaptažodį, bet ir gaunate prisijungimo kodą telefonu ar patvirtinate prisijungimą savo piršto anstpaudu, veido atpažinimo funkcija ar kitu biometriniu metodu. Taip apgaulės galimybė sumažinama iki minimumo.

UŽDUOTYS

I. Informacijos apie geresnio saugumo alternatyvas paieška ir įvertinimas.
Žiniasklaidoje rasti informacijos apie alternatyvas bei įvertinti: žiniasklaidos priemonės patikimumą (ar galima pasitikėti ta priemone, priimant sprendimą, naudotis viena ar kita geriau privatumą saugančia priemone ar paslauga); ar verta pasitikėti šia socialinių tinklų paslauga (kas yra savininkai, iš kokios šalies, kiek informacijos apie juos galime rasti).
II. Kaip pasirinkti paieškos sistemą.
Reikalingos priemonės: Kompiuteris
1. Paklauskite, kokias interneto paieškos sistemas moksleiviai žino, kokie jų skirtumai, privalumai, trūkumai. Papasakokite apie interneto burbulus, jei moksleiviai iki šiol apie tai negirdėjo.
2. Atsidarykite www.google.lt, www.duckduckgo.com, www.ecosia.org ir į atitinkamus paieškos laukus įrašykite „interneto burbulas“. Palyginkite, kuo skiriasi rezultatai. Kodėl manote, kad rezultatai būtent tokie?
3. Pasvarstykite klasėje, kodėl moksleiviai rinktųsi vieną ar kitą paieškos sistemą? Kas svarbiau – privatumas, geresni (naujesni?) paieškos rezultatai ar aplinkos apsauga? Ar tai suderinama?
III. Užklasinis projektas „Šifravimo vakarėlis mokykloje“
Kai nusprendžiate daugiau sportuoti, realiame pasaulyje einate į sporto klubą. Nusprendusiems labiau pasirūpinti privatumu internete, gali būti naudinga apsilankyti šifravimo vakarėlyje (angl. Cryptoparty). Lietuvoje tokių vakarėlių pasitaiko retai, tad siūlome mokyklai pačiai suorganizuoti šifravimo vakarėlį ar popietę. Tai ypač tiktų, pavyzdžiui, Saugesnio interneto dienai (kasmet vasario 5 d.) paminėti. Patartina popietės ar vakarėlio pradžioje aptarti šifravimo popietės elgesio kodeksą (angl. Code of Conduct). Informacinių technologijų srityje labiau pažengę moksleiviai galėtų būti šio vakarėlio „šifravimo angelais“. Mokytojams toks vakarėlis galėtų tapti galimybe išbandyti naujus mokymo(si) metodus ir prisiimti veikiau organizatoriaus nei „viską žinančiojo“ vaidmenį. Tokios popietės gali tapti ir reguliarios.

ŠALTINIAI

1)Kaip elgtis, kad asmeniniai duomenys telefone būtų saugūs // LRT (lietuvių k.). Prieiga per internetą: https://www.lrt.lt/naujienos/mokslas-ir-it/1/243276/perspeja-kaip-elgtis-kad-asmeniniai-duomenys-telefone-butu-saugus
2)Paieškos sistema „Duck Duck Go“: www.duckduckgo.com
3)Internetas kaip miestas (anglų k.). Prieiga per internetą: https://internetas.city
4)Ar jau atsisveikinote su teise į privatumą? E. Snowdeno dokumentai ir Lietuva // Universiteto žurnalistas (lietuvių k.). Prieiga per internetą: http://www.universitetozurnalistas.kf.vu.lt/2015/01/ar-jau-atsisveikinote-su-teise-i-privatuma-e-snowdeno-dokumentai-ir-lietuva/
5)Saugumo internete gidas (anglų k.). Prieiga per internetą: https://securityinabox.org/

6)Saugumas internete žurnalistams // Centre for investigative journalism (anglų k.). Prieiga per internetą: http://www.tcij.org/resources/handbooks/infosec
7)9 paieškos varikliai, siūlantys tai, ko negali Google // Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/9-paieskos-varikliai-siulantys-tai-ko-negali-google.d?id=61829973
8)Vokietijos Federalinė Žvalgybos tarnyba perspėja apie anoniminio tinklo Tor naudojimą // Netzpolitik (vokiečių k.). Prieiga per internetą: https://netzpolitik.org/2017/geheime-dokumente-der-bnd-hat-das-anonymisierungs-netzwerk-tor-angegriffen-und-warnt-vor-dessen-nutzung
9)Kodėl metaduomenys yra svarbūs // Surveillance Self-Defense (SSD) (anglų k.). Prieiga per internetą: https://ssd.eff.org/en/module/why-metadata-matters
10)Kaip būti saugesniam internete: išmanieji įrenginiai, šnipinėjimas, slaptažodžiai. Prieiga per internetą: https://www.youtube.com/watch?v=5j6oPZ4NMAM
11)Privatumas socialiniuose tinkluose // Auguinternete (lietuvių k.). Prieiga per internetą: https://www.auguinternete.lt/lt/patarimai/irankiu-sarasas/socialiniai-tinklai
12)Privatumas paieškos sistemose (anglų k.). Prieiga per internetą: https://restoreprivacy.com/private-search-engine/
13)Privatus naršymas „Mozilla“ naršyklėje. Prieiga per internetą: https://support.mozilla.org/lt/kb/privatus-narsymas
14)Kodėl svarbus privatumas internete ir kaip jį užtikrinti // Ted (anglų k.). Prieiga per internetą: https://ideas.ted.com/why-online-privacy-matters-and-how-to-protect-yours/
15)Kodėl svarbus privatumas // Choosetoencrypt (anglų k.). Prieiga per internetą: https://choosetoencrypt.com/privacy/why-you-should-take-your-privacy-seriously/?fbclid=IwAR0uTQbTB25dupWKku169eodRLfyAoWnq-VBgN4BtyVYnkou1PsLODHZBLM
16)Cryptoparty (anglų k.). Prieiga per internetą: https://www.cryptoparty.in
17)Google ir HTTPS // Eweek (anglų k.). Prieiga per internetą: https://www.eweek.com/security/google-makes-https-encryption-default-for-search
18)Privatumas naršklėse // NYTimes (anglų k.). Prieiga per internetą: https://www.nytimes.com/2018/04/19/technology/personaltech/browser-privacy-mode.html

5. Socialinių tinklų ypatumai

Patį populiariausią pasaulyje „Facebook“ prekės ženklą dažnai minime kaip socialinio tinklo sinonimą, tačiau derėtų patikslinti, kad socialiniais tinklais laikytini visi technologinės prigimties tarpininkai internete, vartotojams suteikiantys galimybę interaktyviai keistis informacija ir bendrauti. 2018 m. www.statista.com pateikiamais duomenimis, „Facebook“ (2,2 mlrd. vartotojų) ir vaizdo įrašų peržiūros ir dalijimosi platforma „Youtube“ (1,9 mlrd. vartotojų) – pasaulyje populiariausi socialiniai tinklai, trečią ir ketvirtą vietas dalijasi susirašinėjimo programėlės „WhatsApp“ (1,5 mlrd. vartotojų) ir „Facebook Messenger“ (1,3 mlrd. vartotojų). Išskyrus „Youtube“ (kuris yra paieškos sistemos „Google“ dalis), į ketvertuką patenkantys socialiniai tinklai šiuo metu nuosavybės teise priklauso „Facebook“ vadovui Markui Zuckerbergui ir kitiems akcininkams. Nedaug atsilieka ir to paties savininko valdomas „Instagram“ (1 mlrd. vartotojų). Taigi „Facebook“ savininkai apie vartotojus turi tikrai labai daug informacijos.

Nenuostabu, kad socialiniai tinklai, kaip jau sužinojote iš ankstesnių skyrių, yra didžiųjų duomenų kasyklos. Maža to, nemokamai socialiniais tinklais galima naudotis todėl, kad asmeniniai duomenys, kuriais ten pasidalijama, turi tokią didelę vertę, kad socialiniams tinklams

labai apsimoka visas kitas paslaugas siūlyti nemokamai. Anot kai kurių visuomenininkų, „Facebookui“ esame tokie naudingi, kad pats laikas būtų pagalvoti, ar nevertėtų iš tinklo pareikalauti pinigų už tai, kad juo naudojamės.

„Facebook“ sėkmė remiasi vadinamąja socialine diagrama (angl. Social Graph). Diagrama parodo, su kuo paskyrą socialiniame tinkle turintis asmuo draugauja, kokią muziką mėgsta, kokius leidinius ir straipsnius skaito, kur fiziškai yra (gyvena, dirba, keliauja, lankosi), kur mėgsta atostogauti. Mygtukas „Patinka“ bei kitos emocijos „Facebook“ socialiniam tinklui parodo, kas žmogui internete atrodo įdomu, dėl ko jis liūdi, kas juokinga, ką jis ypač mėgsta. Remdamasis visa šia informacija „Facebook“ gali reklamos užsakovams, perkantiems jo platformoje reklamą, pasiūlyti specialiai jiems pritaikytą, individualizuotą reklamą. Įvairios įmonės ir organizacijos be galo suinteresuotos „Facebook“ turima informacija. Šia informacija “Facebook” neprekiauja su trečiaisiais asmenimis, tačiau dalis informacijos (kurią skelbiate viešai) apie jus ir jūsų draugus gali būti prieinama įmonėms ir paslaugoms, prie kurių jungiatės naudodamiesi savo „Facebook“ paskyra.

2018 m. šiam socialiniam tinklui buvo nepavydėtini: krėtė daug privatumo pažeidimų skandalų, kurių rezultatas – apie 3 mln. vartotojų, ištrynusių savo socialinio tinklo paskyras, o kompanijos vertė rinkoje smuko daugiau kaip 120 mlrd. dolerių. Įvertinus iš vartotojų perspektyvos tai, kad „Facebook“ tiek daug kritikuotas, yra gan gerai, vadinasi, jam keliama aukštesnė paslaugų kokybės ir asmens duomenu saugumo kartelė.

Dabar truputį apie tai, kas nutiko. 2018 m. viduryje „Facebooką“ sukrėtė garsusis “Cambridge Analytica“ privatumo pažeidimo skandalas. „Cambridge Analytica“ – Didžiojoje Britanijoje registruota įmonė, apsimesdama, jog renka vartotojų duomenis mokslo tyrimų tikslais, sukūrė ir per „Facebook“ tinklą išplatino žaidimą „This Is Your Digital Life“ (panašų į Lietuvoje prieš porą metų populiarius „Sužinok, į kokią įžymybę esi panašus“, „Kurio „Sostų karų“ personažo bruožų turi daugiausiai“, „Top5 draugai, kurie brangina tavo draugystę labiausiai“). Įmonė surinko labai detalius duomenis apie „Facebook“ vartotojus ir jų draugus, įsitraukusius į žaidimą. Manoma, tokių buvo 87 milijonai (daugiausia JAV ir Didžiojoje Britanijoje, bet ir Australijoje bei Naujojoje Zelandijoje). Surinktieji „Cambridge Analytica“ duomenys buvo panaudoti visai ne mokslo ir pažinimo tikslams, o politinėse kovose paskleidžiant įvairiausią informaciją: nuo tiesioginės, labai tiksliai individualizuotos agitacijos, politinių konkurentų kompromitavimo per „Facebook“ socialinį tinklą ir kituose informacijos kanaluose iki melagingų žinių (angl. Fake News) paskleidimo tiems, kurie būtų linkę jomis patikėti. Teigta, kad „Cambridge Analytica“ reikšmingai prisidėjo prie respublikonų kandidato Donaldo Trumpo sėkmės JAV prezidento rinkimuose 2016-aisiais. Prezidentinė rinkimų kampanija buvo kupina sufabrikuotos ir melagingos informacijos, tarkim, esą pats popiežius parėmęs D. Trumpo kandidatūrą (tai buvo netiesa, o milijonai patikėjo!). Panašu, „Cambdridge Analytica“ reikšmė pergalei naujojo prezidento buvo įvertinta – Steve’as Bannonas, šios įmonės kampanijos metu vadovas, buvo pakviestas tapti D. Trumpo patarėju ir šias pareigas ėjo iki 2017-ųjų. Negana to, atsirado liudininkų, teigusių, jog „Cambridge Analytica“ prisidėjo per socialinius tinklus kurstydama euroskeptiškas nuotaikas, kai Didžioji Britanija balsavo dėl tolesnės narystės Europos Sąjungoje. Tiek D. Trumpo pergalė, tiek „Brexitas“ pasiekti įveikus konkurentus palyginti nedidele balsų persvara, todėl, manoma, „Cambridge Analytica“ vykdyta tikslinė rinkodara, kai rinkėjams pumpuota ne tik kruopščiai individualizuota agitacija, bet ir melagingos žinios apie konkurentus, galėjo tokiems rezultatams būti lemiama.

Apie „Cambridge Analytica“ veiklą pirmieji įtarimai žiniasklaidoje pasirodė dar 2015-aisiais. Tačiau „Facebook“ kaip įmanydamas bandė nuslėpti duomenų nutekėjimą, kuris įvyko pirmiausia dėl paties socialinio tinklo programinės įrangos saugumo spragų. Pagreitį duomenų skandalas įgijo, kai „Cambridge Analytica“ dirbęs programuotojas Christopheris Wylie viską išklojo žiniasklaidai. Jis taip pat liudijo, jog prie „Cambdridge Analytica“ surinktų vartotojų duomenų prieigą turėjo ir Rusijos specialiosios tarnybos.

Jau pačioje 2018-ųjų metų pabaigoje „Facebooką“ sukrėtė dar vienas privatumo pažeidimo skandalas. Paaiškėjo, jog šis socialinis tinklas suteikė labai plačią prieigą prie vartotojų duomenų didiesiems savo partneriams – „Microsoft“, „Amazon“, „Spotify“, „Netflix“. Anot „New York Times“, kuris gavo tai įrodančius dokumentus, „Spotify“ ir „Netflix“ turėjo galimybę skaityti visų „Facebook“ vartotojų privačius susirašinėjimus. Daugelis didžiųjų partnerių galėjo be sutikimo gauti detalią informaciją apie „Facebook“ vartotojų, besiregistruojančių jų platformose naudojantis „Facebook“ paskyra, draugų paskyras ir kontaktinę informaciją.

Negana to, 2019 m. pradžioje paaiškėjo ir dar viena „Facebook“ nepalanki aplinkybė – socialinis tinklas mokėjo vartotojams (iki 20 Eur per mėnesį), daugiausia paaugliams, naudojantiems „Facebook“ savo mobiliuosiuose įrenginiuose, už teisę prieiti apskritai prie visų jų duomenų ir veiklos tuose įrenginiuose. 20 eurų už 0 privatumo! Informacija naudota „Facebook“ rinkodaros tyrimų tikslams, o konkrečiai – rengtasi kovai su konkurentu „Snapchat“, kuris ypač išpopuliarėjo tarp paauglių.

Šiandien, po privatumo pažeidimo skandalų, „Facebook“ teigia, jog yra daug stipriau apribojęs trečiųjų šalių galimybes gauti vartotojų duomenis. Kompanija taip pat suteikė gerokai daugiau įrankių paskyrų savininkams reguliuoti savo privatumo nustatymus. Be to, pakoregavo ir savo tikslinių auditorijų politiką – dabar reklamos užsakovai tinkle turi mažiau galimybių nukreipti reklamą pagal tokius parametrus kaip politinės pažiūros. Nors duomenų rinkimo politika ir pakeista, vis dėlto pats „Facebook“ prieigą turi prie viso skelbiamo turinio, netgi kas rašoma privačiose vartotojų žinutėse, ir tai puikiai išnaudoja savo versle. Pasakytina, jog „WhatsApp“ susirašinėjimo programėlė, kol nebuvo parduota „Facebook“ savininkui, laikyta viena privačiausių ir saugiausių rinkoje. Deja, pasikeitus savininkui, vartotojų privatumas buvo gerokai apribotas.

