Tallinna Ülikool

Digitehnoloogiate instituut

Digitaalse jalajälje vähendamine vabavara abil

Bakalaureusetöö

Autor: Risto Ruuben

Juhendaja: Edmund Laugasson

Autor: ..... „ ..... „ 2016

Juhendaja:..... „ ..... „ 2016

Instituudi direktor:..... „ ..... „ 2016

Tallinn 2016

Autorideklaratsioon

Deklareerin, et käesolev bakalaureusetöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Risto Ruuben (sünnikuupäev: 15.05.1994)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Digitaalse jalajälje vähendamine vabavara abil“ mille juhendaja on Edmund Laugasson, säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

(digitaalne) allkiri ja kuupäev

Sisukord

Sissejuhatus 6

1. Mis on digitaalne jalajälg 7

2. Mis on vabavara 8

3. Mis infot ja kuidas on kasutaja kohta võimalik saada 9

   3.1. Veebilehitseja küpsised 9

   3.2. Flash küpsised 10

   3.3. Otsingumootorid 10

   3.4. Seadme sõrmejälg 11

   3.5. Asukoha jälgimine 12

4. Digitaalse jalajälje vähendamine võimalused erinevate vabavarade abil 14

   4.1. VPN (Virtual Private Network) 14

   4.2. Veebilehitseja ajaloo kustutamine 15

   4.3. Andmete krüpteerimine 16

   4.4. Tor (The Onion Router) 17

   4.5. Veebilehitseja lisandid 18

      4.5.1. HTTPS Everywhere 18

      4.5.2. AdBlock Plus 18

      4.5.3. Disconnect 19

      4.5.4. NoScript ja ScriptSafe 19

      4.5.5. Privacy Badger 20

   4.6. Turvalise operatsioonisüsteemi valik 21

5. Uuring 23

5.1. Metoodika ja eesmärk 23
5.2. Analüüs 24
5.3. Järeldused 44
Kokkuvõte 45
Summary 47
Kasutatud kirjandus 49
Lisad 53
Lisa1 53

Sissejuhatus

Iga päev, sõltumata oma tahtest lisame me digitaalsesse maailma infot iseenda kohta.. See info, mida digitaalses maailmas tekitame, aitab firmadel sihtida kindlaid turge ja kasutajaid, aitab teisel vaadelda kasutaja ajalugu ning reklaamifirmadel jälgida kasutaja tegevust mitmete erinevate veebilehtede vahel. Iga tegevus digitaalses keskkonnas võib jätta maha digitaalse jalajälje.

Seega on tähtis teada, millist informatsiooni me jätame maha oma tegevustega digitaalses maailmas ning mis selle tagajärjed olla võivad. Kuigi tänapäeval on pea võimatu mitte jätta maha mingisugust digitaalset jalajälge on siiski võimalik seda vähendada erinevate meetmete sealhulgas ka vabavara abil**.**

Antud töös tutvustab autor digitaalset jalajälge lähemalt ning toob välja millist infot see kasutaja kohta sisaldada võib. Samuti räägib autor millised on digitaalse jalajälje tagajärjed ning kuidas saab selle eest ennast kaitsta vabavaralisi lahendeid kasutades.

Antud teema eesmärk on tutvustada kasutajatele erinevaid vabavaralisi vahendeid ning sellega seonduvalt käitumisharjumuste muutmist, mille abil oleks digitaalset jalajälge võimalik vähendada.

Eesmärgi saavutamiseks uurib autor, kuidas digitaalne jalajälg tekib, millist informatsiooni digitaalsest jalajäljest saab ja millised vabavaralised lahendused aitavad digitaalset jalajälge vähendada ning viib läbi uuringu, milles uuritakse inimeste teadmisi digitaalse jalajälje osas. Uuringu põhjal üritatakse leida vastused järgmistele uurimisküsimustele:

- Millised vabavaralised vahendid tagavad väikesema digitaalse jalajälje?
- Millised kasutusharjumuste muutmised tagavad võimalikult väikese digitaalse jalajälje saamiseks antud vabavaraliste vahenditega?
- Kuidas motiveerida kasutajaid vähendama digitaalset jalajälge?
- Millised on kasutajate teadmised digitaalsest jalajäljest ning kas on kasutulele võetud meetmeid selle vähendamiseks?
- Kas ollakse nõus kasutama vähemtuntumaid ning vabavaralisi lahendusi digitaalse jalajälje vähendamiseks?

1. Mis on digitaalne jalajälg

Digitaalne jalajälg on kogum andmeid mis eksisteerib tänu kasutaja tegevustele digitaalses maalimas, mida on võimalik seostada kindla kasutajaga. Digitaalse jalajälje saab jagada kaheks grupiks aktiivne ning passiivne info. (Wigmore, 2014)

Aktiivne jalajälg on andmed mida kasutaja on meelega maha jätnud. Selleks võib olla sotsiaalmeedias nagu näiteks Facebookis või Twitteris postitamine. Veel jätavad kasutajad aktiivse jälje maha järgmiste tegevustega: ajabeebi postitused, piltide ja videofailide üleslaadimine, elektronposti saatmine, telefoni kõned ning jututoad. (What is a Digital Footprint, 2007)

Passiivne jalajälg on samas andmekogum, mille on kasutaja maha jätnud mitteteadlikult läbi oma tegevuste. Nendeks võib olla veebilehtede külastamine, otsingud veebis läbi otsingumootorite, digitaalsed ostud internetipoodides. (Wigmore, 2014)

Digitaalne jalajälg on praktiliselt permanentne ja kui info on avalik või isegi poolavalik nagu näiteks sotsiaalmeedia postitused, pole kasutajal suurt kontrolli selle üle, kuidas seda teised kasutada võivad. (What is a Digital Footprint, 2007)

2. Mis on vabavara

Vabavara on tarkvara, mille lähtekood on kõigile kättesaadav ja muudetav, jagatav, õpitav ning jooksutatav. Lähtekood on programmeerijate poolt kirjutatud koodiread. Lähtekood ise tuleb arvutile sobivasse kujusse tõlgendada ehk kompileerida. Kompileeritud kood on inimesele praktiliselt loetamatul kujul ning seda pole võimalik muuta. (The Open Source Definition, 2007)

Kombineeritud kujul on tavaliselt kõik tarkavara, mis jõuab kasutajani, seda nii omandvara kui ka vabavara puhul. Omandvara on tarkvara mis on saadaval raha eest kui ka tasuta, kuid mõlemal juhul on omanduslik. Vabavara puhul on kasutajal võimalik koodi analüüsida, teha muudatusi koodi ja see ise ära kompileerida oma muudatustega. Seega kipub vabavara arendus tihti kasutama avalikku arvamust ja soovitusi oma arenduses ning tihti panustavad mitmed suured grupid tarkvara arendusse. (What is Free Software?, 2016)

Levinud tarkvaralitsentsid, mille all vabavara väljastatakse, on MIT, Apache litsents, GNU GPL, GNU LGPL ja BSD.(Licenses, 2016)

3. Mis infot ja kuidas on kasutaja kohta võimalik saada

3.1. Veebilehitseja küpsised

Veebilehitseja küpsised, inglise keeles *cookies* on üks levinuimaid viise kuidas saada infot kasutaja kohta. Külastades mitmeid veebilehti salvestatakse kasutajaga seotud andmed väikeste failidena. Seega veebilehitseja küpsised on andmeosad, mida salvestatakse kasutaja digitaalsesse seadmisse külastava veebiserveri poolt. (What is a cookie?, kuupäev puudub)

Veebilehitseja küpsised võivad sisaldada kasutaja poolt tehtud eelnevaid eeldusi ning valikuid. Kui kasutaja läheb tagasi eelnevalt külastatud veebilehele, saadetakse serverile küpsises peituv info, mida on võimalik kasutada veebilehe kohandamiseks, et kasutajale tekkiks tuttav vaatepilt. Kuigi küpsiste kasutamine võib kasutaja elu mugavamaks teha, on veebilehitseja küpsiseid võimalik ära kasutada, ning jälgida milliseid veebilehti on kasutaja külastanud. (What is a cookie?, kuupäev puudub)

Veebilehitseja küpsised saab jagada kahte rubriiki, milleks on esimese osapoole küpsised ning kolmanda osapoole küpsised. Kui esimest kasutatakse kasutajale erinevate pakkumiste tegemiseks ning veebilehe kasutajale mugavamaks muutmiseks, siis kolmanda osapoole küpsised jagavad kasutaja andmeid teistele osapooltele nagu näiteks reklaamifirmad. (How does third-party ad serving work?, kuupäev puudub)

Sama veebilehitseja liigi alla kuuluvad ka jälitusküpsised, mis jälgivad kasutaja veebilehtede ajalugu, mida üldjuhul kasutatakse kasutajale huvipakkuvate reklaamide edastamiseks. (How does third-party ad serving work?, kuupäev puudub)

Veebilehitseja küpsiseid on tavaliselt võimalik blokeerida erinevate kõrvaliste rakenduste abil ning mõned veebilehitsejad pakuvad sarnaseid võimalusi.