Kelios problemos, kylančios socialiniuose tinkluose, yra specifinės. Tai 1) melagingų žinių sklaida, 2) neapykantos kalbos sklaida, 3) virtualios patyčios, kurios intensyvumu ir poveikiu yra didesnės nei anapus virtualybės, 4) sekstingas. Aptarkime kiekvieną iš jų.

5.1 Melagingos žinios

Melagingos (arba sufabrikuotos) žinios (angl. Fake news) - tai informacija, kurią pasitelkus skelbiama netiesa ir kuri nuo pat pradžios iki galo yra išgalvota, kuria siekiama apgauti skaitytojus (auditoriją). Melagingų žinių nereikėtų painioti su šališkai pateikta informacija arba nekokybiškai parengta informacija (kai pateikti vienas ar keli klaidingi faktai). Dažnai melagingomis žiniomis pavadinama žiniasklaidoje pasirodanti, adresatui tiesiog nepatinkanti medžiaga – net kai kurie garsūs politikos lyderiai tai, kas nepatinka, vadina melaginga ar sufabrikuota žinia. Vis dėlto šališkai pateikta informacija atspindi nuomonę–- vadinasi, galima diskutuoti apie ją ir tokią nuomonę kritikuoti, o dėl žiniasklaidoje pasitaikančios nekokybiškai parengtos informacijos sąžiningas autorius visada atsiprašys skaitytojų ir klaidas ištaisys, pripažindamas, jog suklydo. O melagingų žinių skleidėjai faktams ir tiesai neturi jokių sentimentų. Jie beatodairiškai bandys įtikinti auditoriją, kad išgalvoti faktai yra tiesa, į diskusijas apie faktų tikslumą nesileis, o ir blokuos tokias diskusijas keliančius oponentus ar tiesiog trins jų komentarus.

Melagingų žinių populiarėjimas susijęs su dviem pagrindiniais veiksniais:

1) Komerciniu (patraukliai ir sensacingai parašytos melagingos žinios gali atnešti pelno, nes pritraukia daug auditorijos į mažus interneto puslapius, todėl jiems lengviau parduoti reklamą ir iš to užsidirbti; reklama tokiuose puslapiuose domisi itin abejotinos vertės ir kokybės produktų gamintojai);
2) Politiniu (melagingos žinios gali būti skleidžiamos siekiant suformuoti tam tikrą nuomonę arba imtis norimų veiksmų).

Netrūksta melagingų žinių, rengiamų humoristiniais tikslais, pavyzdžiui, visiems žinomi Lietuvos žiniasklaidos pokštai, kai balandžio 1-ąją paskelbiama išgalvotų žinių ir žmonės spėlioja, kuri yra netikra. Anglakalbėje interneto erdvėje galima rasti satyros puslapių, skelbiančių netikras žinias, kad pralinksmintų auditoriją – pvz., www.onion.com. Savotiški yra globalaus sąmokslo teorijas skelbiantys šaltiniai, pavyzdžiui, jog Elvis Presley's arba Michaelas Jacksonas iki šiol gyvi, o valstybių lyderės Angela Merkel, Theresa May ir Dalia Grybauskaitė buvo bendraklasės, susimokiusios užvaldyti Europą.

Vis dėlto per socialinius tinklus skleidžiamos melagingos žinios gali turėti neatitaisomų pasekmių. Viename Indijos kaime gyventojai jau kurį laiką per „WhatsApp" dalijosi neaiškios kilmės žinia apie organų prekybai grobiamus vaikus. Gyventojai raginti būti budrūs, nes esą vaikų grobikai bet kada gali pasikėsinti ir į jų atžalas. Žinią iliustravo eilėmis suguldytų mirusių vaikų nuotrauka, kuri, pasirodo, buvo tikra – tačiau joje pavaizduoti ne organų prekeivių nukankinti vaikai, kaip buvo teigta, o tragiškas vaizdas iš Sirijos – per cheminio ginklo ataką žuvusių vaikų nuotrauka. Deja, gyventojai to nežinojo ir buvo ne juokais įbauginti. Vieną dieną į jų kaimelį užsuko grupė nevietinių vyrų, jie, sėdėdami kompanijoje po medžiu ir gurkšnodami arbatą, pavaišino pro šalį ėjusią vietinę mergaitę sausainiu. Gyventojai tiesiog pašėlo! Vienas per kitą „WhatsApp" socialiniu tinklu pradėjo skleisti žinia, jog šie vyrai atvyko grobti jų vaikų organų prekybai. Netrukus minia miestelio administraciniame pastate užspeistus svečius mirtinai sumušė. Po šio įvykio „WhatsApp" savininkai programėlėje įdiegė automatinį prierašą „persiųsta iš kito šaltinio" (angl. Forwarded), kad naujienomis per „WhatsApp" mėgstantys dalytis gyventojai stabtelėtų ir pamąstytų, ar tai, ką žinute gavo iš savo draugo, galėtų būti netiesa.

Lietuvoje tokių tragiškų įvykių dar nebuvo, tačiau nemažai melagingų žinių buvo paskleista apie krašto apsaugos sistemą: meluota apie krašto apsaugos savanorio savižudybę, apie tai, kad NATO kariai iš Vokietijos Jonavoje išprievartavo nepilnametę, apie tai, kad per NATO karines pratybas Alytuje žuvo vaikas. Melagingos žinios lietuvių kalba paskelbiamos neaiškios prigimties, nors gan skaitomuose interneto svetainėse – www.ldiena.lt, www.bukimevieningi.lt, www.pozicija.org, www.ekspertai.eu, kai kuriuose „Wordpress" tinklaraščiuose, uždarose

„Facebook“ grupėse, rusų kalba melagingos informacijos paskelbiama www.baltnews.lt. Reklamai skirtos melagingos žinios skelbiamos specialiai reklaminiams tikslams sukurtose svetainėse. Be to, Lietuvoje jau ne kartą buvo įsilaužta į žiniasklaidos priemonių (tv3.lt, BNS) turinio valdymo sistemas ir melagingos žinios paskelbtos kaip tų žiniasklaidos priemonių straipsniai. Tai ypač pavojinga, nes jei informacija įmanoma suabejoti, kai ji paskelbta neaiškios prigimties portale, tai autoritetingame žinių portale paskelbta informacija atrodo solidi ir patikima. Tiesa, tokie atvejai parodė, kad dalis žiniasklaidos internetinio turinio valdymo sistemų turėjo rimtų saugumo spragų – šie programišių įsilaužimai buvo gera proga tas spragas panaikinti ir ateityje būti budresniems.

Kaip galima būtų atskirti ir suprasti, ar paskleista žinia melaginga? Šis klausimas yra vienas svarbiausių mūsų informaciniame amžiuje, kai melagingos žinios gali nešti pelną ir politinių dividendų. Didžiausio pasaulyje žiniasklaidos laisvės istorijai skirto muziejaus Newseum edukatorių komanda siūlo taikyti E.S.C.A.P.E (angl. Evidence, Source, Context, Audience, Purpose, Execution) strategiją, kai vertinami įtartini ir abejonių keliantys informacijos šaltinius. Apžvelkime kiekvieną strategijos dėmenį:

1. E. – Įrodymai

Žinią grindžiančių faktų tikrinimas. Išsirinkite ir patikrinkite bent tris svarbiausius straipsnio faktus: jei žinia iliustruojama įvykio nuotrauka, patikrinkite (pvz., naudodami „Google“ nuotraukų paiešką) nuotrauką ir ar ji išties susijusi su įvykiu. Patikrinkite, ar žinioje minimi faktai pateikiami ir kituose, nesusijusiuose šaltiniuose. Jei nors vienas iš jūsų išsirinktų patikrinti faktų neatitinka tikrovės, tirkite toliau.

2. S. – Šaltinis

Šaltinio vertinimas susideda iš trijų pakopų: 1) Informacijos šaltinio, kuriame paskelbta medžiaga, vertinimo (ar tai žinoma ir patikima laikoma žiniasklaidos priemonė; ar žiniasklaidos priemonė turi skiltį „Apie“, ar skelbia apie savo redakcijos komandą; 2) Teksto autoriaus vertinimo (ar toks autorius egzistuoja; ar jis profesionalus žurnalistas, o gal jo kompetencijų sritis kita; kaip dažnai autorius bendradarbiauja žiniasklaidoje?); 3) Cituojamų asmenų vertinimo (jei faktus pateikia kompetentingai pristatomas ekspertas, patikrinkite, ar toks ekspertas apskritai egzistuoja ir ar jis turi pakankamai kompetencijos komentuoti, faktus patvirtinti arba paneigti).

3. C. – Konteksto tyrimas

Kontekstas tiriamas atsakant į kelis klausimus: kokia pagrindinė paskleistos informacijos žinia ir pristatoma problema? Ar pristatant problemą netrūksta paaiškinimų ir konteksto? ar tema / problema atskleidžia visą svarstomo klausimo paveikslą ar vis dėlto trūksta dėlionės detalių, o problema išimta iš konteksto? Į šiuos klausimus galima atsakyti tiriamai žiniai suradus keletą alternatyvių šaltinių, todėl užduotis rasti, ką kiti šaltiniai apie tokią problemą / temą praneša, yra būtinybė.

4. A. – Auditorija

Kam skirta ši informacija? Į šį klausimą atsakyti keliais lygmenimis: kokiai auditorijai skirtas / įdomus kanalas, kuriame paskelbta informacija; kaip paskelbta medžiaga atliepia tikslinės auditorijos nuomonę, poreikius ar smalsumą? Ką kita medžiaga, publikuojama analizuojamame kanale, pasako apie auditorijos interesus? Atsakius į šiuos klausimus, galima gan tiksliai apibūdinti tipišką žinios auditoriją ir numanyti, kodėl žinia skirta būtent jai.

5. P. – Tikslas

Koks paskelbtos medžiagos tikslas? Gali būti keletas: 1) edukuoti ir informuoti (tokioje žinioje bus daug detalių faktų, konteksto, relevantiškų šiai žiniai pranešti šaltinių. Edukuoti, informuoti siekiančios istorijos retai kada bus melagingos); 2) parduoti / autoriui arba žinios leidėjui padėti užsidirbti pinigų (patikrinkite, ar šalia pranešimo nėra kvietimo ko nors įsigyti, paremti, gal paskelbta reklama produkto, apie kurį pranešama); 3) padaryti įtaką auditorijos sprendimams, veiksmams, nuomonei (tokia žinia parašyta taip, kad skaitytojui kels daug emocijų, bus naudojama aštri ir arši leksika, išsakoma griežta kritika, arba – atvirkščiai – liaupsės). Įmanomas atvejis, kad paskelbta

žinia turės keletą tikslų, tačiau visur galima identifikuoti pagrindinį. Gerai pasvarstykite ir įvertinkite, kuris paskleistos žinios tikslas svarbiausias, ir pagal tai nuspręskite, ar žinia atrodo patikima.
6. E. – Įgyvendinimas
Kai vertinamas įgyvendinimas, reikėtų atkreipti dėmesį, kaip žinia sukurta. Reikėtų įvertinti šiuos parametrus: aiškumą (autoriaus gebėjimą aiškiai pristatyti problemą ir ją pagrindžiančią informaciją), stilių (kalbėsenos toną – patikimoje medžiagoje bus santūresnis), kalbos taisyklingumą (žurnalistai, kurių tikslas – patikimos informacijos sklaida, yra kalbos profesionalai, todėl jų tekstai bus patikimesni) ir vizualinę teksto prezentaciją (ar kanalo vizualinio dizaino stilius originalus, o gal nukopijuotas nuo kito panašaus, geros reputacijos kanalo; ar konkretaus teksto šriftas ir žymėjimas kuo nors skiriasi nuo paskelbtos kitos medžiagos tame pačiame kanale).

5.2 Neapykantos kalba

Neapykantos kalba (angl. Hate Speech) – tai tokia asmens saviraiška, kuria niekinami žmonės ar ištisos žmonių grupės dėl savybių, kurios nuo jų objektyviai nepriklauso arba priklauso itin mažai – pavyzdžiui, rasės, tautybės, lytinės orientacijos, tikėjimo, socialinės padėties, išvaizdos ir panašiai. Neapykantos kalba gali sutapti ir sykiu būti melaginga žinia arba patyčios, tačiau nebūtinai. Lietuvos Respublikos įstatymuose terminas „neapykantos kalba“ nevartojamas, tačiau Baudžiamajame kodekse numatyta atsakomybė kurstantiems neapykantą:

170 str.
2. Tas, kas viešai tyčiojosi, niekino, skatino neapykantą ar kurstė diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų,
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.
3. Tas, kas viešai kurstė smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba finansavo ar kitaip materialiai rėmė tokią veiklą,
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.

Baudžiamasis kodeksas numato, kad už neapykantos kurstymą atsakomybė gali būti taikoma ir juridiniam asmeniui, tačiau, pavyzdžiui, „Facebook“ dėl neapykantos kalbos sklaidos dar niekas nėra apskundęs Lietuvos institucijoms.

Neapykantos kalbos sklidimas per socialines medijas taip pat gali turėti itin tragiškų pasekmių. Automatizuotas neapykantos kalbos atpažinimas dirbtinio intelekto priemonėmis lietuvių kalba vis dar neišplėtotas, todėl globaliais socialiniais tinklais sklindanti neapykantos kalba, ypač mažesnių tautų ar rečiau vartojamomis kalbomis, gali pasiekti didelį kiekį žmonių ir vietinėmis kalbomis nekalbantys socialinių tinklų administratoriai jos nepastebės. Pavyzdžiui, Mianmare pradėjęs veikti „Facebook“ tapo neapykantos kalbos platforma iki šiol vykstančiam etniniam valymui. Vakarinėje šalies dalyje gyvenanti musulmonų rohindžų etninė religinė mažuma nuo 2016-ųjų pačios valstybės struktūrų ir budizmą išpažįstančių daugumos gyventojų yra užpuldinėjama, žudoma, prievartaujama, daugelis jų buvo priversti bėgti iš šalies į kaimyninį Bangladešą. Per „Facebook“ birmietiškai sklido raginimai žudyti, prievartauti, deginti, sušerti rohindžus kiaulėms, vietine kalba per socialinį tinklą garbintas Adolfas Hitleris ir jo „žydų politika“, rohindžai vadinti išsigimėliais, šunimis, prievartautojais. Tokios žinutės be jokių apribojimų sklandė socialiniame tinkle metų metus. Jungtinių Tautų Organizacija pareiškė, kad jei ne socialiniai tinklai, genocidas niekada nebūtų įgijęs tokio masto. Ir pats „Facebook“ pripažino, kad galėjo reaguoti skubiau.

Nors socialinis tinklas jau sukūrė įrankių pranešti apie neapykantos kalbą, jų efektyvumas nepasiekė piko, kadangi socialinis tinklas neturi visame pasaulyje padalinių, galinčių kompetentingai vertinti neapykantos kurstymą vietinėmis kalbomis. Be to, „Facebook“ socialiniame tinkle neapykantos kalba tarpsta uždarose tinklo grupėse, kuriose nestinga skatinimo smurtauti, engti ir diskriminuoti, kurios vienija nutolusius, bet tos pačios ideologijos vienijamus narius.

5.3 Patyčios

Patyčios socialiniuose tinkluose gali turėti ypač tragiškų pasekmių, kadangi, tarpininkaujant technologijoms, patyčias gerokai sudėtingiau valdyti. Virtualus tyčiojimasis gali vykti bet kuriuo paros metu bet kurioje interneto erdvėje, o stebėti gali neapibrėžtas kiekis vartotojų. Įžeidžios žinutės, nuotraukos ir tekstai taip pat ilgai išlieka prieinami, todėl vėl netikėtai iškilę seni patyčių epizodai žmogui, iš kurio tyčiotasi, tarsi smogia iš naujo. Patyčių aukoms virtualioje erdvėje sunku nuo tų epizodų pasislėpti, o ir aprėpti patyčių mastą. Pradeda atrodyti, kad visi aplinkiniai viską žino apie socialiniame tinkle patirtą gėdą, susidaro bejėgiškumo ir nebaudžiamumo įspūdis. Kibernetinėje erdvėje egzistuojančios patyčios dažniausiai vyksta tarp 13–18 metų paauglių. Dar svarbu pabrėžti, jog apie patyčias virtualioje erdvėje dėl gėdos, pažeminimo jausmo ir bejėgystės paaugliai neretai bijo kam nors prasitarti ir prašyti pagalbos. Dėl to tuomet, kai paaugliai pasiryžta kreiptis dėl pagalbos – reaguoti būtina, nes jie žengė išties labai svarbų žingsnį.

Geriau suprasti patyčių fenomeną ir jį suvaldyti pavyks atidžiau panagrinėjus žmogaus psichologiją ir patyčias skatinančius veiksnius. Galima išskirti keletą priežasčių, dėl kurių tyčiojamasi: 1) Asmeninis nesaugumas. Toks besityčiojantis žmogus nesijaučia gerai pats savo kūne, vertinamas ir vertingas. Kad pasijustų vertingas, toks žmogus sieks galios kontroliuoti kitus. Pasirinktas būdas gali būti kitų žmonių žeminimas ir įžeidinėjimas; 2) Pavydas. Tai vienas dažniausių motyvų. Pavydūs žmonės mano nusipelnantys didesnio pripažinimo, nei gauna. Todėl, norėdami geriau pasijusti būdami savimi, jie išjuoks, įžeis ar pasityčios iš kitų, kurie, jų manymu, pripažinimo gauna daugiau, nei nusipelno; 3) Prasti socialiniai įgūdžiai. Gali būti atvejų, kai besityčiojantis žmogus turi tokius prastus socialinius įgūdžius, kad nesuvokia įsitraukęs į patyčių ratą. Maža to, besityčiojantieji gali nesuvokti, kad jų komentarai ir tyčiojimasis gali žeisti; 4) Kita tyčiojimosi priežastis – besityčiojantis iš tiesų savo patyčių objektą mėgsta, o ne nekenčia, ir mano, kad „patraukti per dantį“ gali būti smagu. Taip gali elgtis gana artimi ir draugiški aplinkiniai. Pastaruoju atveju suvaldyti patyčias lengviau – užtenka nubrėžti ribas ir aiškiai pasakyti, jog pašiepiantys komentarai iš tiesų yra įžeidūs.

Verta pastebėti, kad paauglystėje sprendimų priėmimo įgūdžiai, kaip ir socialiniai įgūdžiai, tebėra formavimosi stadijos. Antai smegenų žievė, atsakinga už atsakingą sprendimų priėmimą, iki galo išsivysto maždaug 25-aisiais žmogaus gyvenimo metais, todėl tiek paauglių sprendimas tyčiotis, tiek reakcija į patyčias gali būti spontaniški, neapgalvoti dėl žmogaus raidos tendencijų. Turėdama tai galvoje, programavimą išmananti Risha Prabhu socialiniams tinklams sukūrė patyčių filtrą „Pamąstyk dar kartą“ (angl. „ReThink“), kuris, tik aptikęs įžeidžiantį turinį žinutėje, dar prieš ją paskelbiant socialiniame tinkle, autorių įspėja: „Ši Tavo žinutė gali įskaudinti. Ar esi tikras, kad nori ją paskelbti?“ Anot autorės, išanalizavusios 1500 atvejų, kai ketinta paskelbti įžeidžius komentarus socialiniuose tinkluose, patyčių, veikiant tokiam filtrui, sumažėjo net 93 procentais.

Apibrėžus priežastis, reikia aptarti ir galimus būdus reaguoti į patyčias. Keletas patarimų:

- Jei esate užsipuolamas virtualioje erdvėje, kad ir kaip sunku būtų, elkitės ramiai ar bent išlaikykite ramią povyzą (neparodykite, kaip tai jus paveikė). Tai visai nereiškia, kad

patyčios jūsų neturėtų paveikti – apie tai, kaip jaučiatės, pasikalbėkite su draugu, kuriuo pasitikite, ar suaugusiuoju.

- Gerai įvertinkite, ar verta socialiniuose tinkluose atsakyti besityčiojantiems žmonėms. Jei įsitrauksite į virtualų susirašinėjimą, didelė tikimybė, kad jus sieks pažeminti ir puls dar aršiau. Jei nusprendėte atsakyti, atsakykite tik vieną kartą konstatuodamas, pavyzdžiui, kad asmens sprendimas tyčiotis yra vertas paniekos, o ginčus galima spręsti civilizuotais būdais. Patikinkite, kad esate suinteresuotas tik tais civilizuotais būdais. Pasakius tiek, toliau į jokias diskusijas socialiniuose tinkluose nebesivelkite – ignoruokite ir dinkite iš akiračio. Toks komentaras pademonstruos, kad išliekate ramus ir galite pakilti aukščiau tyčiojimosi, o skaitantieji jūsų komentarą įsitikins: pats esate stiprus ir nesileidžiate pažeminamas. Mokėdami apsiginti visuomet kelsite pagarbą.
- Patyčias virtualioje erdvėje fiksuokite – jei jos eskaluosis tiek, kad bus verta įtraukti mokyklą ar net teisėsaugą, labai pravers, jei būsite surinkę įrodymų paketą. Geriausias metodas tokį surinkti – tai daryti susirašinėjimo kopijas, kopijuoti ekraną, fotografuoti mobiliuoju telefonu. Laikykite šiuos įrodymus saugiai ir su niekuo nesidalykite, išskyrus jus apginti galinčias institucijas.
- Jei patyčios pasiekia netoleruotiną lygį ir taikiai išsiaiškinti nepavyksta, praneškite socialinių tinklų administratoriams, paprašykite, kad įžeidžiančios žinutės būtų ištrintos. Apie patyčias administratoriams turėtų pranešti ir draugai, artimieji, nes išsiuntus daug pranešimų didėja tikimybė, kad įrašai bus pašalinti.
- Jei patyčios pasiekia netoleruotiną lygį, blokuokite besityčiojančių asmenų paskyras socialiniuose tinkluose, išmeskite juos iš draugų. Esant poreikiui, pakeiskite savo telefono numerį, susikurkite naują paskyrą, ištrynę senąją. Visa tai padės ignoruoti besityčiojančius - įsisąmoninkite, jog tai darote ne norėdami pasislėpti, o norėdami nusikratyti blogų emocijų. Išlikite orus, nesileiskite palaužiamas.
- Jei patyčias patiriate ne jūs, o jūsų draugas, pažįstamas – apginkite draugą. Pasakykite viešai, kad besityčiojančių žmonių elgesys yra niekingas.

5.4 Sekstingas

Niekas nenorėtų, kad privačios, ypač intymios nuotraukos, gauti meilės laiškai būtų pasviešinti. Deja, interneto mieste tokia praktika pasitaiko dažnai ir šio miesto gyventojams turi skaudžių pasekmių. Turime omenyje vaikų ir paauglių sekstingą. Kas yra sekstingas? Paramos vaikams centras sekstingą apibrėžia kaip atvirai seksualaus turinio žinučių, apnuoginto ar nuogo kūno nuotraukų, filmukų siuntimą ar gavimą naudojantis mobiliuoju telefonu, kompiuteriu ar kita skaitmenine priemone. Šis žodis yra angliškų žodžių sex (seksas) ir texting (keitimasis žinutėmis) junginys.

Psichologinės sekstingo priežastys ir pasekmės. 2011 m. Sonios Livingstone ir kt. publikuotos studijos, kurios metu buvo apklausti vaikai 25-iose Europos šalyse, duomenimis, 15 proc. 11–16 metų europiečių yra gavę „seksualinio turinio žinučių ar vaizdų, kuriuose kalbama apie užsiėmimą seksu arba vaizduojami nuogi ar seksu užsiimantys žmonės“; 3 proc. vaikų sako, kad patys siuntė tokias žinutes arba jas viešino; 1 iš 8 vaikų, gavusių tokias žinutes, arba beveik 2 proc. visų vaikų tokios žinutės nuliūdino. Tik 4 iš 10 vaikų, kuriuos sekstingas sutrikdė, užblokavo jas siuntusį žmogų arba ištrynė nepageidaujamas žinutes. Galima numanyti, kad paauglių sekstingo ir iš jo kylančių problemų mastas išaugo.

Kodėl vaikai siunčia seksualinio pobūdžio informaciją skaitmeninėmis priemonėmis? Didelę įtaką paaugliams daro garsenybės ir jų įvaizdis, taip pat „Instagram“ ar kitų socialinių tinklų

žvaigždės. Paaugliai nori būti panašūs į mėgstamas garsenybes, jas mėgdžioja, įskaitant ir savęs fotografavimą seksualizuotomis pozomis.

Taip pat galima teigti, kad informacijos apie socialinių tinklų ir apskritai interneto veikimą stoka prisideda prie sekstingo plitimo. Pavyzdžiui, tarp paauglių ypač populiarus socialinis tinklas „Snapchat“ vartotojams sukuria iliuziją, kad jų fotografijos (angl. Snaps) po kelių sekundžių automatiškai dingsta iš gavėjo ekrano. „Niekas kitas mano nuotraukos nepamatys“, – dažnai mano paaugliai ir ilgai nesvarstę išsiunčia pusnuogio kūno fotografiją savo vaikinui ar merginai ar net nepažįstamam žmogui. Tačiau kiekviename išmaniajame telefone ekrano kopijavimo funkcija (angl. screenshot) leidžia fotografijos gavėjui pasidaryti nuotraukos kopiją ir išsisaugoti ją išmaniajame įrenginyje. Iš ten nuotraukos gali būti įkeltos į kitus socialinius tinklus ir taip tapti prieinamos dideliam ratui žmonių. Kita „Snapchat“ problema – programėlės profiliai pagal standartinius nustatymus yra viešai prieinami, tad bet kas, žinantis naudotojo vardą, gali pasižiūrėti, ką šis paskelbė savo istorijoje (angl. Story).

Susirašinėjimų platforma „WhatsApp“ yra dar problemiškesnė. Naudojant šią platformą išsiųstos nuotraukos ir filmukai, kitaip nei „Snapchat“, nedingsta automatiškai, tad jų turinys gali dar lengviau išplisti. Fotografijų dalijimosi platformos „Instagram“ automatiniai nustatymai taip pat nenumato jokio privatumo ir gali būti peržiūrėti net tų, kurie neturi profilio. Todėl labai svarbu pradėjus naudoti šią platformą pasikeisti savo paskyros privatumo nustatymus.

Kita sekstingo plitimo priežastis – asmuo nemoka nubrėžti asmeninių ribų ir, viena vertus, negeba pasakyti „ne“, antra vertus, negerbia kito asmeninių ribų. Sekstingas kai kuriems paaugliams taip pat atrodo kaip vienas iš saugesnio sekso būdų, tačiau retai susimąstoma apie galimas neigiamas šio elgesio pasekmes.

Viena dažniausiai pasitaikančių paauglių sekstingo padarinių – elektroninės patyčios. Apsinuoginusio paauglio nuotrauka yra siunčiama mylimam žmogui, šis nusprendžia persiųsti draugui ir netrukus apie tai kalba visa mokykla. Seksualinio pobūdžio susirašinėjimai, nuotraukos ar filmukai gali būti paviešinti ir pametus telefoną, jei jį rado piktų kėslų turintis žmogus. Iš sekstingo kylančios patyčios yra platesnės problemos – visuomenės požiūrio į apnuogintą ar nuogą kūną – atspindys[1].

Kitaip nei tiesioginės komunikacijos atveju, skaitmenine forma paviešinta informacija yra ilgai prieinama, gali būti randama naudojantis paieškos varikliais, ją galima kiek nori kartų kopijuoti. Skaitmeninis formatas leidžia informaciją išimti iš pirminio ir įkelti į visai kitą kontekstą. Tai lemia, kad sekstingo pagrindu atsiradusias patyčios, kaip ir bet kokias elektronines patyčias daug sunkiau sustabdyti.

S. Livingstone ir kt. studijos duomenimis, Lietuvos vaikai, palyginti su kitų Europos šalių vaikais, yra neblogai susipažinę su interneto galimybėmis ir jas naudoja (juos pralenkia tik Nyderlandų vaikai), tačiau ir interneto pavojai juos paveikia labiau nei kitų šalių vaikus. Lietuvos vaikai išsiskiria patiklumu, o sekstingu, kaip žinia, užsiima ne tik bendraamžiai, bet ir piktavališkais tikslais netikrus profilius susikūrę žmonės. Net 23 proc. vaikų iš Lietuvos su žmonėmis, su kuriais pirmiausia susipažino internete, susitinka, tai yra vienas aukščiausių rodiklių, palyginti su kitomis Europos šalimis. Sekstingas gali tapti įrankiu vaikui prisivilioti ir jam seksualiai išnaudoti. Pasitelkus sekstingą vaikas taip pat gali tapti prekybos žmonėmis auka.

Teisinės sekstingo pasekmės. Be psichologinių pasekmių aukai, sekstingas gali turėti skaudžių teisinių pasekmių intymias vaiko fotografijas, vaizdo įrašus ar susirašinėjimus paviešinusiam asmeniui. Už nusikaltimus interneto mieste gali būti nubausta realiame pasaulyje, o vaiko intymių fotografijų, vaizdo įrašų ar susirašinėjimų paviešinimas internete ar net tokios medžiagos laikymas savo telefone pagal Lietuvos Respublikos įstatymus yra nusikaltimas. Apibūdinant vaikus Baudžiamajame įstatyme naudojamos šios sąvokos:

1) vaikas, nepilnametis – asmuo, kuris nėra sulaukęs 18 metų,

2) asmuo, jaunesnis negu 16 metų,

3) mažametis (mažametis vaikas) – asmuo, jaunesnis nei 14 metų.

Intymių fotografijų, vaizdo įrašų ar susirašinėjimų paviešinimas internete pažeidžia Visuotinėje žmogaus teisių deklaracijoje įtvirtintas teises į asmens saugumą, privatumą, apsaugą nuo savavališko kišimosi į susirašinėjimą, už juos Lietuvos Respublikos baudžiamajame kodekse numatyta baudžiamoji atsakomybė.

Už sekstingo metu gautos informacijos paviešinimą bausmių yra įvairių: pradedant viešaisiais darbais ir baigiant laisvės atėmimu iki aštuonerių metų. Lietuvos prokuratūros teigimu, atsakomybės pobūdis priklauso nuo vaiko, kurio intymios fotografijos, vaizdo įrašai, susirašinėjimai buvo paviešinti, amžiaus, paviešintos medžiagos pobūdžio, t. y. ar ji priskirtina pornografijai, ar ne. Bausmės pobūdis taip pat priklauso nuo to, kokiu būdu fotografijos, vaizdo įrašai ar susirašinėjimai buvo gauti ir kokio amžiaus buvo medžiagą paviešinęs asmuo. Baudžiamojon atsakomybėn traukiami asmenys, sulaukę 16 metų, ir juridiniai asmenys.

Lietuvos prokuratūra informuoja, jog tuo atveju, jei fotografijos, vaizdo įrašai, susirašinėjimai nėra pornografinio turinio, jų darymas ir paviešinimas be asmens ar jo teisėto atstovo leidimo gali būti kvalifikuojamas pagal Lietuvos Respublikos baudžiamojo kodekso (toliau – BK) 167 straipsnį kaip neteisėtas informacijos apie privatų asmens gyvenimą rinkimas ir pagal BK 168 straipsnį kaip neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas. Už šias abi veikas baudžiama viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų. Už neteisėtą informacijos apie asmens privatų gyvenimą atskleidimą ar panaudojimą pagal BK 168 straipsnį baudžiama tik tada, kai nukentėjusysis ar jo atstovas pateikia pareiškimą policijai arba kai to reikalauja prokuroras.