Üks võimalikest programmidest on Disconnect, mis blokeerib tuntud kolmandatel osapooltel veebi aktiivsuse jälgimise. (Disconnect, 15.01.2015)

Küpsistest loobumiseks saab kasutaja loobuda info jagamisest Network Advertising Initiative liikmetega. Selleks tuleb minna Network Advertising Initiative kodulehele ning avaldada soovi loobuda info jagamiseks. (Networkadvertising, kuupäev puudub)

3.2. Flash küpsised

Mõni hulk veebilehti kasutavad sellist küpsise tüüpi milleks on Flash küpsised, inglisekeeles *flash cookies*. Flash küpsised on palju vastupidavamad kui tavalised küpsised, kuna tavalised meetodid nende eemaldamiseks ei tööta, ning seega on nendest raskem vabaneda, kuna isiklike andmete, ajaloo ning vahemälu tühjendamine ei suuda Flash küpsiseid digitaalsest seadmest eemaldada. Lisaks teeb nendest vabanemise palju keerulisemaks see, et neid ei saa üldjuhul kustutada ühegi kättesaadava viirustõrje programmiga. (Use of Cookies on About Cookies Website, kuupäev puudub)

Siiski on olemas mõni vahend Flash küpsiste eemaldamiseks, millest tuntumad on Motzilla Firefox veebilehitseja laiend nimega BetterPrivacy ning Adobe lehel pakutav rakendus, mis aitavad kaasa Flash küpsiste kustutamisele. (About this Add-on, 27.04.2016)

3.3. Otsingumootorid

Otsingumootorid on üks levinuimaid viise, kuidas kasutaja digitaalselt jalajälge moodustada saab. Tänapäeva populaarseim meetod infootsinguks internetis on kasutada otsingumootoreid. Otsingumootorid võivad salvestada kasutaja IP aadressi, kasutatud otsingusõnu ning seega annavad hea ülevaate kasutaja huvidest ning aitavad saada kasutaja kohta tohutul hulgal informatsiooni. (Prabhu, 2015)

Mõned otsingumootoritega tegelevad firmad on väitnud, et säilitavad nende kasutajate informatsiooni parema teenuse saavutamiseks ning säilitavad kasutaja andmeid üle aasta, mis on palju pikem ajaühik kui tegelikult vajalik. Seda arvesse võttes tasub kasutajal olla otsingumootorite valikul väga ettevaatlik oma digitaalse jalajälje vähendamiseks. (Prabhu, 2015)

On olemas ka otsingumootoreid nagu DuckDuckGo, mis väidab, et ei salvesta ega jaga isikliku informatsiooni ja ei kasuta küpsiseid ning IP aadressi, et kasutajat tuvastada. Seega ei tohiks DuckDuckGo otsingumootoril olla piisavalt informatsiooni, et välja selgitada, kas samast arvutist tulnud otsingud on omavahel kuidagi seotud. (Hoffman, 2012)

Lisaks on olemas Startpage otsingumootor, mille privaatsuse eeskirjad olid loodud vastulöögiks firmade poolt informatsiooni pahatahtliku kasutamise vastu. Tuldi järeldusele, et kui kasutajate informatsiooni ei salvestata, pole võimalust privaatsuse rikkumiseks ning heade otsingutulemuse saamiseks kasutab Startpage Google otsingumootorit, kuid enne Googlele tulemuste saatmist eemaldab kõik tuvastava informatsiooni kasutaja päringutest. Ixquick on veel üks otsingumootor, mis töötab samal põhimõttel nagu Startpage, aga erinevuseks on see, et otsingu tulemused ei ole ainult Google'lt saadud. (Hoffman, 2012)

Juhul, kui siiski otsingumootorit kasutada ei soovi, on mõistlik kasutada digitaalselt jalajälgi vähendavaid meetodeid, mis blokeerivad võimalikult palju otsinguks mittevajaliku infot. Parim lahendus oleks kasutada VPN teenuseid ning veebilehitseja lisandeid, nagu näiteks Disconnect veebilehitseja lisand. (Disconnect, 15.01.2015)

3.4. Seadme sõrmejälg

Seadme sõrmejälg on info, mis on kogutud seadmest endast, ning töötab printsiibil, et iga seade erineb kuidagi teistest. Näiteks võib seadetel olla erinev tarkvara, kellaaeg, fondid, erinev kiibi kood, seadme nimi ning igasugu erinevaid omadusi, mis teeb kasutaja seadme jalajälje unikaalseks. Kui kasutaja ühenduse loob, edastab kasutaja seade andmed, mida on võimalik koguda ning liita. Selle tulemusel saame unikaalse sõrmejälje seadmele, millele saadakse määrata kindel number selle tuvastamiseks. (About Device Fingerprint/Deviceprint, kuupäev puudub)

Seadme sõrmejälje loomine on populaarsust kogunud ja on küpsiseid kiiresti asendamas. Asutused eelistavad seadme sõrmejälje loomist küpsistele tänu selle blokeerimise raskuse tõttu võrreldes küpsistega. Küpsised on kaitsetud kustutamise ning aegumise vastu ja muutuvad kasutuks, kui kasutaja otsustab uut veebilehitsejat kasutada. Mõned veebilehitsejad blokeerivad kolmanda osapoole küpsiseid vaikimisi, ning veebilehitseja laiendused on leidnud lahendusi, mis võimaldavad nende kustutamist ning blokeerimist. (How to protect against device fingerprinting, 2014)

Erinevalt küpsistest, ei jäta seadme sõrmejälg kasutaja seadmetesse jälge ning seetõttu on raske teada, millal ja mis tegevusi hetkel jälgitakse. Seadme jalajälje vastu on olemas mõned võimalused, nagu näiteks oma unikaalsuse kontrollimine. Üks koht kus kasutaja saab oma unikaalsust kontrollida on Panopticlick, mis annab kasutajale ülevaate mis infot saadakse, võimaldades kasutajatel näha, kui kergesti on kasutajad äratuntavad veebis. (Is your browser safe against tracking?, kuupäev puudub)

Sõrmejälje loomised on peaaegu nähtamatud ning peaaegu püsivad. Pole lihtsat meetodit, kuidas neid kustutada. Kasutajad, kes on kindlameelsed sõrmejälje vältimise osas, võivad kasutada Tor-i või keelata Javascripti ja Flashi käivitumist oma arvutis, kuid see võib muuta mõned lehed kasutuskõlblikuks, jättes tähtsaid elemente laadimata. (How to protect against device fingerprinting, 2014)

3.5. Asukoha jälgimine

Veebileht või rakendus võib määrata kasutaja seadme füüsilise ligikaudse asukoha, kasutades selleks erinevaid meetmeid. Näiteks on üldjuhul, kuid mitte alati võimalik IP-aadressi põhjal leida ligikaudne asukoht. Seega on võimalik IP-aadressi põhjal leida kasutaja ligikaudne paiknemise koht. (Lookup IP Address Location, kuupäev puudub)

Selleks, et varjata oma IP-aadressi, on olemas erinevaid meetmeid. Üks lihtsamaid lahendusi oleks kasutada veebilehitsemisel Tor veebilehitsejat, mis peidab kasutaja IP-aadressi ära ning sellega takistatakse võimalus kasutaja asukoha leidmiseks. Teine võimalus on kasutada Virtuaalset privaatset võrgustiku ehk VPN teenust, mis asendab kasutaja IP-aadressi mõne enda omaga ning eelnevalt Tor-ist peidab kogu kasutaja internetiliikluse ära. (Tor: Overview, OpenVPN Community Software, kuupäev puudub)

Kasutaja asukoha infot võidakse kasutada kasulikul otstarbel, näiteks näidata kasutaja telefonis ilmaennustust lähtuvalt kasutaja asukohast. Samas on see suur privaatsuse risk, kui kasutaja asukohainfot hoopis andmebaasi kogutakse ja teiste allikatega liidetakse. Selle põhjal on võimalik välja selgitada kasutaja liikumisharjumused, ehk kus ollakse suure osa ajast või mis marsruuti kasutakse igapäevasteks sõitudeks. Seega on antud info põhjal on võimalik ennustada kasutaja hetkest ja tulevast asukohta isegi siis, kui teda hetkel jälgida pole võimalik. (Location tracking, kuupäev puudub)

4. Digitaalse jalajälje vähendamine võimalused erinevate vabavarade abil

4.1. VPN (Virtual Private Network)

Internetis liikudes kasutatakse tavaliselt krüpteerimata ühendust ning tänu sellele on liikuvad andmed inimkeeles loetaval kujul kättesaadavad. Kuna tavaliselt kasutaja andmed liiguvad läbi mitmete erinevate seadmete ning võrkude, on võimalik, et andmeid võidakse teel sihtkohta pealt kuulata. Pealt kuulatud infot on võimalik kasutaja vastu ära kasutada, et teada saada kasutaja sisselogimis andmeid või muud isikliku infot. Lisaks aitab VPN pääseda mööda riiklikest piirangutest info varjamiseks ning selle abil on võimalik vältida valitsuse nuhkimist. Üks meetod, kuidas infot kätte saada on läbi sniffer rakenduste, mis on võimelised analüüsima võrgust läbituid andmeid. Ohu vältimiseks on mõistlik kasutada VPN-i ehk Virtual Private Network. (Why you should use a VPN, kuupäev puudub)