Jeigu fotografijos, vaizdo įrašai, susirašinėjimai yra pornografinio turinio, jų darymas ir paviešinimas, priklausomai nuo jų sukūrimo būdo ir aplinkybių, yra kvalifikuojami kaip disponavimas pornografinio turinio dalykais pagal BK 309 straipsnį arba pagal BK 162 straipsnį kaip vaiko išnaudojimas pornografijai. Lietuvos visuomenės informavimo įstatymas pornografinio pobūdžio informaciją apibrėžia kaip informaciją, „kai atvirai ir detaliai rodomas tikras ar suvaidintas lytinis aktas, lytiniai organai, tuštinimasis, masturbacija arba lytiniai iškrypimai (pedofilija, sadizmas, mazochizmas, zoofilija, nekrofilija ir kt.), ir tai yra pagrindinis tokios informacijos tikslas“. Už pornografinio turinio medžiagos, kurioje vaizduojamas vaikas, gaminimą, laikymą ar platinimą baudžiama bauda arba laisvės atėmimu iki ketverių metų. Tokiomis bausmėmis gali būti nubaustas, pavyzdžiui, 16-metis, socialiniuose tinkluose išplatinęs nuogos bendraklasės, kuriai, tarkim, 17 metų, fotografijas. Nubausti gali būti ir bendraklasiai, kurie minėtą fotografiją atsisiuntė į savo išmanųjį įrenginį ir per pertraukas rodė kitiems, tačiau, žinoma, dėl nusikaltimo sudėties ir bausmių kiekvienu atveju sprendžia teismas. Jei fotografija buvo rodoma, pavyzdžiui, 15-mečiams, už tokią veiklą gali tekti atsakyti ir pagal BK 153 straipsnį „Jaunesnio nei 16 metų asmens tvirkinimas“. Ši veika baudžiama laisvės apribojimu arba areštu, arba laisvės atėmimu iki penkerių metų.

BK 162 straipsnis numato, kad „tas, kas verbavo, vertė arba įtraukė vaiką dalyvauti pornografinio pobūdžio renginiuose, arba išnaudojo vaiką tokiems tikslams, arba išnaudojo vaiką pornografinei produkcijai gaminti, arba pelnėsi iš tokios vaiko veiklos, baudžiamas laisvės atėmimu iki aštuonerių metų“. Pavyzdžiui, primygtinis prašymas nusirengti prieš kamerą ir gauto vaizdo įrašo išsiuntimas bendraklasiams, priklausomai nuo to, kas vaizduojama išsiųstame įraše, teismo gali būti traktuojamas kaip išnaudojimas pornografinei produkcijai gaminti.

Net darydamas ir laikydamas savo paties fotografijas, vaizdo įrašus bei savo susirašinėjimus su kitu nepilnamečiu, vaikas gali būti patrauktas baudžiamojon atsakomybėn, jei ši medžiaga priskiriama pornografijai ir jam yra suėję 16 metų. Be to, pasak Lietuvos prokuratūros, tuo atveju, jei vaikui suėję 16 metų, o vaikui, su kuriuo jis susirašinėja seksualinio pobūdžio žinutėmis, nėra suėję 16 metų, toks susirašinėjimas gali būti kvalifikuojamas pagal BK 153 straipsnį kaip jaunesnio nei 16 metų asmens tvirkinimas.

Svarbu pridurti, kad baudžiamąją atsakomybę užtraukia ir kitų žmonių susirašinėjimo, net jei jis nėra intymaus turinio, perėmimas, fiksavimas ar stebėjimas, kai tai daroma be jų ar jų teisėtų atstovų sutikimo. Net ir nepaviešinus susirašinėjimo, tai yra pagal BK 166 straipsnį kaip asmens susižinojimo neliečiamumo pažeidimas. Pagal minėtą straipsnį baudžiama viešaisiais darbais, bauda, laisvės apribojimu, areštu arba laisvės atėmimu iki dvejų metų.
Bet kuris, gavęs kito žmogaus nuotraukų, vaizdo įrašų ar asmeninių susirašinėjimų, turėtų juos nedelsdamas ištrinti, kad netaptų nusikaltimo bendrininku. Šiuo atveju nesvarbu, ar atsiųsta informacija yra seksualinio pobūdžio, ar ne.

Ką daryti? Kalbantis su moksleiviais apie sekstingą svarbu jų nekaltinti dėl dalijimosi intymiomis nuotraukomis. Viena, sekstingas yra požymis, kad paaugliai bręsta seksualiai, ir jiems svarbu išmokti suprasti, kokių pasekmių gali turėti vienas ar kitas seksualumo išraiškos būdas. Antra, nukentėjusiems nuo sekstingo paaugliams reikia ypač daug palaikymo, o smerkimas mažina norą ieškoti pagalbos.

Kaip elgtis, jei klasėje yra moksleivių, jau nukentėjusių nuo sekstingo ir / ar patyčių? Pirmiausia, svarbu sukurti atmosferą, kuri moksleiviui signalizuotų, kad jumis galima pasitikėti ir į jus kreiptis pagalbos. Jei moksleivis papasakojo apie sekstingo atvejį (pavyzdžiui: kas nors jį spaudžia dalytis seksualinio pobūdžio nuotraukomis ar filmukais), patikinkite, kad jis yra ne vienas ir niekas neturi teisės versti jo daryti to, ko nenori, ir kartu pasvarstykite, kokių tolesnių veiksmų reikėtų imtis.

Jei su moksleiviu siejamas seksualinio pobūdžio turinys jau plinta socialiniuose tinkluose, pats moksleivis, priklausomai nuo savo amžiaus, arba jo teisėtas atstovas gali kreiptis į socialinio tinklo administratorių ir paprašyti šį turinį pašalinti. Su sekstingu susijusios informacijos paviešinimas dažnai sukelia psichologinių kančių, tad moksleiviui gali būti naudinga pasikalbėti su mokyklos ar savivaldybės psichologu. Sekstingą ir / ar patyčias išgyvenusiems vaikams emocinę paramą internetu ir telefonu taip pat teikia „Vaikų linija“ (www.vaikulinija.lt) ir – nuo 16 metų – „Jaunimo linija“ (www.jaunimolinija.lt). Kitas žingsnis – kreiptis į teisėsaugos institucijas.

UŽDUOTYS

I. Vizualios informacijos tikrinimas.
Pamoka bus interaktyvesnė, jei naudokite virtualaus balsavimo sistemas Sli.do, www.mentimeter.com ar kt. – taip moksleiviai labiau įsitrauks. Paaiškinkite jiems, kad daug informacijos internete grindžiama vaizdais, tačiau mums gali būti rodoma ne tai, kas rašoma, kad rodoma. Norėdami neapsigauti turime nuolat kritiškai mąstyti ir pasitelkti jau turimas žinias. Ekrane atidarykite šią nuorodą https://firstdraftnews.org/articulate/obsc/story_html5.html ir pakvieskite moksleivius atpažinti, kur daryta nuotrauka. Paraginkite tikrinti informaciją visais jiems prieinamais būdais.
II. Užduotis turėtų būti atliekama mėnesį ar kelias savaites.
Pradėkite pamoką paaiškindami, kas yra patyčios ir kodėl jos tarp paauglių dažnesnės nei tarp suaugusiųjų (naudokite Jums pateiktą medžiagą). Paklauskite moksleivių, ar kas iš jų pačių arba iš draugų, pažįstamų yra susidūręs su patyčiomis ir dėl kokių priežasčių, jų nuomone, patyčių pasitaiko. Fasilitatorius (mokytojas) turėtų įsiterpti sudėliodamas akcentus, kodėl patyčių pasitaiko. Pasibaigus diskusijai, pateikite moksleiviams užduotį: sukurti istoriją apie patyčias patyrusį žmogų; istorija turi būti realistiška, tačiau visi veikėjai ir situacijos turi būti išgalvotos. Kad būtų įdomiau, pakvieskite istoriją papasakoti videopasakojimo forma, patiems tampant aktoriais ir filmuojant mobiliaisiais telefonais. Videopasakojime turi būti užfiksuota patyčių situacija ir jos kontekstas, kas sukėlė ir kodėl. Parodyti situaciją iš besityčiojančių asmenų ir patyčias patiriančio asmens

perspektyvos. Kuriant tokį vaizdo įrašą, geriausia dirbti 5–6 vaikų grupėje. Šiai užduočiai atlikti skirkite savaitę. Po savaitės pamokos metu visi kartu peržiūrėkite moksleivių videopasakojimus. Po kiekvieno pasakojimo patikslinkite detales, paklauskite, kodėl pasirinkta tokia istorija, kaip, jų manymu, patyčių problema galėtų būti sprendžiama.

III. Užduotis raštu, minčių lietus arba filmukai „Kas yra sekstingas“.
1) Pamoką galite pradėti nuo užduoties „Eglės pasakojimas“. Užrašykite ant lentos: „Niekas nepadaro tavęs tokios pažeidžiamos kaip nuotraukos, kuriose tu nuoga“, – sako Eglė, jai 15 metų. Kas galėjo nutikti Eglei, kad ji taip galvoja? Parašykite trumpą pasakojimą.“ Tegul moksleiviai parašo trumpą savo sugalvotą istorijos versiją. Paprašykite keleto moksleivių garsiai perskaityti jų sugalvotas istorijas.
2) Prieš pradėdami kitas užduotis įsitikinkite, kad visi žino, kas yra sekstingas. Jei moksleiviai negirdėjo termino „sekstingas“, galite:
a) suorganizuoti minčių lietų „Kas yra sekstingas“. Užrašykite ant lentos „Sekstingas“ ir paklauskite moksleivių, su kokiomis asociacijomis jiems siejasi šis žodis. Naudojant šį metodą ypač svarbu atkreipti dėmesį, kad moksleiviai nebūtų įžeidinėjami, o jei taip atsitinka, svarbu pabrėžti, kad toks elgesys nebus toleruojamas.
b) perskaityti sekstingo apbrėžimą: „Sekstingas yra atvirai seksualaus turinio žinučių, apnuogintų ar nuogų kūno nuotraukų, filmukų siuntimas ar gavimas, naudojantis mobiliuoju telefonu, kompiuteriu ar kita skaitmenine priemone. Šis žodis yra angliškų žodžių „sex“ (seksas) ir „texting“ (keitimasis žinutėmis) junginys.“ (Šaltinis: „Tėvams ir specialistams: kas yra sekstingas?“, Paramos vaikams centras. Prieiga per internetą: http://www.pvc.lt/lt/component/content/article/2-be-kategorijos/292-tevams-ir-specialistams-kas-yra-sekstingas)
c) parodyti filmuką: „Handysektor“ filmukas „Kas yra sekstingas?“ 3 min.
Anglų kalba: https://www.youtube.com/watch?v=IIRxL-gimmE&index=7&list=PLWY203OqMpZbO7D0rIYAkc28Gsr3IbJMF
Vokiečių kalba (tinka per vokiečių kalbos pamokas): https://www.handysektor.de/artikel/handysektor-erklaert-was-ist-eigentlich-sexting/
Lenkų kalba: https://www.youtube.com/watch?v=56md6VjH0A0&index=4&list=PLWY203OqMpZbO7D0rIYAkc28Gsr3IbJMF

IV. Užduotis raštu, diskusija „Neigiamos sekstingo pasekmės“.
1) Dabar, kai visiems aišku, kas yra sekstingas, metas pereiti prie antrosios užduoties raštu. Užrašykite ant lentos: „Jei būčiau žinojęs, kas atsitiks, niekada nebūčiau persiuntęs Justės nuotraukos Jonui. Labai graužiuosi dėl savo elgesio“, – sako Mantas, jam 15 metų. Kas galėjo nutikti Mantui, kad jis taip galvoja?“ Tegul moksleiviai parašo trumpą savo sugalvotą Manto istorijos versiją. Pakviskite keletą moksleivių garsiai perskaityti užrašytas istorijas.
2) Pamoką tęskite kartu su klase apibrėždami ir diskutuodami apie neigiamas sekstingo pasekmes, jas surašykite ant lentos. Prisiminkite Eglės bei Manto istorijas ir drauge su klase pasvarstykite, kokius probleminius sekstingo aspektus paliečia jų istorijos.
Galimos sekstingo pasekmės:

- Neteisėtas intymių fotografijų ar filmukų persiuntimas per trečiuosius asmenis („antrinis sekstingas“). Kalbėdami apie šį aspektą būtinai pabrėžkite, kad neteisėtas seksualinio turinio persiuntimas yra nusikalstama veikla ir kad nepersiųsdami turinio sekstingo aukas apsaugome nuo neigiamų emocijų. Pabrėžkite visų sekstinge dalyvaujančių atsakomybę.
- Aukos kaltinimas, skirtingas vaikinų / berniukų ir merginų / mergaičių elgesio vertinimas (kekšės įvaizdis; „pati kalta“). Temiškai aptarkite stereotipinius lyčių vaidmenų modelius ir empatijos trūkumą.

- Skaitmeninės / elektroninės patyčios, kurios sukelia didžiulę psichologinę žalą
- Teisiniai aspektai, ypač baudžiamąją atsakomybę užtraukianti vaikų pornografija sekstinge.
- Spaudimas naudojantis sekstingo metu persiųstas nuotraukas ar vaizdo įrašus (Angl. Sextortion).
- Buvusių partnerių ar geriausių draugų pasitikėjimo praradimas.

V. Darbas grupėmis. Projektas „Kaip apsisaugoti nuo sekstingo“.
1) Patartina, kad prieš imdamiesi projekto moksleiviai jau būtų susipažinę su šia tema ankstesnėje pamokoje. Projektui atlikti reikalingas laikas – 45 minutės. Pamokos pradžioje supažindinkite moksleivius su viena iš kampanijų, skirtų sekstingo prevencijai:
a) Lietuvos policijos filmukas „Pavojai internete“, 10 min. 35 sek. (lietuvių kalba): https://www.youtube.com/watch?v=JdSS51C08Fo&frags=pl%2Cwn.
b) Plakatai iš Šveicarijos edukacinės kampanijos vokiečių kalba: „Sekstingas gali padaryti tave žinimą – net jei to nenori.“ Plakatus galite parsisiųsti iš čia: https://www.projuventute.ch/index.php?id=2492.
c) Reakcijų memai iš Jungtinės Karalystės. „Zipit“ mobilioji programėlė (anglų kalba): https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/zipit-app/. Galite pasiūlyti moksleiviams parsisiųsti nuotraukų iš programėlės galerijos. Jeigu jie susidurtų su spaudimu atsiųsti seksualinio pobūdžio nuotraukų, būtų tam pasiruošę.
d) „Forever“ vaizdo įrašas iš Airijos (bei kiti vaizdo įrašai ir informacija) anglų kalba: https://www.webwise.ie/lockers/lockers-resource-videos/.
2) Suskirstykite moksleivius į grupes po 4–6. Tegu jie patys sukuria nedidelę kampaniją, skirtą informuoti, kaip galima apsisaugoti nuo neigiamų sekstingo pasekmių. Tegul parengia pasirinktinai:
a) Informacinį 2 puslapių plakatą (reikės perlenkto A4 lapo);
b) „Powerpoint“ pristatymą – 3 skaidres (reikės kompiuterio ir „Powerpoint“ programos);
c) Reakcijų memus, kaip reaguoti, jei kas nors prašo atsiųsti apsinuoginusio nuotraukas (reikės išmaniojo telefono, kompiuterio arba planšetinio kompiuterio ir memų generatoriaus, pvz., www.memegenerator.net);
d) 30 sek. vaizdo įrašą išmaniuoju telefonu.
Tam skirkite 30 minučių.
3) Pamokos pabaigoje kiekviena grupė trumpai pristato savo kampaniją ar informacinę medžiagą klasei. Visoms grupėms pristačius kampanijas, galima peržvelgti, galbūt yra dar nepaminėtų būdų kovoti su sekstingu. Apie juos taip pat pasikalbėkite su moksleiviais.
4) Pasikalbėkite su pačiais moksleiviais ir mokyklos administracija ir nuspręskite, ar nevertėtų surengti kampanijų / informacinės medžiagos parodą.