VPN on süsteem mitmetest privaatsetest võrkudest, mis on üksteistega ühendatud üle avaliku võrgu. Ühenduse loomisel toimub tavaliselt autentimine ning andmete turvaliseks ülekandeks kasutatakse krüpteerinut ühendatud võrkude vahel. See tähendab, et kui kasutaja ei pea muretsema, et keegi tema andmeid pealt kuulab, kuna pealt kuulatud andmetega pole midagi peale hakata kuna neid pole ilma võtmeta võimalik lugeda. Seega ei sõltu kasutaja andmete edastamise protokollidest ning võib kasutada erinevaid krüpteerimata võrke. (How Virtual Private Networks Work, 2008)

VPN teenuste kasutamiseks on kasutajal võimalik kasutada mõnda VPN teenusepakkuja programmi. VPN teenuse pakkuja osas tuleks veenduda, et teenus on usaldusväärne, kuna on olnud juhtumeid, kus VPN teenuse pakkujad on oma klientide tegevused üles andnud, seega tasub arvestada, et kõik VPN teenusepakkujad ei pruugi olla usaldusväärsed. (How nsa proof are VPN providers?, 2013)

Üks tuntud lahendus on OpenVPN, mis on tasuta ning avatud kõigile. Selle kasutamiseks on vaja installida nende rakendus vaides endale lähima regiooni ning mis parim on see, et selle kasutamine ei vaja kasutaja registreerimist. Lisaks pakuvad nad tugevat krüpteerimist kasutades AES-256 ja AES-128 standardeid. Veel on seda lihtne üles seada ning nende enda kodulehel on olemas ka lihtne õpetus selle tööle saamiseks. (Introduction, 2016)

4.2. Veebilehitseja ajaloo kustutamine

Juhul kui kasutaja arvutisse on salvestatud veebilehitsemise ajalugu on võimalik ette võtta meetmeid nende eemaldamiseks. Suur osa leevenenumaid veebilehitejad sisaldavad võimalust kustutada veebilehitsemise ajalugu. Antud meetudi miinuseks on see, et kustutus toimub ainult antud veebilehitsejas ning kui kasutajal on kasutuses mitut erinevat veebilehitsjat tuleb seda kõikides erinevates veebilehitsejates manuaalselt eraldi teha. (Browser Hygiene: The Importance of Clearing Cache and Cookies, kuupäev puudub)

Selle probleemi lahendamiseks on olemas erinevaid vabavaralisi lahendusi, mis aitavad protsessi lihtsamaks ja kiiremaks teha. Üks selline vabavaraline tarkvara on BleachBit. Eelnimetatud tarkvara suudab kustutada vahemälu ehk inglise keeles cache, küpsiseid, veebisirvimis ajalugu, ajutisi faile, erinevaid logisid populaatsemates veebilehitsejates nagu Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Opera, Apple Safari. Tarkvara on loodud nii Microsoft Windows süsteemile ja erinevatele Linux versioonidele ning antud failide kustutamine aitab kasutajal lisaks andmekandjale ruumi juurde saada. (Clean Your System and Free Disk Space, kuupäev puudub).

4.3. Andmete krüpteerimine

Andmete krüpteerimine aitab kaitsta kasutaja andmeid võõraste eest. Näiteks krüpteerimata andmed on kaotatud või varastatud seadete kettalt lihtsasti kätte saadavad, ning kuna seadmed sisaldavad väga palju isikliku informatsiooni kasutaja kohta, on mõistlik piirata võimaliku kahju nagu näiteks identiteedi vargusest ja raha kaotusest kuni avaliku maine rikkumiseni. (Data Encryption in Transit Guideline, kuupäev puudub)

Krüpteeritud andmetele on võimalik ligi pääseda ainult kindla võtme kasutusega ehk andmete dekrüpteerimine loetavale kujule on võimalik ainult võtme omamisega. Võtit tuleb samamoodi valvata nagu füüsilist võtit ning jälgida, et keegi sellest koopiat ei tee ning samuti ei tohi võtit ära kaotada. Võtme kaotamisel võib tekkida olukord, kus kasutaja ise ei pääse enam ligi enda andmetele. Seega tasub olla väga ettevaatlik võtme säilitamisega. Lisaks tasub teadlik olla et krüpteerimise ning dekrüpteerimise võti võivad, aga ei pea olema erinevad. Võtmed ise on tavaliselt pikad ning sisaldavad suvalisi bitijadasid, mida inimesed pole võimelised meelde jätma, ning seega on tavaliselt olemas ka lühem võti, mida on lihtsam meelde jätta. (Rouse, 11.2014)

GNU Privacy Guard on tasuta ning avalik rakendus Windows, Linux ja OS X platvormile, mis suudab krüpteerida kirju, tavalisi faile ja failide kaustu ning vajadusel ka terve ketta. GNU Privacy Guard toetab lisaks mitmeid erinevaid krüpteerimisstandardeid ning tüüpe. Lisaks kuna tegu avaliku lahendusega on seda võimalik kasutada mitmete erinevate tööriistadega ja programmidega, ning kasutajal on võimalik vaadata ka rakenduse koodi, et kindlaks teha rakenduse turvalisus, ning vajaliku oskuse puhul pakkuda ka erinevaid lahendusi kuidas tarkvara paremaks muuta. (Hansen, 2015)

Veracrypt on nagu GNU Privacy Guard avalik rakendus Windows, Linux ja OS X platvormil ja oma avalikuse tõttu peetakse üldjuhul usaldusväärseks tarkvaraks ning suudab krüpteerida kaustu ja terveid andmekandjaid. Krüpteerimiseks kasutatakse sümmeetrilist krüptograafiat. (Idrassi, 2014)

4.4. Tor (The Onion Router)

Tor ehk „The Onion Router" on vabavaraline programm, mis aitab vähendada digitaalset jalajälge. Selle eesmärgi saavutamiseks Tor anonümiseerib kasutaja ning teisejärguliselt krüpteerib andmeid. See tähendab seda, et kolmandatel osapooltel ei ole võimalik saada kasutajat tuvastavat informatsiooni nagu näiteks asukoht. Kasutaja anonümiseerimiseks suunab Tor andmeliikluse läbi ülemaailmsete releede, mida eksisteerib tuhandete kandis. (Tor: Overview, kuupäev puudub)

Programm töötati algselt välja USA ühendriikide mereväele, kus selle pealmiseks eesmärgiks oli kaitsta valitsuse vahelist andmeliiklust, kuid tänaseks on see kasutusele võetud ka tavakasutaja poolt, kelleks võivad olla kontoritöötajad, ajakirjanikud jne. (Inception, kuupäev puudub)

Tor-i peamine kasvamise põhjus on tsensuur ja inimeste jälgimine, mis hetkel maailmas aina kasvab. Tänu Tor-ile on võimalik tsentsuurist ja massjälgimisest eemalduda ning saada ligipääs infole, mida varem polnud võimalik saada. Tori kasutavat kasutajat on tuvastada väga keeruline või peaaegu võimatu. (Tor: Overview, kuupäev puudub)

Siiski ei ole olemas lõplikult turvalist lahendust ning ka Tori kasutusel tuleb arvestada süsteemi nõrkustega. Esimesena, mida võib kasutaja koheselt märgata on see, et Tor-i kasutamine aeglustab kasutaja internetis surfamise kiirust, kuna turvalisuse tagamiseks peab andmeliiklus läbima rohkem etappe kui tavaliselt. (Why is Tor so slow?, kuupäev puudub)

Teisena tuleb arvestada sellega, et inimene ise võib oma digitaalset jalajälge maha jätta avaldades erinevatele teenustele Tor-i kasutamise ajal reaalset informatsiooni, mis kaotab suuresti Tor-i kasutusele võtmise mõtte. (Tor: Overview, kuupäev puudub)

4.5. Veebilehitseja lisandid

Kuigi üldjuhul peetakse reegliks, et väiksema hulga veebilehitseja lisandite kasutamine tagab kasutajale väiksena digitaalse jalajälje, on sellel reeglil erandid. Mõned veebilehitseja lisandid aitavad digitaalset jalajälge vähendada. Antud teemas käsitletakse veebilehitseja lisandeid, mis teostavad rohkem lihtsamat filtreerimist pakkudes kaitset küpsiste, jälitajate(trakers), kolmanda osapoole skriptide ning muude tahtmatute lisandite vastu. Valitud said veebilehitseja lisandid, mis on olemas võimalikult paljudel enimkasutatud veebilehitsejatel. (Watching Them Watching Me: Browser Extensions'Impact on User Privacy Awareness and Concern, 2016)