VI. Užklasinė veikla
Nueikite su paaugliais į spektaklį „Lė-kiau-lė-kiau“, jei tik jis rodomas jūsų mieste.

ŠALTINIAI

1)Vienoje Lietuvos mokykloje buvo iškabinėtos nuogos moksleivės nuotraukos. Pati moksleivė ir jos mama į tai sureagavo labai ramiai. Jų požiūris į nuogą kūną buvo ta priežastis, dėl kurios patyčios šiuo atveju neįsibėgėjo. Šaltinis: Lietuvos radijo laida „Paraštės“. Prieiga internete: http://www.lrt.lt/mediateka/irasas/1013632436/parastes-2017-03-05-22-07#wowzaplaystart=0&wowzaplayduration=2986000

2)Pagalvok, prieš rašant // Ted (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=YkzwHuf6C2U
3)Facebook ir neapykantos kalba // BBC (anglų k.). Prieiga per internetą: https://www.bbc.com/news/technology-45196167
4)Bitiukova, Natalija. Neapykantos kurstymas Lietuvoje. Dažniausiai užduodami klausimai. Vilnius, 2014. Prieiga per interetą: http://manoteises.lt/wp-content/uploads/2014/07/Neapykantos_kurstymas_DUK_20110629.pdf
5)Selfies, Sexting, Selbstdarstellung“ . Erschienen: 2018 , Juli (2. aktualisierte Auflage). DIN A4, 68 Seiten.
6)Herausgeber: Initiative. Datenschutz geht zur Schule. Erschienen: 2018 , November (3. vollständig überarb. Auflage). DIN A4, 324 Seiten
7)Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online. Prieiga per internetą: http://eprints.lse.ac.uk/33731/
8)Saugesnis internetas Jūsų vaikams. Prieiga per internetą: https://www.auguinternete.lt/
9)EU Kids online 2014 m. Studija. Prieiga per internetą: http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf
10)Tarp Lietuvos paauglių plinta sekstingas // 15min (lietuvių k.). Prieiga per internetą: https://www.15min.lt/vardai/naujiena/lietuva/tarp-lietuvos-paaugliu-plinta-sekstingas-1050-424261
11)Sekstingas – paauglių tykanti grėsmė // Pajūrio naujienos (lietuvių k.). Prieiga per internetą: http://pajurionaujienos.lt/?sid=14240&act=exp
12)Jaunimas socialiniuose tinkluose: kodėl privatumas noriai išmainomas į patogumą? // Teisė Pro (lietuvių k.). Prieiga per internetą: http://www.teise.pro/index.php/2018/06/22/jaunimas-socialiniuose-tinkluose-kodel-privatumas-noriai-ismainomas-i-patoguma/
13)Lietuvos Respublikos Baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas (lietuvių k.). Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/YbDReLlpRC
14)Paaugliams – rūpestis dėl intymių nuotraukų internete // Alfa (lietuvių k.). Prieiga per internetą: https://www.alfa.lt/straipsnis/16130184/paaugliams-rupestis-del-intymiu-nuotrauku-internete
15)7 patarimai tėvams, kad jūsų vaikas būtų saugesnis socialiniuose tinkluose// Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/gyvenimas/seima/7-patarimai-tevams-kad-jusu-vaikas-butu-saugesnis-socialiniuose-tinkluose.d?id=76367123
16)Saugumas internete. Prieiga per internetą: https://www.nukentejusiems.lt/iki18/kas-yra-nusikaltimas/saugumas-internete/
17)Nusikaltimai prieš vaikus. Prieiga per internetą: https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-pries-vaikus/184
18)Lietuvos Respublikos visuomenės informavimo įstatymas, 1996 m. liepos 2 d. Nr. I-1418. Suvestinė redakcija nuo 2019-01-01 iki 2019-06-30. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/KambyVXeSS
19)Paramos vaikams centro medžiaga tėvams ir specialistams. Prieiga per internetą: http://www.pvc.lt/lt/component/content/article/2-be-kategorijos/315-tevams-ir-specialistams
20)Video transliacija „Mąstau, todėl nesiunčiu – kaip mokytojai gali padėti mokiniams išvengti sekstingo spąstų.“ Pokalbis su Paramos vaikams centro psichologe, programos „Vaikystė be smurto" vadove Ieva Daniūnaite. Prieiga per internetą: http://mokytojotv.blogspot.com/2018/02/mastau-todel-nesiunciu-kaip-mokytojai.html
21)Paraštės. Kaip elgtis paaugliams, susidūrus su patyčiomis internete arba išplitus intymioms nuotraukoms? Kas yra sekstingas? Laidoje taip pat rasite patarimų tėvams, kaip elgtis, kai jūsų vaikas susiduria su interneto pavojais. Kalba Vaikų linijos savanorė ir Paramos vaikams centro programos „Vaikystė be smurto" vadove Ieva Daniūnaite. Prieiga per internetą:

http://www.lrt.lt/mediateka/irasas/1013632436/parastes-2017-03-05-22-07#wowzaplaystart=0&wowzaplayduration=2986000
22)Sekstingas // Klicksafe (vokiečių k.). Prieiga per internetą: https://www.klicksafe.de/themen/problematische-inhalte/sexting/
23)Informacija apie žmogaus teises (lietuvių k.). Prieiga per internetą: manoteises.lt
24)Klausk tėčio ir (ar) mamos: kaip pasirengti lytiniam švietimui namuose. Metodinis vadovas (lietuvių k.). Prieiga per internetą: http://www.askproject.eu/upload/deliverables/toolkit/new/LT_D7_Toolkit.pdf
25)Interneto galimybės, rizikos ir saugumas (anglų k.). Prieiga per internetą: www.eukidsonline.net
26)Video apie sekstingą (anglų k.). Prieiga per internetą: https://www.webwise.ie/category/videos/classroom-videos/
27)Šeimos planavimo ir seksualinės sveikatos asociacija (lieryvių k.). Prieiga per internetą: www.tavogyvenimas.lt
28)Karinės operacijos ir socialiniai tinklai // Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/news/daily/demaskuok/mauste-nato-karius-vos-uz-60-doleriu-eksperimenta-atlike-ekspertai-ispeja-kitu-taikiniu-busite-jus.d?id=80441665
29)Melagingos žinios Lietuvoje // Lietuvos žinios, TSPMI (lietuvių k.). Prieiga per internetą: https://www.tspmi.vu.lt/komentarai/nato-pratyboms-nauja-fake-news-doze-esa-kariai-uzmuse-vaika-n-maliukevicius/
30)Kaip atpažinti Fake news. // Lietuvos žinios (lietuvių k.). Prieiga per internetą: https://www.lzinios.lt/mokslas-ir-svietimas/kaip-atpazinti-fake-news-/261279
31)Netikros naujienos ir neapykantos kalba Facebook'e // NPR (anglų k.). Prieiga per internetą: https://www.npr.org/sections/alltechconsidered/2016/11/17/495827410/from-hate-speech-to-fake-news-the-content-crisis-facing-mark-zuckerberg
32)Kaip WhatsApp skleidžia netikras naujienas Indijoje // Wired (anglų k.). Prieiga per internetą: https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/
33)Europos kova su internetine dezinformacija// Europos Komisija (lietuvių k.). Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018DC0236&from=EN
34)Populiariausi pasaulyje socialiniai tinklai // Statista (anglų k.). Prieiga per internetą: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
35)Neapykantos kalba. Žmogaus teisių stebėjimo institutas. 2018 (lietuvių k.). Prieiga per internetą: https://hrmi.lt/wp-content/uploads/2018/10/Kovojant-su-neapykantos-nusikaltimais-ir-neapykantos-kalba-Europoje.pdf

6. Hakeriai, interneto chuliganai ir nusikaltėliai

Turbūt nėra miesto, kuriame neegzistuotų nusikalstamas pasaulis – jis kaip nepagydoma lėtinė liga įsimeta į visas visuomenes. Interneto miestas – ne išimtis. Nusikaltėliai ir chuliganai veikia grupuotėmis ar po vieną, be to, daug kas apsiginklavęs programavimo žiniomis. Tikrame pasaulyje interneto chuliganai gali atrodyti kaip tvarkingi vaikinai ir merginos, nepraleidžiantys pamokų ir visada padarantys namų darbus, ar net kostiumuoti respektabilūs profesionalai, tačiau virtualiame mieste atsiskleidžia visai kitokios jų charakterio savybės ir vertybės. Šiame skyriuje aptarsime, kaip internete tvarkomi nešvarūs reikalai, kokius metodus naudoja chuliganai ir kaip jiems pasipriešinti.

Kompiuterių virusai ir kitos kenkėjiškos programos – tai lyg virusinės ligos žmonių pasaulyje. Jų tikslas – įsilaužti į elektroninius prietaisus, sutrikdyti kompiuterių ir jų tinklų darbą,

bent iš dalies perimti kontrolę. Kai mūsų prietaisai užsikrečia, tenka gydyti, nespasekmės, kaip ir užleidus virusinę ligą, gali būti liūdnos, mat virusai linkę daugintis. Skirtingai nei mūsų gyvenamoje ekosistemoje natūraliai susiformuojantys virusai, kompiuterių pasaulyje virusus sukuria programuotojai. Kartais legalių programų kūrėjai sąmoningai palieka pravirą atsarginį įėjimą, kad patys galėtų patekti ir surinkti informaciją apie jų sukurtos programos naudojimą, bet per tą atsarginį įėjimą patenka ne tik kūrėjai – gali patekti ir piktų kėslų turintys asmenys. Jie, pabrėžiant blogas užmačias, vadinami programišiais arba hakeriais, t. y. įsilaužėliais.

Kodėl programišiai kuria virusus? Pirmieji pasaulyje kompiuterių virusai buvo sukurti kaip programuotojų profesiniai juokeliai. Paskui, programavimo žinioms sklindant ir populiarėjant, motyvai, kaip ir pati programuotojų bendruomenė, išsiplėtė. Dingstys kurti ir skleisti virusus gali būti įvairiausios: pavydas; noras sau ar kitiems programišiams įrodyti, kad gali sukurti ir paskleisti virusą; noras pakenkti ar atkeršyti nepatinkančioms įmonėms ar organizacijoms; noras užsidirbti pinigų bet kokia kaina, kad ir labai nešvariais būdais; noras išnaudoti kitų žmonių kompiuterių išgales kriptovaliutų kasybai. Į virusų kūrimą įsitraukia ir žvalgybą, kontržvalgybą, sekimą, baudžiamąjį persekiojimą vykdančios teisėsaugos, saugumo ir kitos valstybės institucijos. Kenkėjiškų programų atakos gali būti taktinės kaip karo lauke, ir tokius karus gali finansuoti ištisos viena kitai priešiškų valstybių struktūros. Dalis įsilaužėlių tai daro turėdami gerų paskatų – atskleisti visuomenės interesų pažeidimą, pinigų iššvaistymą, politikų, verslininkų nesąžiningumą. Vis dėlto pasakytina, kad daugiausia kenkėjiškų programų kuriamos siekiant užsidirbti – tai interneto miesto šešėlinis verslas. Kas tiesa, tas ne melas – karai iš realaus pasaulio keliasi į interneto miestus, o juose jūsų niekuo dėtas kompiuteris gali tapti zombių kompiuterių tinklo (angl. botne) nariu ir – jums to nė neįtariant arba nesuprantant – dalyvauti kibernetinėse atakose, vagystėse, kituose nusikaltimuose.

Galite įtarti, kad kenkėjiškos programos tarpsta kompiuteryje, jeigu jis: 1) pradeda lėčiau veikti (sulėtėja ir pats kompiuteris, ir interneto greitis), 2) dažnai „užstringa“, „persikrauna“, ekranas tampa mėlynas, 3) kompiuterio kietajame diske, kuris šiaip jau gan talpus, gerokai sumažėja vietos, 4) nors kompiuteriu nieko ypatinga neveikiama, bet intensyviai naudojamas internetas, 5) kompiuteris kaista ir, atrodo, nuolat yra „apkrautas“ – sistemos ištekliai naudojami itin intensyviai, 6) kur buvę kur nebuvę iššoka įvairiausių reklamų langai (taip gali būti, jei paspaudėte ant interneto lentelės, kuria gavote džiugų sveikinimą laimėję pinigų ar kelionę, todėl jūsų prietaise buvo suinstaliuotas virusas), 7) be leidimo pasikeičia interneto pradžios langas ir nepavyksta atkurti senojo, 8) spaudžiamos nuorodos nukelia visai ne ten, kur norėta patekti, 9) interneto naršyklėje apsigyvena keistos programėlės ir įrankiai, kurių niekada patys neparsisiuntėte. Gali atsitikti ir taip, kad kenkėjas tyliai ir nepastebimai tarpsta jūsų kompiuteryje. Vienintelis būdas jo atsikratyti – perinstaliuoti operacinę sistemą, nuolat diegti operacinės sistemos atnaujinimus ir turėti patikimą antivirusinę programą, kuri reguliariai skenuotų prietaisą ieškodama virusų ir saugumo spragų. Pastebėjus kompiuteryje veikiantį virusą, geriausia išjungti kompiuterį ir nunešti jį tiesiai į servisą, kad sutvarkytų profesionalai. Jie įvertins, ką geriausia daryti – tiesiog pašalinti virusą ar iš naujo įdiegti visą operacinę sistemą. Jums po tokios atakos derėtų pakeisti visus visose paskyrose naudojamus slaptažodžius: jei viruso tikslas buvo surinkti informaciją apie jūsų slaptažodžius, greičiausiai tai jau padaryta, todėl perinstaliavus programinė įrangą kenkėjiška programa bus pašalinta, bet programišiai, jau turėdami slaptažodžius, galės juos toliau sėkmingai naudoti. Geriausias būdas užkirsti kelią prieigai prie jūsų duomenų, interneto socialinių tinklų ir elektroninio pašto paskyrų – pakeisti visus slaptažodžius naujais.

Kenkėjiškos programos kompiuterius pasiekia internetu, kai naršoma po programišių užgrobtus puslapius, bet nebūtinai – infekuotos programos gali pasiekti, jei spaudžiate ant reklamų gan populiariuose interneto tinklalapiuose parsisiųsdami iš pirmo žvilgsnio patikimą programinę įrangą, bet ne iš oficialaus platintojo puslapio. Labai dažnai kenkėjai kompiuterius pasiekia elektroniniu paštu – taip nutinka net labai protingiems ir išsilavinusiems žmonėms, paspaudusiems

ant nuorodos, kurią esą atsiuntė draugas, pavaldinys ar verslo partneris (iš tiesų pažįstami atsiuntė, nes jų pašto dėžutės buvo užgrobtos). Taip pat virusu kompiuterį galima užkrėsti per infekuotas laikmenas (pvz., USB). Tam, kad kompiuteryje atsirastų kenkėjiška programinė įranga, dažnai reikia kokio mūsų pačių įsitraukimo: ką nors atsisiunčiame, instaliuojame, paspaudžiame, suteikiame leidimus tvarkyti sistemos operacijas ir panašiai. Todėl labai svarbu lengvabūdiškai nespausti „sutinku“, kai ekrane pasirodo lentelė, prašanti jūsų leidimų.

Kokių būna kenkėjiškų programų?