4.5.1. HTTPS Everywhere

HTTPS Everywhere on populaarne veebilehitseja lisand, mis olemas Google Chrome ja Mozilla Firefox, Operal. Veebilehitseja lisand on avatud kõigile ning on kättesaadav tasuta. Lisandi ülesanne on krüpteerida ühendus mitmetel erinevatel veebilehtedel kus on selleks võimalus, ning on loodud koostöös The Tor Projecti ja Electronic Frontier Foundationiga. Turvaline ühendus tagatakse sellega, et hüperteksti edastusprotokolli ehk HTTP ühenduse asemel kasutatakse turvalist hüperteksti edastusprotokolli ehk HTTPS ühendust. Erinevalt HTTP ühenusest on HTTPS ühendus suhtlevate seadete poolt krüpteeritud. (Ads Take a Step Towards "HTTPS Everywhere", 2015)

4.5.2. AdBlock Plus

AdBlock Plus on populaarne veebilehitseja lisand, mida üldjuhul kasutatakse lehekülje sisusse ettejäävate reklaamide eemaldamiseks. Lisaks on teada, et selle kasutamine võib teha veebilehtede laadimise kiiremaks, kuna osa lehe sisust enam ei laeta alla. (About Adblock Plus, kuupäev puudub)

Samas võib selle lisandi kasutamine mõnel juhul veebilehe „katki teha", näiteks ei pruugi veebilehe sisu olla korrektselt vormitud või võib mõne lehele tähtsa elemendi töötamist takistada. (Not all issues are Adblock Plus bugs, kuupäev puudub)

Siiski suudab AdBlock Plus veebilehitseja lisand teha ka muud, nimelt vähendada kasutaja digitaalset jalajälge lülitades välja jälgimise(traking), kuid see seade tuleb kasutajal endal sisse lülitada. (About Adblock Plus, kuupäev puudub)

4.5.3. Disconnect

Disconnect on veebilehitseja lisand Google Chrome ja Mozilla Firefox, Opera ja Apple Safari veebilehitsejas, mille eesmärk on aidata kasutajal hoida kontrolli oma personaalse info üle, blokeerides peamiselt jälitamis(traking) taotlusi. Olgu mainitud, et antud lahendusel on olemas ka tasuline versioon, kuid antud eesmärgi saavutamiseks töötab tasuta versioon ning seega pole tasulise lahenduse kasutamine vajalik. Lisaks on programmi kood kõigile avalik. (Disconnect, kuupäev puudub)

Peale jälitamistaotluste blokeerimise suudab lisand blokeerida osadel veebilehtedel reklaame. Disconnect annab infot külastatud lehtede kohta, nagu näiteks kokkuvõtte reklaamide ja sisu päringute kohta samal ajal, kui need laevad veebilehele. (Disconnect, kuupäev puudub)

Iga kategooria kohta on võimalik saada täpsemat infot. Näiteks, millised firmad neid päringud tegid ning millised on nende sidemed antud veebilehtedega. Lisaks näitab lisand, kui palju kiiremini leht laadis, ning kui palju andmemahtu kasutaja kokku hoidis kasutades lisandit. (Disconnect, kuupäev puudub)

Veel on võimalik kasutajal lisand peatada kindlatel lehtedel kui selleks peaks vajadus tekkima. Lühidalt öeldes Disconnect eraldab kasutaja kõikidest teistest domeenidest peale vaadatava veebilehe enda. (Disconnect, kuupäev puudub)

4.5.4. NoScript ja ScriptSafe

NoScript on Mozilla Firefox veebilehitseja lisand ning ScriptSafe Google Chrome veebilehitseja lisand. Kuigi tegu on erinevate veebilehiteja lisanditega täidavad mõlemad lisandid samasugust eesmärki, milleks on peatada kõik skriptid veebilehtedel töötamast. Kaasa arvatud Java, JavaScript, Flash ning teised, mis on võimelised jooksutama pahatahtliku koodi veebilehe taustal. (Noscript, kuupäev puudub, Scriptno, 2011)

Tegu on väga agressiivsete veebilehiteja lisanditega, ning tänu sellele on lisandid tuntud sellepoolest, et nad lõhuvad paljud veebilehed ära ehk võivad takistada veebilehe korrapärast kujundust ning halvemal juhul veebilehe funktsionaalsust. (Noscript faq, kuupäev puudub)

Lahendus sellele on manuaalne skriptide sisse lülitamine, kuid see võib olla väga ajamahukas ning tavakasutaja ei pruugi teada, milliseid skripte on ohutu sisse lülitada nii, et veebileht ka korralikult töötaks. Tegu on ühekordse protsessiga ning seega, kui kasutaja külastatud lehtede arv on piiratud, on tegu hea lahendusega digitaalse jalajälje vähendamiseks. (Noscript faq, kuupäev puudub)

4.5.5. Privacy Badger

Privacy Badger on populaarne veebilehitseja lisand, mida on võimalik kasutada Google Chrome ja Mozilla Firefox veebilehitsejas. Lisand mis jälgib kolmandate osapoolte tegevust, samal ajal kui kasutaja külastab erinevaid veebilehti ning blokeerib nende jälitusküpsised. (Privacy Badger FAQ, kuupäev puudub)

Lisand selle asemel, et blokeerida mõned kindad leheküljed, küpsised ning muud aktiivsused, jälgib kolmandate osapoolte ebasoovitavat käitumist ning vastavalt sellele koostab oma blokeerimisnimekirja. Tänu sellele omadusele on tegu väga ressursikerge veebilehitseja lisandiga, kuid selle tagajärjel on kasutaja digitaalne jalajälg alguses vähem kaitstud kui mõnel teisel rakendusel oleks. (Privacy Badger FAQ, kuupäev puudub)

Lisandit on kerge kasutada ning igal lehel, mida kasutaja külastab annad lisand kasutajale teada, millised domeenid kasutajat antud veebilehel jälgivad ning annab kasutajale võimaluse blokeerida domeenilt pärinevad küpsised või täielikult domeen blokeerida. (Privacy Badger FAQ, kuupäev puudub)

4.6. Turvalise operatsioonisüsteemi valik

Tavaliselt enamik kasutajad kasutavad seadme ostes sellele installitud populaarset operatsioonisüsteemi kuna installitud operatsioonisüsteem on tuttav ning seega lihtne kasutada. Seega on enamik populaarsed operatsioonisüsteemid kasutaja andmete saamiseks suured sihtmärgid pahavarale ja muudele infokogumis meetoditele ohvrid. (Qubes OS, kuupäev puudub)

Trails on üks vabavaralistest operatsioonisüsteemidest, mis aitab kasutajal säilitada privaatsust ja anonüümsust jättes maha kasutajast jälje ainult siis kui kasutaja seda ise soovib. Operatsioonisüsteem on disainitud olema paindlik ning kaasaskantav mälupulga, mälukaardi ja plaadi peal iseseisvalt ilma olemasoleva operatsioonisüsteemi kasutamiseta. See tähendab, et kasutaja saab operatsioonisüsteemi alati endaga kaasa võtta ja mujal seda kasutada ning operatsioonisüsteem on seadistatud mitte kasutama seadmes olevaid andmekandjaid peale andmekandja millele operatsioonisüsteem ise on installitud. Ainuke koht kus andmeid peale Trailsi enda andmekandja on süsteemi mälus, mis kustutab endast andmed automaatselt kui arvuti on välja lülitatud. Seega kasutaja ei jäta endast maha ühtegi jälge peale operatsioonisüsteemi kasutamist ning andmeid pole võimalik taastada, kuna neid pole kuskil mujal hoitud kui Trailsi enda installitud andmekandjal, mida kasutaja saab alati endaga kaasas kanda. (Tails, kuupäev puudub)

Operatsioonisüsteem sisaldab ka võimalust krüpteerida andmekandjat kasutades Linux Unified Key Setup ehk LUKS-i ning automaatselt kasutab HTTPS ühendust seal kus võimalik, kasutades selleks HTTS Everywhere veebilehitseja lisandit. Veel on OpenPGP standardit kasutades krüpteeritud Trails elektronposti tarkvara ja dokumendid. . (Tails, kuupäev puudub)

Trails tuleb algselt kaasa eelseadistatud tarkvaraga, mis on sätestatud eelkõige turvalisust silmas pidades. Näiteks on kõik pealelatud tarkvara seadistatud kasutama Tor võrku ning juhul, kui tarkvara üritab ühendust saada ilma Tor võrguta siis tarkvara ühendus on automaatselt blokeeritud. Lisaks on võimlik kasutada ka teisi anonüümseid võrke. (Tails, kuupäev puudub)

Peale Trails-i on olemas veel erinevaid turvalisusele keskenduvaid operatsioonisüsteeme nagu näiteks OpenBSD ja Qubes OS. Qubes OS on vabavaraline operatsioonisüsteem, mis pakub kasutajale turvalisust läbi isolatsiooni ja ajutiste keskkondade läbi virtualiseerimise. Näiteks saab kasutada ühet virtuaalmasinat selleks, et külastada mitte usaldusväärset veebilehte ja teist virtuaalmasinat, et tegeleda pangandusega ilma, et kasutaja peaks muretsema, mida mitte usaldusväärne süsteemiga teha võib. See tähendab, et kui üks kindel osa süsteemist langeb rünnaku alla siis teised osad jäävad puutumata. (Qubes OS, kuupäev puudub)

5. Uuring

5.1. Metoodika ja eesmärk

Käesoleva uuringu eesmärgiks on leida vastused järgnevatele punktidele:

- Saada ülevaade kui teadlikud ollakse privaatsusest internetis.
- Kas ja mida on ette võetud digitaalse jalajälje vähendamiseks?
- Kas üldse ollakse nõus muutma käitumisharjumusi digitaalse jalajälje vähendamiseks?
- Kas usaldatakse vähemtuntumaid ning vabavaralisi lahendusi digitaalse jalajälje vähendamiseks omandvara asemel?