Reklaminės kenkėjiškos programos (angl. adware) – tai interneto naršyklę užkrečiančios programėlės, todėl lankantis įvairiausiuose internetiniuose puslapiuose nuolat pasirodo reklamų, siūlančių pirkti įvairiausius produktus. Dažniausiai tie produktai būna prastos kokybės, jų efektyvumas neįrodytas arba įrodytas jų neefektyvumas, bet vis tiek siekiama parduoti (pavyzdžiui, vaistai nuo grybelio, karpų, lieknėjimo tabletės ir pan.). Dalis kenkėjiškų reklaminių programų išties kelia gana daug nerimo, nes gali į kompiuterius patekti, jei asmuo patikimoje svetainėje tiesiog atsidūrė netinkamu laiku, nors ir nieko nepaspaudė. Patikimose svetainėse tokios reklamos atsiduria per tarpininkus, pvz., „Google AdWords“ programą, kurią naudoja daugelis reklamos užsakovų. Kaip apsisaugoti? Būdų visiškai apsisaugoti dar neišrasta, tačiau galima naudoti reklamos blokus (angl. adblockers) ar įdiegti „click to play“ naršyklės įskiepį, kad videoreklamos nesimatytų tol, kol to patys nenorėsime.

***Šnipinėjimo programos (angl. spyware*)** – programos, skirtos informacijai apie kompiuterio savininką ir jo veiksmus tinkle rinkti. Esama keletas tipų: 1) slaptažodžių šnipai – šios programėlės iškart arba pagal pareikalavimą siunčia visą sukauptą informaciją apie kompiuteryje naudotus slaptažodžius į išorinį serverį, kurio duomenis valdo šnipinėtojai; 2) elektroninės bankininkystės šnipai – tai programėlės, besitaikančios į bankų saugumo spragas, kad galėtų modifikuoti pervedimus ir pasisavinti lėšų; 3) programos, skirtos įvairiausiai informacijai rinkti, priklausomai nuo tokių programų iniciatorių ar užsakovų poreikių: stebėti naršyklės istoriją, pasiklausyti aplink mobilųjį telefoną vykstančius pokalbius, įrašinėti ar fotografuoti vaizdą įjungus prietaiso vaizdo kamerą ir panašiai (tokia informacija taip pat gali būti tuoj pat siunčiama išoriniam serveriui arba saugoma prietaise, kol šnipinėtojai pareikalaus gauti visą paketą; 4) klaviatūros šnipai (angl. keylogs) – programos, sekančios, kas spaudžiama klaviatūroje, ir pranešančios apie tai programų savininkams.

Virusai – tai programėlės, prisiklijuojančios prie kitos programinės įrangos, įsiterpiančios į geros programinės įrangos kodą.

Kirminai – į virusus panašios programėlės. Jų tikslas – daugintis tinkle.

Trojos arkliai arba trojanai – itin pavojingi, mat apsimeta naudinga programine įranga ar jos papildu, gali būti instaliuojami kartu su legalia ir patikima programine įranga, bet iš tiesų geruolio apvalkale slepia kenkėjišką programą – virusą, šnipą ar kt., kuris, tik patekęs į kompiuterį, pradeda veikti.

Išpirkos prašančios programėlės (angl. ransomware) – tai programėlės, kurios, patekusios į kompiuterį, per kelias sekundes užkoduoja visus kompiuteryje esančius failus ir už juos pareikalauja išpirkos. Vienintelis būdas failus atgauti – jei neturite atsarginio failų paketo (angl. backup) – sumokėti išpirką. Todėl svarbu nuolat turėti atsarginį pačių svarbiausių failų paketą, kad išpirkos reikalautojai negalėtų jūsų šantažuoti.

Jei jūsų kompiuteris nuolat striginėja, naudoja daug interneto, kaista, o jo darbo krūvis labai intensyvus – nepaisant to, kad nieko ypatinga neveikiate, – tai labai geras pagrindas įtarti, kad įdiegta kenkėjiška programinė įranga kompiuterį pavertė zombiu ir įjungė į kitų tokių pačių zombių tinklą. Ką veikia zombiai ir jų tinklai?

Dvi pagrindinės veiklos:

I. DDOS atakos – tai tinklų ir puslapių „nulaužimai“, kai serveris gauna tiek užklausų ir prašymų atidaryti tam tikrą puslapį (ne po vieną kartą, o ištisai), kad nėra pajėgus visų

užklausų aptarnauti, todėl sutrinka jo veikla. Jūsų kompiuteris gali būti vienas iš tų zombių, siunčiančių melagingas užklausas serveriui teikti jam paslaugas. Lietuvoje jau buvo įvykusi ne viena tokia ataka. Viena garsiausių – 2009 m. sausio 16 d., kai prie Seimo vyko riaušės. Apie tai pranešinėjęs „Delfi.lt“ serveris buvo „nulaužtas“ ir kurį laiką neprieinamas.

II. Kriptovaliutų kasyba. Kriptovaliutų, pvz., garsiojo bitkoino vertė yra susieta su tikra pinigine išraiška, 2019 m. pradžioje vieno bitkoino vertė buvo 3,3 tūkst. eurų. Norint pervesti vieną bitkoiną iš savo virtualios piniginės kitam žmogui, reikalinga tokį pervedimą patvirtinti. Jie patvirtinami tik tada, kai išsprendžiamos sudėtingos matematinės lygtys (todėl kriptovaliutų pervedimai vyksta gana lėtai). Tie, kurie sprendžia matematines lygtis ir teisingai išsprendžia pirmieji, už tai gauna bitkoinų. Matematinės lygtys tokios sudėtingos, kad negali būti išspręstos rankiniu būdu – tai atlieka galingi kompiuteriai. Kuo jie galingesni, tuo tikimybė, kad išspręsi lygtį pirmas, didesnė. Veikdami galingi kompiuteriai sunaudoja daug elektros ir programinių išteklių. Tad kriptovaliutos kasyba pirmiausia turi apsimokėti. Dalis kriptovaliutų kasėjų nėra sąžiningi ir bando pajungti kitų žmonių kompiuterių išteklius kriptovaliutoms kasti – jie apkrečia kenkėjiška programine įranga kompiuterius ir sujungia juos į zombių tinklą, kuris, spręsdamas matematines lygtis, uždirba kriptovaliutos programišiui.

Yra keletas populiarių būdų, kaip kenkėjiška programinė įranga pasiekia prietaisus:

1. Per nuorodas, kurias paspaudžiate gavę jas į, tarkim, savo elektroninį paštą ar susirašinėjimo programėlę (procesas dar vadinamas žvejyba , angl. phishing). Siuntėjas gali teigti, jog paspaudę nuorodą peržiūrėsite linksmą vaizdo įrašą ar perskaitysite juokingą anekdotą, tačiau tai gali būti tik priedanga. Nuorodų gali atsiųsti ir pažįstami, ir nepažįstami asmenys. Pažįstami atsiųstų tuomet, kai jų elektroninio pašto dėžutės ar paskyros socialiniuose tinkluose būna užgrobtos (paprastai tų pačių žvejų, gavusių prieigą prie elektroninio pašto dėžutės kontaktų). Dažnai užtenka vien paspausti tokią nuorodą, kad į kompiuterį būtų atsiųstas failas, jis kaipmat bus suinstaliuotas ir pradės juodą darbą. Patartina nespausti nuorodų, kai neaiškus jų gavėjas, o pažįstamo žmogaus prieš spaudžiant jo atsiųstą nuorodą vertėtų atsiklausti, ar jis siuntė nuorodą ir ką rasite puslapyje, į kurį tos nuorodos būsite nukreipti. Dar vienas metodas patikrinti, ar nėra rizikos spausti, – tai užvesti kompiuterio pelę ant nuorodos ir pasižiūrėti, koks ekrane pasirodo galutinis interneto adresas. Jei nuoroda ketina jus nuvesti į saugią, jums žinomą interneto svetainę, tuomet gana saugu tokią spausti, jei ne – geriau palikti ją ramybėje. Patikrinkite, ar jums žinomos interneto svetainės adresas parašytas tikrai teisingai, o jei ne – tai taip pat gali būti spąstai!

2. Internetinio šnipinėjimo rinkoje veikia industrija šnipinėjimo programų, kurios įsiūlomos kaip nemokama naudinga programinė įranga (pvz., kompiuterio kietojo disko valymo programėlė, alternatyvus internetinės paieškos variklis, nauja parsiunčiamų failų valdyklė). Dėl to prieš atsisiųsdami būtinai patyrinėkite išsamiau: ar nemokamas naujas įrankis yra tikrai patikimas ir kokybiškas, sužinokite, kaip apie jį atsiliepia kiti vartotojai (jei daug neigiamų atsiliepimų arba jei atsiliepimų iš viso nėra – geriau nerizikuoti ir tokios neparsisiųsti). Kartais interneto vartotojai, ieškodami, kaip atsisiųsti filmus, muziką ar knygas nemokamai, yra reikalaujami kartu instaliuoti tam tikrą grotuvą ar programinę įrangą – didelė tikimybė, jog vietoj norimo pamatyti filmo atsisiųsite kenkėją.

3. Nemokama programinė įranga gali būti įdiegta kartu su įvairiais šnipinėti skirtais priedais, kurie lieka net šią programinę įrangą ištrynus. Daug šnipų galima atsisiųsti kartu su „nulaužta“ arba piratine programine įranga.

4. Atviros interneto prieigos tinkle daugelis kompiuteriu ir telefonu siunčiamų failų, ypač jei siunčiami ne per koduotus kanalus, sklando atvirai ir yra laisvai prieinami programišiams. Kartais programišiai įsiterpia į procesą, kai kompiuteris jungiasi prie serverio, ir nusiurbia viską, ką tik

pajėgia nusiurbti. Jei kompiuteris ir mobilusis telefonas perspėja, kad „neįmanoma patvirtinti serverio tikrumo“ (angl. server cannot be verified), tuomet geriau likime be interneto arba naudokimės savo, o ne viešu interneto ryšiu.
5. Ypač lengva kenkėjiškai programinei įrangai patekti, jei prietaisuose neatnaujinama programinė įranga arba naudojama labai sena ir menkai patikima. Kiekviena programinė įranga turi spragų, tačiau tos spragos lopomos.
6. Mobiliųjų prietaisų kenkėjiška programinė įranga gali pasislėpti ypač gerai, kadangi telefonai yra mažučiai, visų vykstančių operacijų ir procesų juose galima ir nepamatyti. Telefonų šnipai atsiranda atsisiuntus užkratą turinčią programėlę (rizikuojama, jei siunčiamasi ne iš oficialių ir patikimų platintojų, pasiekia telefoną per SMS arba gali būti instaliuojama į prietaisą, jei jis nors trumpam pateko į kitas rankas).

UŽDUOTYS

1. Praktinė užduotis.
Patikrinkite, ar jūsų elektroninis paštas kada nors buvo „nulaužtas“? Užduočiai atlikti reikės kompiuterio ir interneto ryšio. Pakvieskite moksleivius atsidaryti šį puslapį https://haveibeenpwned.com/ (anglų k.) ir į paieškos langą įvesti savo elektroninio pašto adresą. Dalis moksleivių sužinos, kad jų elektroninio pašto paskyros jau ne kartą buvo „nulaužtos“, taip pat perskaitys, kokiose atakose. Kai visi patikrins savo adresus, suskirstykite moksleivius į grupes ir paprašykite sukurti 5–10 patarimų, kaip užtikrinti elektroninio pašto saugumą ateityje (pvz., nedelsiant pakeisti slaptažodį, įdiegti dvigubo atpažinimo procedūrą, nespausti ant keistų nuorodų ir pan.).
2. Darbas grupėse per pamoką arba grupinis namų darbas.
Reikės paruošti informatyvų 5 min. pristatymą apie garsiausius virusus pasaulyje ILOVEYOU, „WannaCry“, „Melissa“, STORM, „SQL Slammer“, „2007 StormWorm“, „Mebroot/Torpig“, „NotPetya“, „Cryptolocker“, „Anna Kournikova“, „Klez“, NIMDA ir kaip jie veikė. Užduočiai atlikti reikalingos anglų kalbos žinios, nes dauguma medžiagos pateikiama angliškai.
3. Diskusija „Kokie kenkėjiškų programų kūrimo tikslai?“
Tokią diskusiją geriausia organizuoti po pamokos, kai tema moksleiviams bus išaiškinta. Kas yra hakeriai arba programišiai? Ko jie siekia? Ar gali būti hakerių metodai panaudoti geriems ir kilniems tikslams? Kokiais atvejais? Šios užduoties tikslas – parodyti, kad už technologinės interneto pusės yra žmonės, turintys skirtingų tikslų ir motyvų.

ŠALTINIAI

1)Būk saugus elektroninėje erdvėje //Esaugumas (lietuvių k.). Prieiga per internetą: https://www.esaugumas.lt/
2)Kas yra hakeriai ir ko jie siekia // Malwarebytes (anglų k.). Prieiga per internetą: https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/
3)Programavimas // Mokslo sriuba (lietuvių k.). Prieiga per internetą: http://mokslosriuba.lt/kartumesgalime/laidos/
4)Huawei grėsmės// Lrytas.lt (lietuvių k.). Prieiga per internetą: https://www.youtube.com/watch?v=sqcGHHLjsIU
5)DDOS atakos // Mokslo sriuba (lietuvių k.). Prieiga per internetą: https://www.youtube.com/watch?v=r1ihPVZzVw0

6)Top 10 daugiausiai nuostolių sukėlusių virusų pasaulyje // Watchmojo (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=zqwXpQn93Po
7)Kas yra “botnet” ir kaip jis veikia // Computerphile (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=UVFmC178_Vs
8)Kaip veikia kriptovaliutų kasyklos (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=GmOzih6I1zs
9)Kaip veikia kriptovaliutų kasyklos (anglų k.). Prieiga per internetą: https://www.youtube.com/watch?v=HLYuxoytR3s

7. Duomenų apsauga Europoje ir Lietuvoje

Bandau duomenis apsaugoti ryžtingai, arba Bendrasis duomenų apsaugos reglamentas (BDAR). Realiame pasaulyje patys nusprendžiame, kam duosime savo namų raktus ir kokio stiprumo spynomis norime juos apsaugoti. Jau išsiaiškinome, kokio stiprumo spynų būna internete ir kaip gauti raktus, kuriuos turėsime tik mes patys. Šiame skyriuje aptarsime politinius pokyčius duomenų apsaugos srityje, ką naudinga jie mums, kaip vartotojams, gali atnešti.

7.1 Kas yra BDAR

2018 m. gegužės 25 d. Europos Sąjungoje (ES) buvo pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kuriam galima duoti ir kitą pavadinimą, kad šį trumpinį atsiminti būtų lengviau – „Bandau duomenis apsaugoti ryžtingai“. Šis reglamentas sugriežtino kai kurias duomenų apsaugos taisykles ES ir tapo paskata įmonėms, organizacijoms, valstybės įstaigoms ir visiems kitiems juridiniams bei fiziniams asmenims, kaupiantiems ir tvarkantiems duomenis profesiniais tikslais, į duomenų apsaugą pažvelgti rimčiau. Viena akivaizdžiausių BDAR naujovių – baudos už asmens duomenų apsaugos tvarkymo pažeidimus tapo reikšmingos.
BDAR galima įsivaizduoti kaip persikėlimą iš tėvų buto į atskirą gyvenamąją vietą. Kai anksčiau jūsų namų raktus turėdavo daugiau žmonių, dabar galite pats spręsti, ką įsileisite į namus, kuriems svečiams leisite, pavyzdžiui, apžiūrėti namų biblioteką. „Kažkas yra privatu tada, kai aš pats galiu kontroliuoti prieigą prie to „kažko“, – sako praktinės filosofijos profesorė iš Amsterdamo universiteto Beate Rössler. Kad galėtume apsaugoti savo privatumą skaitmeniniame pasaulyje, turime galėti kontroliuoti, su kuo dalijamės savo duomenimis. BDAR mums ir suteikia didesnę savo duomenų kontrolę internete ir už jo ribų.

BDAR galima suprasti ir kaip europinės demokratijos augimą – su BDAR ES gyventojams buvo suteikta daugiau teisių privatumo srityje. Akstinas atsirasti BDAR kilo iš to, kad duomenų apsaugos reguliavimas ES buvo pasenęs. Senoji duomenų apsaugos direktyva, kurią pakeitė BDAR, priimta 1995 m., kai internetu naudojosi tik procentas viso pasaulio gyventojų! Dažnai pasitaiko, kad imantis harmonizuoti, t. y. sulyginti vienus standartus su kitais pačioje ES ar sulyginti ES ir kitų šalių standartus, yra pasirenkamas prastesnis standartas, kurio savo klientams siekė verslo lobistai. BDAR yra išimtis! Šiuo atveju pasirinktas aukštesnis standartas, daugiausia grįstas Vokietijos modeliu. Svarbu pridurti, kad išaugusios teisės į duomenų apsaugą, kaip ir kitos žmogaus teisės, galioja tiek, kiek sugebame jomis pasinaudoti. Tikimės, kad šis skyrius padės tas teises geriau suprasti.

7.2 Kokias teises įtvirtina BDAR

BDAR aprėpia asmens duomenų tvarkymą visur, kur jie gali būti reikalingi, įskaitant ligonines, mokyklas, valstybės institucijas – ir fiziniame, ir skaitmeniniame pasaulyje, tačiau šiame skyriuje koncentruosimės į BDAR ir internetą. Kas yra asmens duomenys? Tai asmens vardas, pavardė, asmens kodas, adresas, telefono numeris, elektroninio pašto adresas, IP adresas, t. y. bet kokia informacija, kuria galima asmenį identifikuoti. Ypatingi ir jautrūs duomenys, tokie kaip pirštų antspaudai, genetiniai duomenys, religiniai, politiniai, filosofiniai ar kiti įsitikinimai, seksualinė orientacija, narystė profesinėse sąjungose, taip pat duomenys, susiję su asmens teistumu ir sveikata, yra priskiriami specialių kategorijų asmens duomenimis. Jiems tvarkyti taikomos dar griežtesnės taisyklės. Duomenų tvarkymu vadinami visi veiksmai, atliekami su mūsų duomenimis, – duomenų užrašymas, grupavimas, ištrynimas ir t. t.

Būtų netikslu teigti, jog BDAR suteikia visiškai naujas, iki tol ES neregėtas teises. Teisė į informaciją, teisė susipažinti su savo duomenimis, reikalauti juos ištrinti, pakeisti, apriboti ar sustabdyti jų tvarkymą, nesutikti su jų tvarkymu – visos šios teisės jau anksčiau buvo įtvirtintos Europos Sąjungos Duomenų apsaugos direktyvoje bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme. Su BDAR ES piliečiai gavo naują teisę – teisę į duomenų perkeliamumą. Aptarkime šias teises.

2018 m. gegužės 25 d. daugelį elektroninio pašto dėžučių užplūdo laiškai, kuriais įvairios įmonės ir organizacijos pranešė, kaip tvarko mūsų duomenis, ir klausė, ar norime, kad jos ir toliau duomenis tvarkytų. Taip sužinojome, kas dar žino mūsų internetinį adresą, turi duomenų apie hobius, pomėgius, kas seka, ką skaitome (pavyzdžiui, naujienlaiškį siunčiančios organizacijos panorėjusios dažniausiai gali sužinoti, ar atsidarėme jų siųstą naujienlaiškį ir kiek laiko praleidome jį skaitydami) ir pan., ir galėjome nuspręsti, ar norime, kad šie duomenys ir toliau būtų pasiekiami, kaupiami, analizuojami, ar vis dėlto norime, jog jų nebetvarkytų. Šiuo atveju svarbiausia yra teisė nesutikti, kad duomenys būtų tvarkomi. Tiesa, teise nesutikti, kad duomenys būtų tvarkomi, pasinaudoti galime tik tada, kai rinkti ir tvarkyti duomenis nėra būtina, pavyzdžiui, apsaugoti mūsų gyvybei, išmokėti darbo užmokesčiui ar pan. Kai be duomenų tvarkymo nebūtų įmanoma suteikti paslaugos, pavyzdžiui, mokyti moksleivio mokykloje, sutikimo tvarkyti duomenis nereikia, bet žmonės, kurių duomenys tvarkomi, turi būti supažindinti su duomenų tvarkymo politika.

Pagal naująjį reglamentą visos Europos Sąjungoje veikiančios įmonės, įskaitant ir įmones, įsikūrusias trečiosiose šalyse, bet teikiančias paslaugas ES esantiems asmenims, turi ne tik deklaruoti, kokius duomenis renka, bet ir suprantamai pateikti šią informaciją. Taip siekiama užtikrinti teisę į informaciją. Įmonė ar bet koks kitas duomenų valdytojas privalo aiškiai ir suprantamai pateikti informaciją, kokiais tikslais prašoma tvarkyti duomenis (arba kokiais tikslais jie tvarkomi), kiek ilgai jie bus tvarkomi, su kokiomis įmonėmis ar organizacijomis planuojama dalytis tais duomenimis, suteikti informacijos apie visas su duomenų apsauga susijusias teises. Tam tikrais atvejais duomenis tvarkantieji taip pat privalo pranešti, jei duomenys buvo nutekinti ar atsirado kitų duomenų apsaugos pažeidimų. Duomenų valdytojas taip pat privalo sudaryti galimybę duotą sutikimą be jokių kliūčių atšaukti. Prancūzijos duomenų apsaugos priežiūros institucija neseniai skyrė „Google“ bendrovei 50 mln. eurų baudą už netinkamą sutikimo prašymo formą įvairiose jai priklausančiose platformose, tokiose kaip „Youtube“ ir „Google Maps“. „Google“, nors ir atnaujino duomenų rinkimo politiką po BDAR įsigaliojimo, vis tiek buvo nubausta, – Prancūzijos duomenų apsaugos reguliuotojas mano, kad „Google“ duomenų rinkimo politiką per sunku rasti, ji nepateikta taip aiškiai, kaip turėtų būti.

„Mes žinome, kur tu esi. Mes žinome, kur tu buvai. Mes daugiau ar mažiau tiksliai galime pasakyti, ką tu šiuo metu galvoji“, – tai ne kokio nors diktatoriaus ar saugumo tarnybos, o „Google“ bendrovės direktorių tarybos pirmininko žodžiai. Ką „Google“ žino apie mus naudodamiesi teise susipažinti su duomenimis, sužinoti galime nuėję į savo „Google“ paskyrą ir atsisiuntę savo

duomenų kopiją. Jei norime daugiau informacijos apie tai, kaip tvarkomi mūsų duomenys, galime, pavyzdžiui, parašyti „Google“ laišką ir paprašyti suteikti informacijos, kokius duomenis bendrovė turi apie mus ir kaip juos tvarko. Remdamasis BDAR, kiekvienas ES pilietis turi teisę paprašyti bet kurio jo duomenis renkančio subjekto, taip pat ir tokių įmonių kaip „Google“ ar „Facebook“, suteikti jam galimybę peržiūrėti, kokie duomenys apie jį yra surinkti.

Jei manome, kad viena ar kita bendrovė apie turi daugiau duomenų nei norėtume, galime paprašyti, kad tvarkomų duomenų mastas būtų pakeistas (pavyzdžiui, sutinkame, kad bendrovė turėtų mūsų vardą ir pavardę, bet nusprendėme, kad jai nebūtina kaupti mūsų judėjimo trajektorijos duomenų) arba mūsų duomenų tvarkymo būtų apskritai atsisakyta. Jei manome, kad kokia nors įmonė arba institucija turi neteisingus duomenis apie mus, turime teisę reikalauti ištaisyti duomenis. Su šia teise glaudžiai susijusi ir teisė laikinai sustabdyti duomenų tvarkymą. Ja pasinaudoti galime, pavyzdžiui, jei duomenys yra netikslūs, neišsamūs, neteisingi ir laukiame, kol jie bus ištaisyti.

Naujasis ES duomenų reglamentas suteikia teisę reikalauti ištrinti duomenis (teisė būti pamirštam). Kitaip tariant, BDAR suteikia teisę reikalauti, kad duomenų tvarkytojai grąžintų viską, ką išsinešė iš jūsų namų – dienoraščius, senelės nuotraukas ar dar ką nors, kas jums svarbu ir ką norite pasilikti tik sau. Pavyzdžiui, jei paieškų variklyje ieškote savo pavardės ir tarp paieškos rezultatų pastebite paauglystės vakarėlių fotografijas, turite teisę paieškų variklio administratoriaus paprašyti ištrinti nuorodą į šias fotografijas. Pagal BDAR, vartotojui paprašius duomenys turi būti ištrinti visiems laikams. Deja, nepaisant galiojančių teisės aktų, net ir ištrynus „Facebook“ profilį, informacija apie vartotoją vis dar lieka įmonės serveriuose. Tačiau reikia pastebėti, kad teisė būti pamirštam nėra absoliuti ir gali būti atsisakyta duomenis ištrinti, jeigu, pavyzdžiui, juos ištrynus būtų suvaržyta žiniasklaidos ar saviraiškos laisvė arba jei duomenys reikalingi moksliniam tyrimui atlikti. BDAR atsiradusia teise į duomenų perkeliamumą galima pasinaudoti, pavyzdžiui, paprašius savo elektroninio pašto tiekėjo tiesiogiai perduoti asmens duomenis kitam elektroninio pašto tiekėjui. Tačiau dažniausiai taikomas būdas pasinaudoti teise į duomenų perkeliamumą, kai duomenys perduodami jų savininkui ir jis pats perduoda duomenis kitam paslaugos tiekėjui.

BDAR paskatino daug teigiamų pokyčių duomenų apsaugos srityje: dėl BDAR kai kurie interneto tinklalapių administratoriai stengiasi lankytojus sekti mažiau, rinkti mažiau jų duomenų ir statistikai apie lankytojus rinkti ieško alternatyvų, kurios į lankytojų privatumo sferą skverbiasi mažiau nei duomenų rinkimo įrankis „Google Analytics“, pavyzdžiui, nesaugo duomenų, pagal kuriuos galima identifikuoti žmogų.

Duomenų apsaugos užtikrinimo projektuojant (angl. Data protection by design) reikalavimu, įtvirtintu 25-uoju BDAR straipsniu, teigiama, kad apie privatumo apsaugą autoriai galvotų kurdami naują technologiją ar produktą, o ne susimąstytų vėliau, kai paslauga jau sukurta. Šis principas dar vadinamas pritaikytąja privatumo apsauga. Su juo susijęs BDAR taip pat įtvirtintas „duomenų kiekio mažinimo principas“: turi būti renkama, saugoma ir tvarkoma kuo mažiau duomenų. Jei duomenys nereikalingi paslaugai teikti, turi būti nustota juos rinkti. O saugojimo trukmės apribojimo principas nustato, kad suteikus kokią nors paslaugą klientų duomenys, kai jų nebereikia, turi būti ištrinti. Pagal dar vieną principą – numatytąsias privatumo nuostatas (angl. privacy by default) – numatyta, kad ir be specialių informacinių technologijų žinių vartotojui turėtų būti įmanoma apsaugoti savo privatumą. Praktiškai tai reikštų, kad, pavyzdžiui, prisijungiate prie socialinio tinklo ir automatiškai nustatyta privatumo apsauga yra ta, kuri garantuoja didžiausią privatumo lygį toje platformoje. Trys „I“ – informacinis teisingumas, informacinė lygybė bei informacinė autonomija – privačių įmonių bei valstybės institucijų turėtų būti suvokiamos kaip būtinybė privatumui apsaugoti.

7.3 Didieji interneto koncernai ir BDAR

Kol neįsigaliojo BDAR, nebuvo aišku, kieno įstatymais – JAV ar ES – turi remtis JAV interneto milžinės, tokios kaip „Google“ ar „Amazon“, kai teikia paslaugas ES piliečiams. Pagal BDAR, netgi įmonės, esančios už ES ribų, turi taikyti BDAR, jeigu teikia paslaugas ES piliečiams. Interneto versle dabar dominuoja keturi didieji koncernai iš JAV: „Apple“, „Google“, „Facebook“ ir „Amazon“. Nors jų paslaugos tarptautinės, jie mato save, kaip amerikietiškas bendroves. Taip yra iš dalies todėl, kad vartotojų ir duomenų apsaugos teisės JAV yra silpnesnės nei ES. JAV asmens duomenų apsauga kiekvienoje valstijoje reguliuojama vis kitaip, ten nėra bendro „asmens duomenų“ apibrėžimo.

Šių bendrovių dominavimas lemia tai, kad įgyvendinti griežtesnes europines vartotojų ir duomenų apsaugos teises labai sunku. Pavyzdžiui, remiantis BDAR, daugelyje ES šalių asmeniui iki 16 metų (Lietuvoje – asmeniui iki 14 metų), norinčiam naudotis socialiniais tinklais, reikia tėvų ar kitų teisėtų atstovų, pavyzdžiui, globėjų ar institucijos, kuri rūpinasi nepilnamečiu, administracijos sutikimo. Tėvų sutikimo priemonės turi būti veiksmingos, pavyzdžiui, patvirtinimas atsiunčiamas į vieno iš tėvų elektroninio pašto dėžutę. Šio reikalavimo didžiosioms JAV bendrovėms priklausantys socialiniai tinklai Europos Sąjungoje nesilaiko. Galima numanyti, kad tai vyksta iš dalies dėl dominavimo rinkoje, iš dalies dėl tokių paprastų priežasčių, kai tėvai neturi savo elektroninio pašto arba vaikas žino jų elektroninio pašto slaptažodį ir pats duoda „tėvų sutikimą“.

7.4 BDAR – daugiau atskaitomybės ir atsakomybės

Priėmus BDAR buvo sustiprinta visų duomenų rinkėjų atskaitomybė už asmeninių duomenų rinkimą, kitaip tariant, duomenų tvarkytojai turi ne tik saugiai tvarkyti duomenis ir nustatytais tikslais, bet ir būti pasiruošę prireikus įrodyti, kad taip elgiasi, pavyzdžiui, pateikdami tai patvirtinančius dokumentus.

Viena priežasčių pastaruoju metu viešojoje erdvėje daug kalbėti apie BDAR – išaugusi finansinė atsakomybė už pažeidimus. Anksčiau Lietuvos teisės aktuose nustatytos baudos už neteisėtą duomenų tvarkymą ar kitus asmens duomenų teisių pažeidimus buvo nuo 150 iki 3000 eurų1, o dabar įmonės gali būti nubaustos baudomis iki 20 mln. eurų arba 4 proc. nuo apyvartos siekiančia bauda, priklausomai nuo to, kuri suma didesnė. Lietuvoje valstybės institucijoms galioja išimtis – jos negali būti baudžiamos daugiau nei 60 tūkst. eurų bauda. Kita Lietuvos asmens duomenų apsaugos įstatymu taikoma išimtis – draudimas potencialiems darbdaviams rinkti duomenis apie kandidatą į darbo vietą iš to kandidato buvusio darbdavio, nesant kandidato sutikimo.

Lietuvoje duomenų apsaugos pažeidimus nagrinėja Valstybinė duomenų apsaugos inspekcija. Kai duomenų tvarkytojas yra žiniasklaidos priemonė, už asmens duomenų teisių pažeidimų nagrinėjimą atsakinga yra Lietuvos žurnalistų etikos inspektoriaus tarnyba. Dėl turtinės ar neturtinės žalos atlyginimo reikėtų kreiptis į teismą.

1. [1]https://www.e- tar.lt/portal/lt/legalAct /4ebe66c0262311e5bf 92d6af3f6a2e8b/fRh VcDlxRa

UŽDUOTYS

Kadangi vaikai ir paaugliai ima pavyzdį iš suaugusiųjų, vertėtų su administracija peržiūrėti, ar mokymo įstaiga jau prisitaikė prie BDAR reikalavimų, ir tik tada moksleiviams skirti užduotis.
Užduotys tinkamos atlikti per pilietinio ugdymo, teisės, geografijos bei kitas pamokas.