Küsimustikus küsib autor rohkem üldisemaid teadmisi digitaalsest jalajäljest ning üldisi lahendusi kuidas seda vähendada, kuna valitud grupil ei pruugi olla olulisi teadmiseid töös kirjutatud vabavaralistest lahendustest.

Uuringu läbiviimiseks koostas autor küsimustiku milles osales 66 vastajat. Vastamine oli anonüümne. Küsitlus koosnes 20-st küsimusest, millest enamus olid valikvastustega ning mitmikvastustega küsimused, kuhu vastaja sai pakkuda lahendusi mida autor originaalselt ei pakkunud. Ülejäänud küsimused olid avatud vastusega või maatriksküsimused. Küsitlus koostati Google Forms tarkvara abil, mis sai valitud oma avatuse ning mugavuse tõttu. Küsimustiku levitamiseks kasutati peamiselt mugavusvalimit. Küsimustiku näidis on saadaval lisa 1.

5.2. Analüüs

Küsitluses osales erineva vanusega vastajaid. Enamuses olid 17-26 aastased. Kes moodustasid vastavalt 36,36 % küsitlusele vastanud meestest ja 31,82% küsitlusele vastanud naistest. Teine populaarsem vastajate hulk oli vanusegrupis 27-39. Vastavalt 6,06% küsitlusele vastanud meestest ja 7,58% vastanud naistest. Vanuste seas 40 kuni 59 vastavalt 3,03% küsitlusele vastanud meestest ja 7,58% vastanud naistest. Kõige vähem vastajaid oli alla 16 aastaste grupis Vastavalt 1,52% küsitlusele vastanud meestest ja 6,06% vastanud naistest. Seega olid vastanutest 46,97% mehed ja 53,03% naised. Küsitluses oli veel valikus ka üle 60 aastased aga kuna antud küsitluses sellises vanusegrupis vastajaid polnud sai antud grupp eemaldatud all olevas diagrammis.

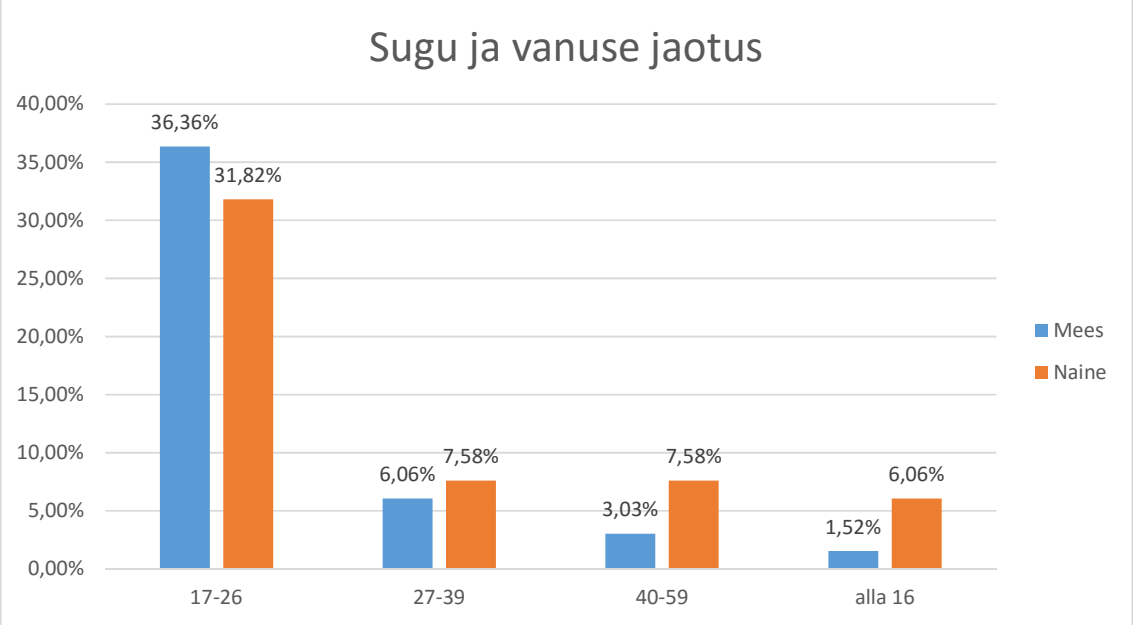

Diagramm 1. Sugu ja vanuse jaotus

Küsimuse „Asutus kus õppis või töötad“ vastajatest olid 69,70% töötamas või õppimas haridusasutustes. 16,67% vastanutest olid erafirmas ning 6,06% ei õpi ega tööta küsitluse vastamise ajal kusagil. Asutust, kus õpitakse või töötatakse ei soovinud avaldada 7,58% vastanutest.

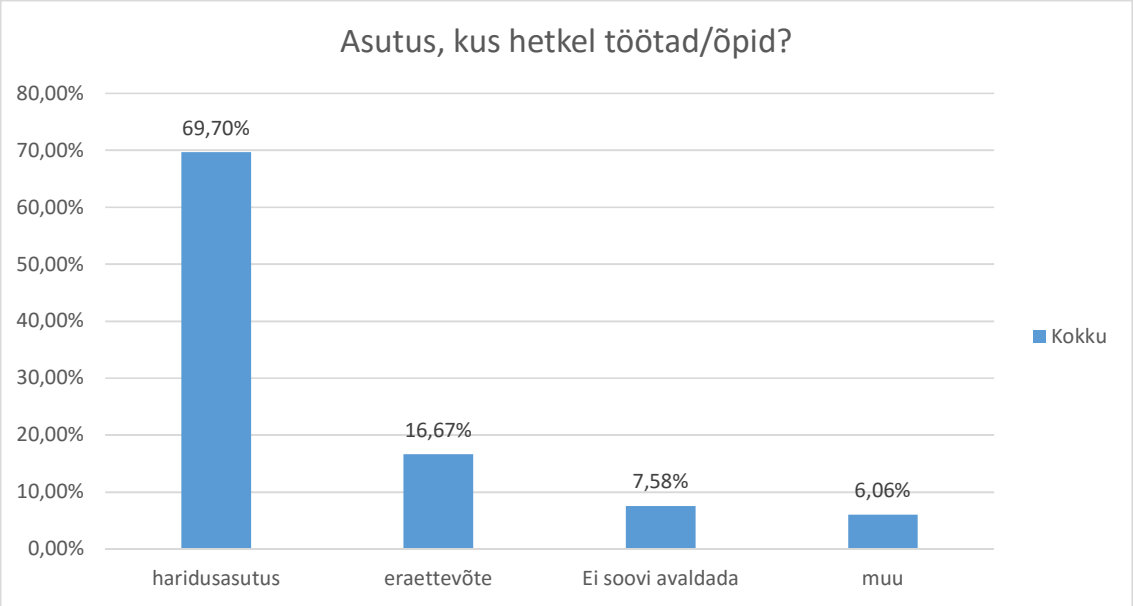

Diagramm 2. Asutus kus õpis või töötad.

Küsimusele „Digitaalne jalajälg on:“ vastasid 98,48% vastajates õigesti, milleks on kõikvõimalik informatsioon, mida inimene on enda kohta internetti maha jätnud. Kõigest 1,52% vastanutest vastas sellele küsimusele valesti milleks oli internetiteenus, mis jätab maha jälje, ning mitte ükski vastaja ei valinud vastuseks jälg, mis on digitaalne, mis oleks samuti vale olnud. Antud andmetest saab järeldada, et küsitluses osalenud on üldiselt teadlikud, mida digitaalne jalajälg tähendab ning ainult üksikud ei tea digitaalse jalajälje tähendust.