I. Darbas grupėmis „Padėk socialiniam tinklui įgyvendinti BDAR“

1 Pamokos pradžioje paprašykite moksleivių sau susirašyti ant popieriaus lapo, kokie verslo subjektai internete jau turi duomenų apie juos. Paklauskite, koks skaičius įmonių renka duomenis apie juos? Tai daug ar mažai? Paklauskite, ar moksleiviai žino, kokius duomenis įmonės renka, ar kada nors tikrino savo socialinių tinklų paskyrų privatumo nustatymus.
2. Paaiškinkite, kas yra BDAR ir kokias teises šis reglamentas suteikia, taip pat apie privatumo užtikrinimo projektuojant principą.
3. Suskirstykite moksleivius į grupes po 4–6. Kiekviena grupė turėtų parengti pasiūlymų, kaip „Facebook“ galėtų pagerinti vartotojų duomenų apsaugą, remiantis BDAR 25 straipsnyje įtvirtintu privatumo užtikrinimo projektuojant principu. Tegu moksleiviai pirmiausia peržiūri „Facebook“ duomenų politikos puslapį: https://lt-lt.facebook.com/policy.php. Pakvieskite kiekvieną grupę aprašyti (pavyzdžiui, ant didelių popieriaus lapų), ką teigiama ir ką neigiama pastebi „Facebook“ duomenų politikos apraše, ypač atkreipdami dėmesį į informacijos suprantamumą ir tinklalapio dizainą. Paprašykite grupių parengti pasiūlymų, kaip paslaugų teikėjo, tokio kaip „Facebook“, duomenų politikos skyrius galėtų būti pagerintas. Idėjų moksleiviai gali ieškoti peržiūrėdami kitų paslaugų teikėjų duomenų politikos aprašus internete. Prieš pamoką pasirūpinkite spalvotomis rašymo priemonėmis, kad moksleiviai savo pasiūlymus galėtų išreikšti kūrybiškai. Tam jie gali naudoti ir elektronines priemones.
4. Pamokos pabaigoje kiekvieną grupę pakvieskite pristati savo pasiūlymus visai klasei.

II. Darbas grupėmis „Informacijos užklausa apie duomenų apsaugą“

1. Pamokos pradžia – taip pat kaip ir I užduoties 1 punktas.
2. Suskirstykite moksleivius į grupes po 4–6. Paaiškinkite, kad valdžios institucijos privalo teikti informaciją savo piliečiams jiems rūpimais klausimais. Tegul kiekviena grupė nusprendžia, kokia duomenų apsaugos tema jiems įdomiausia, ir paieško informacijos šia tema internete. Tada grupė turėtų nuspręsti, į kokį klausimą pasirinkta tema jie norėtų gauti atsakymą ir kokiai institucijai, atsižvelgus į jos kompetenciją, sugalvotą klausimą tinka adresuoti. Paskui grupėje suformuluotas klausimas turėtų būti išsiųstas pasirinktai institucijai ar institucijos darbuotojui. Duomenų apsaugos politika Lietuvoje rūpinasi šios institucijos:
a) Valstybinė duomenų apsaugos inspekcija;
b) Lietuvos žurnalistų etikos inspektoriaus tarnyba. Tarnybai klausimą galima siųsti elektroniniu paštu arba per šią formą: http://zeit.lt/lt/klausiate-atsakome/177;
c) Lietuvos Respublikos Teisingumo ministerija.
Moksleiviai taip pat gali pasirinkti klausimą užduoti Seimo nariui, Europos Parlamento nariui ar kitam politikui.
3. Atsakymų gali tekti palaukti. Kai visos grupės jau turės jiems rūpimus atsakymus, tegul kiekviena grupė pristato gautus atsakymus. Juos aptarkite kartu su klase: ar valdžios institucijų atsakymai išsamūs, ar suprantamai atsako į užduotą klausimą, ką nauja klasė sužinojo apie duomenų apsaugą.

III. Namuose parašyti referatą.
Moksleiviai gali paruošti pristatymą klasei ir / arba parašyti referatą viena iš pasirinktų temų:
Duomenų apsaugos istorija Lietuvoje
Kokios institucijos Lietuvoje atsakingos už duomenų apsaugą?
Kodėl svarbu saugoti savo duomenis ir kaip tam padeda BDAR?
„Teisė būti pamirštam“ Marijaus Kostėjos Gonzaleso (Mario Costejos Gonzálezo) bylos prieš „Google“ kontekste.

IV. Užklasinė veikla
Pasikvieskite į mokyklą duomenų apsaugos pareigūną (specialisto ieškoti galima, pavyzdžiui, per Lietuvos duomenų apsaugos pareigūnų asociaciją http://ldapa.lt). Tegul jis papasakoja apie savo darbą, nušviečia duomenų apsaugos politikos aktualijas ir atsako į moksleivių klausimus. Klausimų pareigūnui moksleiviai gali pasiruošti iš anksto (pavyzdžiui, kaip namų darbų užduotį).

ŠALTINIAI

1)2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Oficialus tekstas (anglų k.). Prieiga per internetą: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=LT
2)BDAR (lietuvių k.). Prieiga per internetą: http://www.privacy-regulation.eu/lt/
3)Europos Sąjungos oficialusis leidinys (lietuvių kalba). Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
4)Tyrimai, kuriais siekta įvertinti Lietuvos vartotojų ir verslo nuostatas apie duomenų apsaugą // HRMI (lietuvių k.). Prieiga per internetą: http://hrmi.lt/duomenu-apsaugos-reforma/
5)Asmens duomenų teisinės apsaugos įstatymas Lietuvoje. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalActEditions/TAR.5368B592234C?faces-redirect=true
6)Katrin Eggert (BvD e. V.), Ralf Heimburger (Mitglied im AK Schule, BvD e. V.), Rudi Kramer (Sprecher der Initiative „Datenschutz geht zur Schule“, BvD e. V.), Riko Pieper (stellv. Sprecher der Initiative „Datenschutz geht zur Schule, BvD e. V.), Frank Spaeing (stellv. Sprecher der Initiative „Datenschutz geht zur Schule, BvD e. V.) [Hrsg (atsakingi redaktoriai)]. Datenschutz geht zur Schule: Sensibler Umgang mit persönlichen Daten. Arbeitsblätter. [Duomenų apsauga ateina į mokyklą. Apgalvotas elgesys su asmeniniais duomenimis. Užduočių ruošiniai]. 2018 m. lapkritis. Prieiga internete: https://www.klicksafe.de/service/materialien/broschueren-ratgeber/datenschutz-geht-zur-schule/#s|Datenschutz%20geht%20zur%20Schule
7)Bitiukova, Natalija; Liutkevičius, Karolis. Privatumo paradoksas: Lietuvos gyventojų nuostatos apie duomenų apsaugą. Žmogaus teisių stebėjimo institutas, 2016.
8)Pliauškienė, Rita. Asmens duomenų apsauga Europos Sąjungoje: Lietuvos atvejo analizė. Baigiamasis magistro projektas. Prieiga per internetą: https://core.ac.uk/download/pdf/80047778.pdf
9)BDAR veikia: per Europą ritasi pirmoji baudų banga // Verslo žinios (lietuvių k.). Prieiga per internetą: https://www.vz.lt/paslaugos/2019/01/14/bdar-veikia-per-europa-ritasi-pirmoji-baudu-banga#ixzz5hifrF9Wf
10)Pokyčiai, kuriuos atneš Europos Sąjungos asmens duomenų apsaugos reforma // Manoteisės (lietuvių k.). Prieiga per internetą: http://manoteises.lt/straipsnis/pokyciai-kuriuos-atnes-europos-sajungos-asmens-duomenu-apsaugos-reforma/

11)BDAR taikymas nepilnamečiams // Telšių žinios (lietuvių k.). Prieiga per internetą: http://tzinios.lt/asmens-duomenu-teisines-apsaugos-istatymas-kartais-virsta-betonine-siena-kartais-atviromis-durimis/
12)Ar gali Google apie mus pamiršti? // Manoteisės (lietuvių k.). Prieiga per internetą: http://manoteises.lt/straipsnis/tavo-teise-buti-pamirstam-vs-google/
13)Duomenų apsauga ir privatumas internete // ES puslapis (lietuvių k.). Prieiga per internetą: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_lt.htm
14)Žmogaus teisės asmens duomenų apsaugos srityje // Žurnalistų etikos inspektoriaus tarnyba (lietuvių k.). Prieiga per internetą: http://zeit.lt/lt/naujienos/zmogaus-teises-asmens-duomenu-apsaugos-srityje/338
15)Jūsų teisės asmens duomenų apsaugos srityje, kai jūsų asmens duomenys naudojami profesiniais tikslais // Žurnalistų etikos inspektoriaus tarnyba (lietuvių k.). Prieiga per internetą: http://zeit.lt/data/public/uploads/2017/12/intikui.pdf
16)Piliečiams skirtos duomenų apsaugos ES gairės. Prieiga per internetą: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_lt.pdf
17)Lietuvos gyventojų tyrimas apie asmens duomenų apsaugą // Valstybinės duomenų apsaugos inspekcija (lietuvių k.). Prieiga per internetą: https://www.ada.lt/go.php/lit/Lietuvos-gyventoju-tyrimas-apie-asmens-duomenu-apsauga---zinanciuju-apie-asmens-duomenu-apsauga-skaicius-padvigubejo
18)Google seka kiekvieną vartotojų žingsnį – ES vis daugėja skundų // Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/mokslas/technologijos/google-seka-kiekviena-vartotoju-zingsnies-vis-daugeja-skundu.d?id=79709741
19)Įsigaliojo nauja Asmens duomenų teisinės apsaugos įstatymo redakcija // Verslo žinios (lietuvių k.). Prieiga per internetą: https://www.vz.lt/verslo-aplinka/2018/07/16/isigaliojo-nauja-asmens-duomenu-teisines-apsaugos-istatymo-redakcija#ixzz5hilDpaEK
20)Duomenų apsauga // Klicksafe (vokiečių k.). Prieiga per internetą: https://www.klicksafe.de/themen/datenschutz/datenschutz-grundverordnung/
21)Duomenys ir privatumas. Prieiga per internetą: http://www.zmogausteisiugidas.lt/lt/temos/duomenys-ir-privatumas
22)Giedrė Tubelytė. Duomenų apsaugos reformos vežimas įsilinguoja – kas papuolė po jo ratais? // Delfi (lietuvių k.). Prieiga per internetą: https://www.delfi.lt/verslas/nuomones/giedre-tubelyte-duomenu-apsaugos-reformos-vezimas-isilinguoja-kas-papuole-po-jo-ratais.d?id=80105511#cxrecs_s
23)Duomenų apsauga // Youngdata (vokiečių k.). Prieiga per internetą: https://www.youngdata.de/datenschutz/cro-und-co/
24)Kaip apsaugoti savo duomenis naršant ar apsiperkant internete // LRT (lietuvių k.). Prieiga per internetą: https://www.lrt.lt/naujienos/mokslas-ir-it/1/219938/kaip-apsaugoti-savo-duomenis-narsant-ar-apsiperkant-internete
25)Bendrasis duomenų apsaugos reglamentas: ką būtina atlikti ir žinoti // Verslo žinios (lietuvių k.). Prieiga per internetą: https://www.vz.lt/informacines-technologijos-telekomunikacijos/2017/09/11/bendrasis-duomenu-apsaugos-reglamentas-ka-butina-atlikti-ir-zinoti
26)Asmens duomenų apsaugos naujovės nuo 2018-05-25 // Elektroninė darbuotojų saugos ir sveikatos valdymo sistema (lietuvių k.). Prieiga per internetą: http://www.sdg.lt/puslapis/asmens-duomenu-apsaugos-naujoves-nuo-2018-05-25
27)Po „Facebook“ skandalo EP nariai siūlo stiprinti asmens duomenų apsaugą // Kauno diena (lietuvių k.). Prieiga per internetą: http://kauno.diena.lt/naujienos/verslas/ekonomika/po-facebook-skandalo-ep-nariai-siulo-stiprinti-asmens-duomenu-apsauga-885929

28)Privatumas internete. Prieiga per internetą: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/online-privacy/index_lt.htm
29)Asmens duomenų apsauga: 11 dažniausių klaidų // Verslo žinios (lietuvių k.). Prieiga per internetą: https://www.vz.lt/verslo-aplinka/2017/06/26/asmens-duomenu-apsauga-11-dazniausiu-klaidu
30)Google gavo 50 mln. Eur baudą už BDAR pažeidimus // Verslo žinios (lietuvių k.). Prieiga per internetą: https://www.vz.lt/technologijos-mokslas/2019/01/22/google-gavo-50-mln-eur-bauda-uz-bdar-pazeidimus
31)Dažniausiai sutikimo net nereikia: darbdavys gali stebėti jūsų buvimo vietą, laiškus, jus patį // 15min (lietuvių k.). Prieiga per internetą: https://www.15min.lt/verslas/naujiena/bendroves/dazniausiai-sutikimo-net-nereikia-darbdavys-gali-matyti-jusu-buvimo-vieta-laiskus-jus-pati-663-1094452
32)Paaiškinantis video. Prieiga per internetą: https://multimedia.europarl.europa.eu/lt/the-eu-general-data-protection-regulation-gdpr_B01-ESN-180515_ev
33)AR LIETUVOS VERSLUI IR VARTOTOJAMS RŪPI ASMENS DUOMENŲ APSAUGA? // HRMI (lietuvių k.). Prieiga per internetą: http://hrmi.lt/duomenu-apsaugos-reforma/
34)Valstybinė duomenų apsaugos inspekcija. Prieiga per internetą: www.ada.lt https://www.ada.lt/go.php/lit/img

Apie autorius

Laura Gintalaitė yra žiniasklaidos bendradarbė, straipsnių autorė, kampanijų organizatorė, demokratijos ir aplinkosaugos aktyvistė, buvusi žurnalistė, dabar gyvenanti Berlyne, Vokietijoje. Laura Vilniaus universitete įgijo žurnalistikos bakalaurą, Linkopingo universitete, Švedijoje, įgijo technologijų ir socialinių pokyčių magistrą. Su didžiaisiais duomenimis Laura dirbo „Greenpeace International“ žiniasklaidos monitoringo ir analizės komandoje Amsterdame. Duomenų apsaugos temomis Laura susidomėjo atsikrausčiusi į Vokietiją – šalį, turinčią ilgas, istoriškai lemtas duomenų apsaugos tradicijas, kur egzistuoja stiprus supratimas apie duomenų apsaugos svarbą ir ne kiekvienas naudoja feisbuką ar instagramą.

Akvilė Venckutė – Lietuvos žurnalistikos centro komunikacijos koordinatorė, Vilniaus universiteto žurnalistikos studijų bakalaurantė. Domisi žiniasklaida, technologijomis, medijų transformacija. Pagal mainų programą semestrą studijavusi Informacijos mokslus Berlyno Humboldt universitete daugiau dėmesio pradėjo skirti ir skaitmeninio raštingumo temoms.

Ignas Krasauskas – dešimties metų patirtį turintis politikos žurnalistas, pastaraisiais metais domėjęsis, kaip užtikrinti, kad tiek kasdienis naudojimasis internetu, tiek profesionalus bendravimas ir informacijos rinkimas būtų saugūs ir privatūs.

Džina Donauskaitė – Lietuvos žurnalistikos centro vadovė, žiniasklaidos tyrėja ir žurnalistikos bei medijų lektorė. Susidomėjo ir pradėjo išsamiau tyrinėti skaitmeninio raštingumo temas dėstydama apie medijas ir kritinį mąstymą Vilniaus ir Vytauto Didžiojo universitetuose bei suaugusiesiems ir vaikams per įvairius neformalius užsiėmimus Lietuvoje ir užsienyje. Klausytojai kaskart apie interneto pasaulį turėjo vis daugiau įdomių klausimų, mokytojų auditorijos vis prašydavo pasidalyti medžiaga dėstyti, todėl Džina inicijavo šios metodologinės priemonės edukatoriams parengimą.