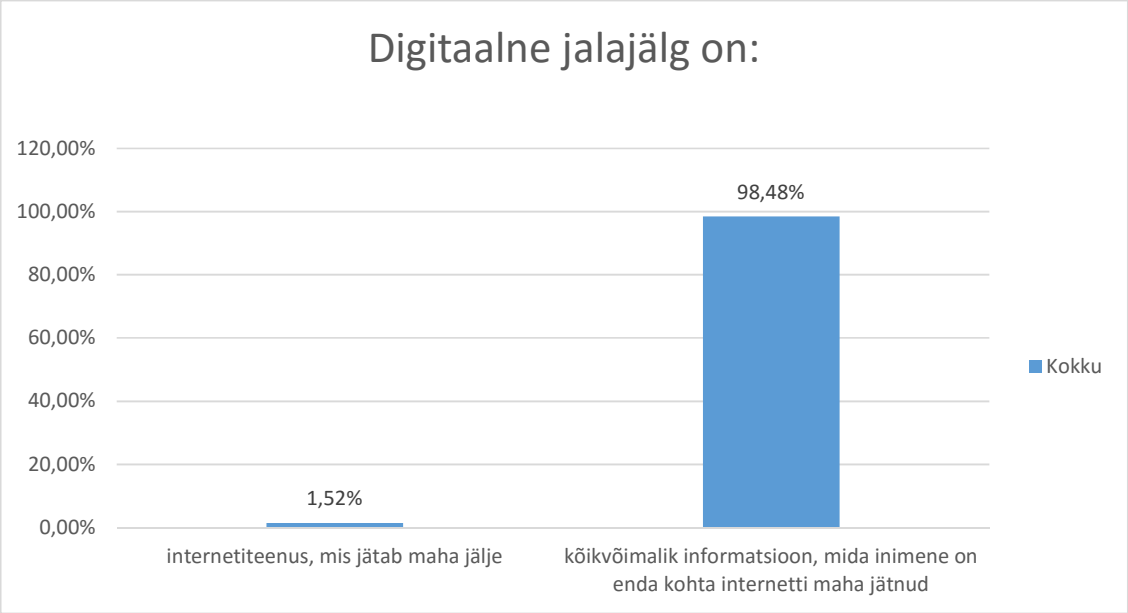

Diagramm 3. Digitaalne jalajälg on:

Küsimusele „Digitaalset jalajälge saab piirata“ oli küsitlusele vastajatel võimalik valida arvud ühest kuni viieni kus üks on üldse ei nõustu, kaks on osaliselt ei nõustu, kolm on neutraalne, neli on osaliselt nõustun ning viis on nõustun täielikult. Küsitluses osalenutest 28,79% nõustusid täielikult, et digitaalset jalajälge saab piirata. osaliselt nõustusid 30,30% vastanutest ning neutraalseks jäid 24,24% vastanutest. 12,12% vastanutest ei nõustunud osaliselt väitega et digitaalset jalajälge saab piirata ning 4,55% arvasid, et digitaalset jalajälge pole võimalik piirata. Antud küsimuse vastusest saab järeldada, et suurem osa vastajatest on teadlikud, et digitaalset jalajälge on võimalik piirata, kuid siiski on olemas piisvat suur vaatajaskond, kes ei nõustunud antud väitega või ei osanud seisukohta võtta.

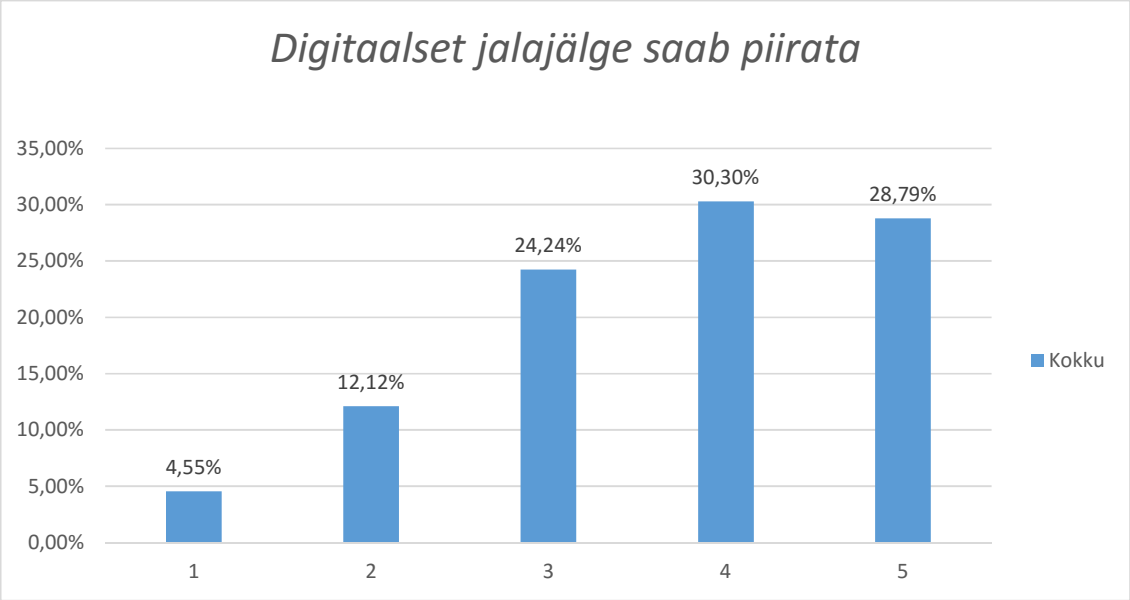

Diagramm 4. Digitaalset jalajälge saab piirata.

Internetti kasutades jääb maha digitaalne jalajälg, mille alusel on võimalik varastada kasutaja identiteet küsimusele vastasid 28,79% vastanutest et on täiesti nõus väitega. 40,91% vastanutest olid osaliselt nõus väitega ning 25,76% olid neutraalsed ning ei osanud seisukohta võtta. Kõigest 4,55% vastanutest ei olnud osaliselt nõus väitega ning ükski vastajatest ei valinud vastuseks 1 ehk üldse ei nõustu. Antud tulemuste alusel saab järeldada, et vastanute seas üldiselt levib arvamus, et digitaalse jalajälje abil on tõesti võimalik varastada kasutaja identiteeti ning seega tekitada reaalset kahju.

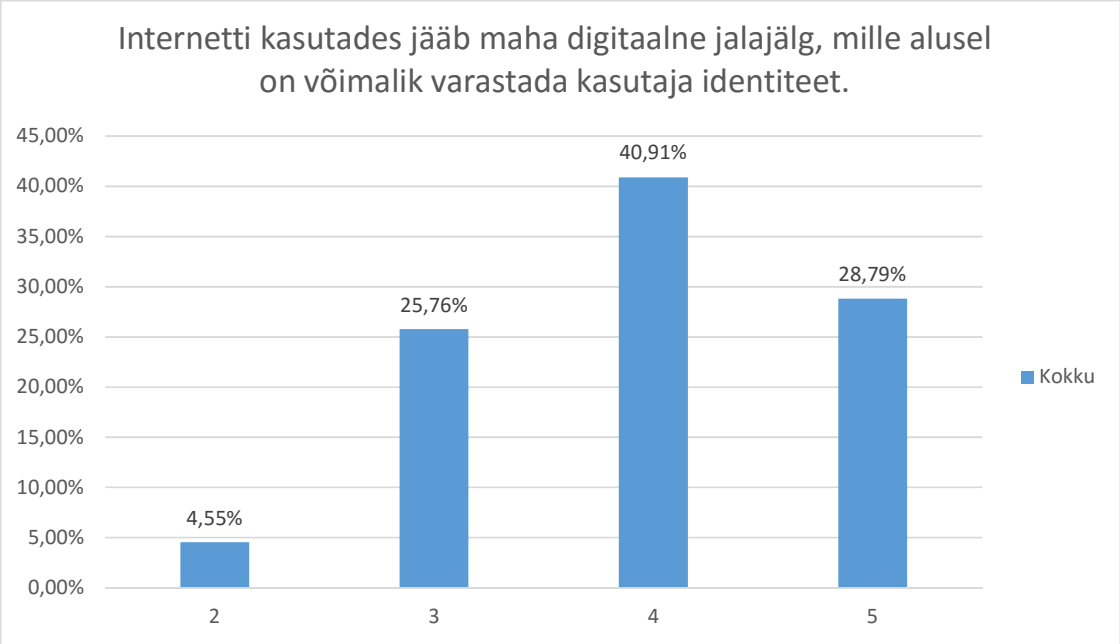

Diagramm 5. Internetti kasutades jääb maha digitaalne jalajälg, mille alusel on võimalik varastada kasutaja identiteet.

Oma privaatsuse pärast internetis tundis väga suurt muret 15,15% küsitluse vastanutest ning osaliselt tundsid muret 37,88% vastanutest. Neutraalse valiku tegid 28,79% vastanutest ja väga ei tunne muret 13,64% vastanutest. Kõigest 4,55% vastanutest ei tundnud üldse muret oma privaatsuse üle internetis. Antud tulemuses saab järeldada, suur osa vastanutest siiski tunneb muret oma privaatsuse pärast internetis kuid on palju ka neid kes väga ei tunne muret privaatsuse üle internetis.

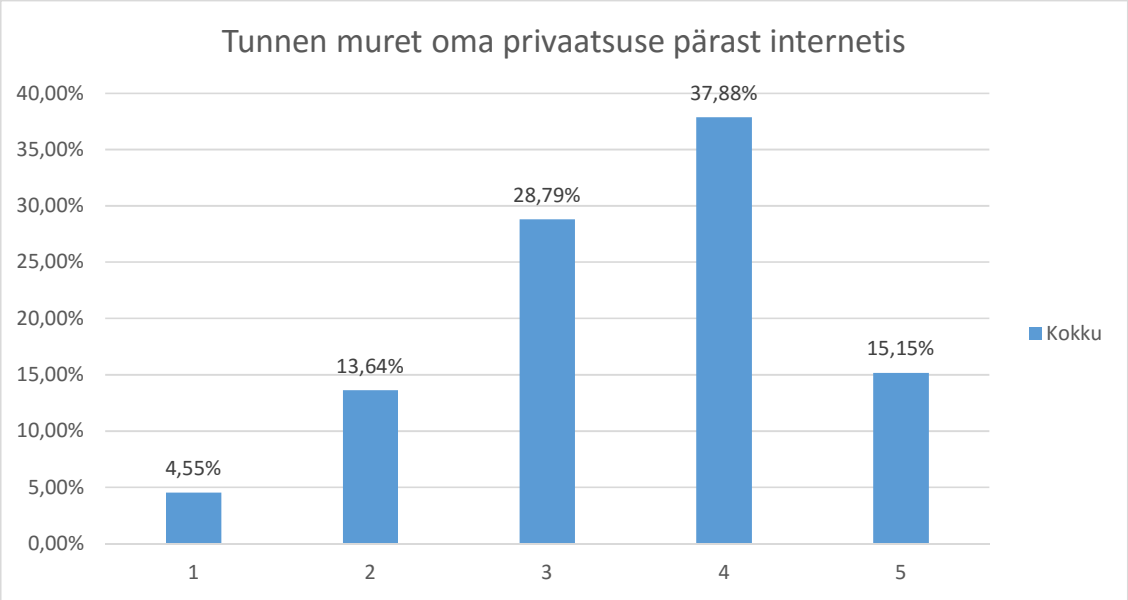

Diagramm 6. Tunnen muret oma privaatsuse pärast internetis.

Küsimuse „Millist infot on võimalik internetist kasutaja kohta saada“ vastasid 97,00% vastajatest e-postiaadress ning nimi. Teine populaarseim valik oli foto 98,50%. 95,50% vastajatest olid nõus et kasutaja füüsiline asukoht ning kasutaja huvid ja hobid on samuti võimalik läbi digitaalse jalajälje saada. 77.30% arvas, et kasutajanimed ja paroolid ning 55,40% leidsid et tervisega seonduv informatsioon on kättesaadav.

Keegi küsitluses osalenutest ei valinud vastuseks ei oska vastata ning 10,60% vastajatest pakus autori mainitutele oma lahendusi juurde. Mõni vastajates arvas, et kas on üldse midagi mida kasutaja kohta tänapäeval saada ei oleks eriti kui piisavalt kaua seadet kasutanud ollakse. Antud vastusest saab järeldada, et kasutajad on teatud määral teadlikud millist informatsiooni on võimalik kätte saada, kuid mitte piisaval määral.

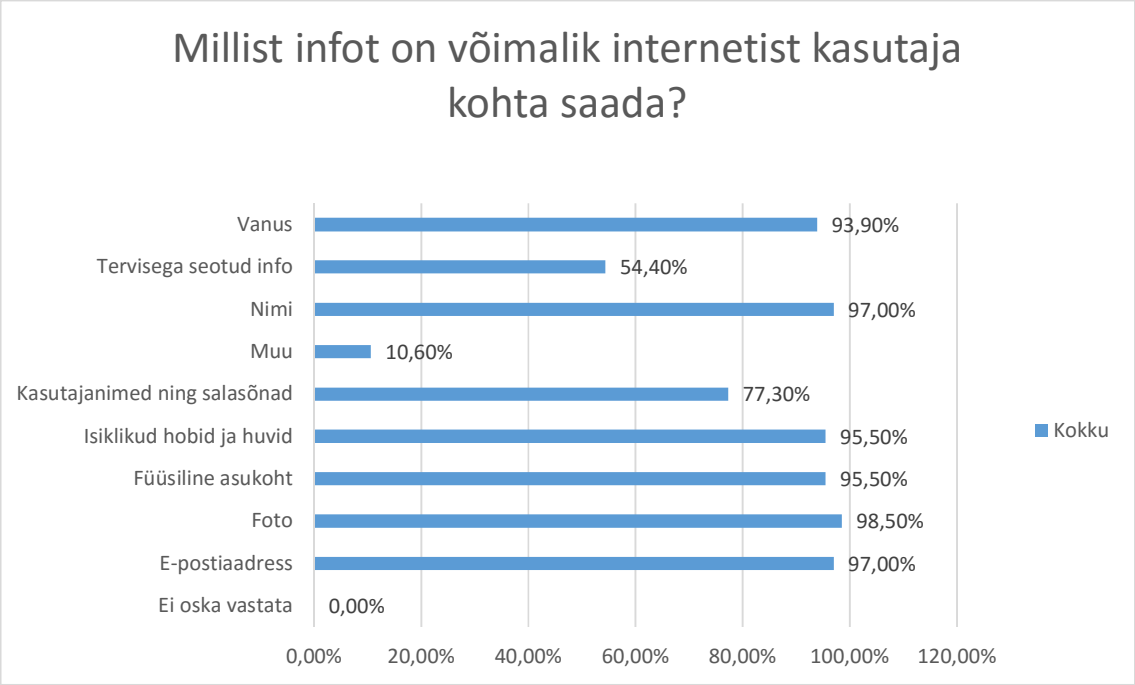

Diagramm 7. Millist infot on võimalik internetist kasutaja kohta saada?

Küsimuse millisel viisil on võimalik kasutaja kohta infot koguda olid vastajad kõige rohkem nõus sotsiaalvõrgustikuga, mille valisid 98,50% vastanutest. Pahavara kasutamise abil nõustus 92,40% vastanutest ning otsingumootorite abil 89,40%.Veel nõustusid 83,30% küsitluses osalenutest, et mobiilsed rakendused on võimelised kasutaja kohta infot koguma ja 78,80% erinevate veebilehtede külastamise abil. Arvuti rakenduste abil kasutaja kohta info saamiseks nõustus 71,20% ning 60,60% leidis, et läbi veebilehitseja lisandite kaudu saab kasutaja kohta informatsiooni.

Veel leidsid 50,00% kasutajatest, et seadme sõrmejäljest on võimalik infot saada ja 7,58% läbi veebilehitseja küpsiste. Kõigest 1.50% vastanutest pakus autori valikutele vastuseid juurde, ning kõik vastajad oskasid vähemalt ühe valiku teha. Antud vastustest saab välja lugeda, et kuigi kõige populaarsemaid meetmeid oskasid enamus valida, jäid vähem tuntud meetmed paljudel siiski valimata. Seega puudub suurel osal vastajatest piisavalt terviklik informatsioon selle kohta, kuidas kasutajatelt infot koguda on võimalik.

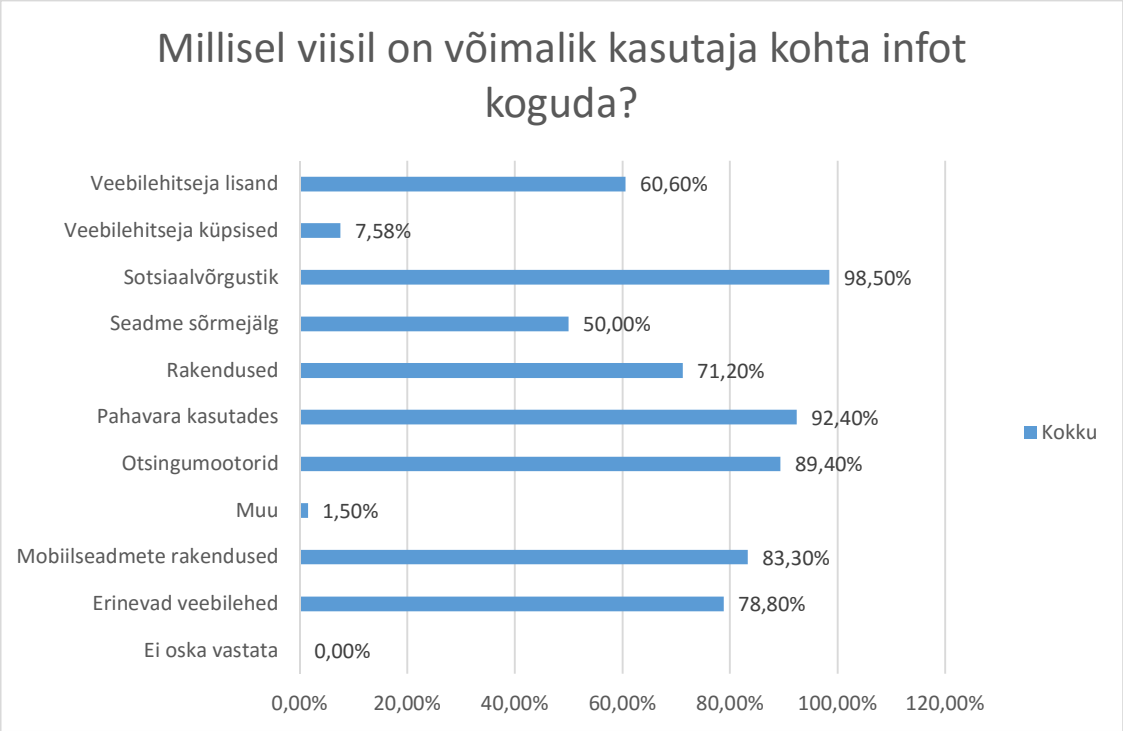

Diagramm 8. Millisel viisil on võimalik kasutaja kohta infot koguda?

Küsimusele „Kuidas on võimalik kahju tekitada kogutud andmetega“ 98,50% küsitluses osalenutest nõustus identiteedivargusega ning 97,00% vastajatest on nõus, et jälitamine ning manipuleerimine võivad tekitada kasutajale kahju. 90,90% arvab, et andmete hävimine ning avalikustamine ja 83,30% leiab, et rahaline kahju tekitab kahju kasutajale. Lisaks leiab 72,70% vastanutest võimaliku kahju rämpspostist ja 69,70% sihitud reklaamide pealt kahju. Veel arvasid 59,10% vastanutest, et kogutud andmetega on võimalik tekitada füüsilist kahju ning kõigest 3,00% vastanutest lisas juurde enda arvamuse. Vastanute seas ei olnud ühtegi inimest kes oleks valinud ei oska arvata. Tulemustest saab järeldada, et üldiselt ollakse nõus et kogutud andmetega saab tekitada kahju jälitamise ja manipuleerimisega ning identiteedi vargusega ja andmete hävimise ja avalikustamisega. Siiski pakuti märksa vähem teisi võimalike kahjusid. See näitab, et küsitluses osalenud ei pruugi olla teadlikud kõikidest võimalikest kahjudest, mida andmete kogumisega oleks võimalik saavutada.

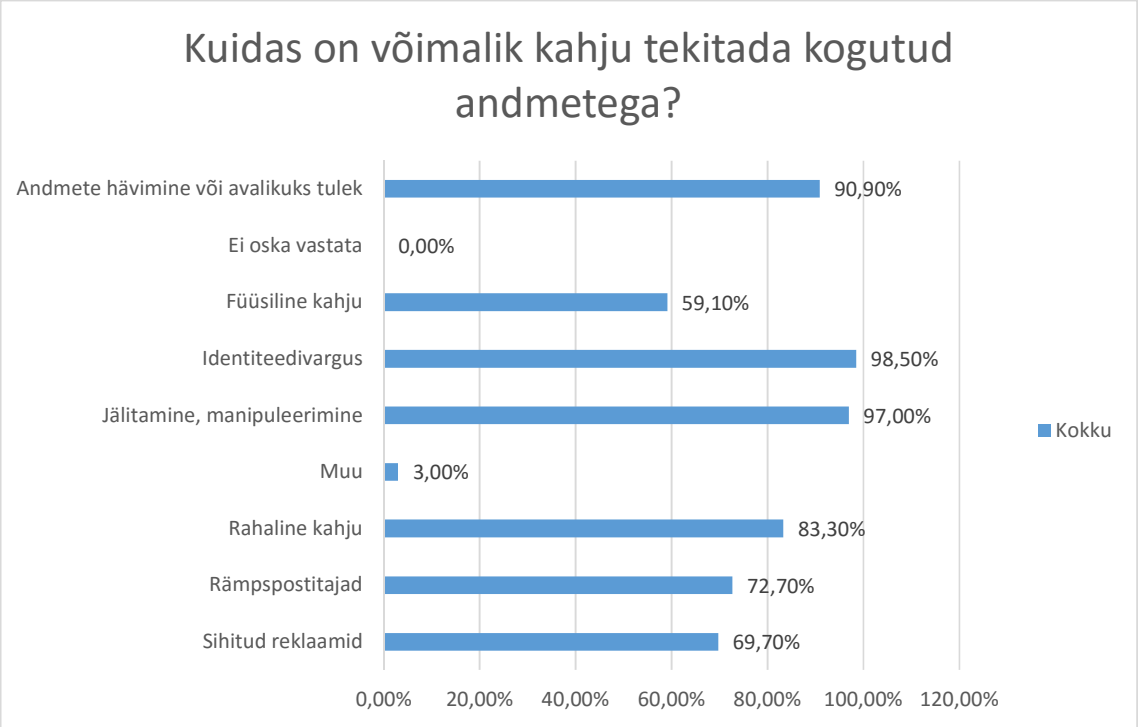

Diagramm 9. Kuidas on võimalik kahju tekitada kogutud andmetega?

Küsimusele „Olen nõus jagama oma digitaalset jalajälge kasu saamise eesmärgil teiste asutustega nagu näiteks valitsused ning erafirmad“ olid vastajad täiesti nõus oma digitaalselt jalajälge kasu saamiseks jagama valitsustele 9,09% ning erafirmadele 3,03% vastanutest. Osaliselt nõus digitaalse jalajälje jagamisega oli valitsustele 9,09% ja erafirmadele 4,55% küsimustikus osalenutest. Vastajatest 25,76% olid neutraalsed nii valitsusele kui ka erafirmale oma digitaalse jalajälje jagamise osas kasu saamise eesmärkidel. 18,18% vastanutest ei olnud väga nõus jagama oma digitaalset jalajälge valitsusele ning 15,15% erafirmadele. Üle veerandi vastajatest ehk 27,27% ei olnud üldse nõus valitsusele ning üle kolmandiku ehk 36,36% vastajatest ei olnud erafirmale oma digitaalset jalajälge jagama kasu saamise eesmärkidel ning 10,61% ei osanud arvamust avaldada valitsusele digitaalse jalajälje jagamise osas ning 15,15% erafirmale digitaalse jalajälje jagamise osas kasusaamise eesmärgil.

Vastustest saab järeldada, et üldiselt ei nõustuta digitaalse jalajälje jagamisega kasu saamise eesmärkidel, kuid oli ka hulk vastajaid kes ei osanud arvamust avaldada. See näitab, et kasutajate teadlikkus antud teemal on liiga väike. Lisaks saab tulemustest välja lugeda, et üldiselt ollakse rohkem nõus digitaalset jalajälge jagama kasu saamise eesmärgil valitsusele rohkem kui erafirmadele.

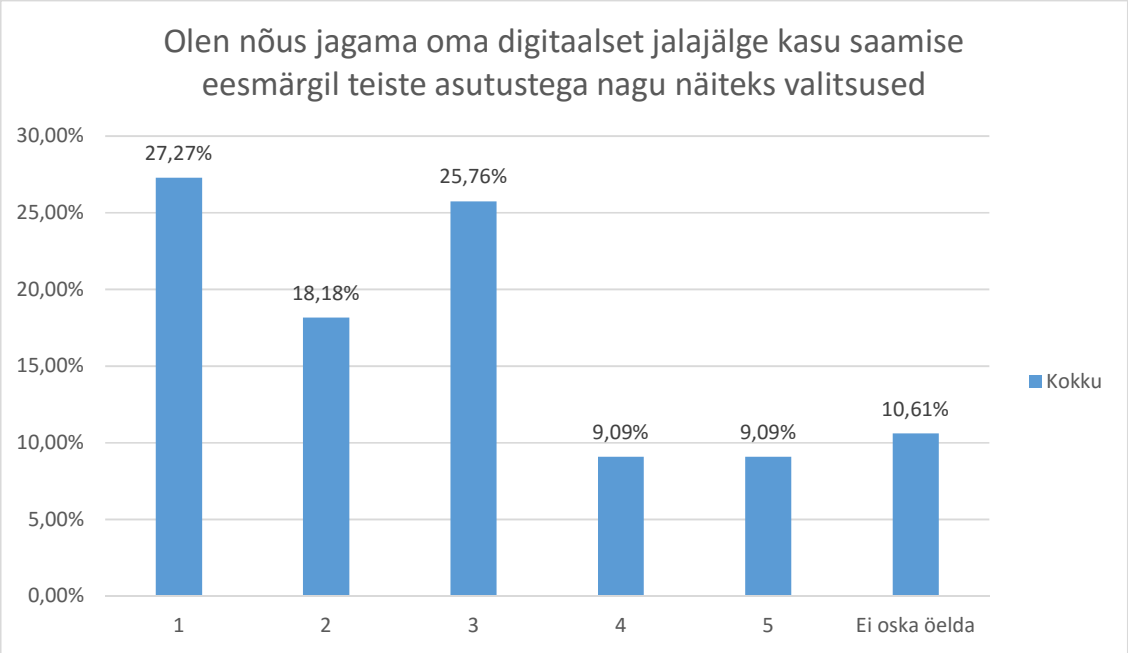

Diagramm 10. Olen nõus jagama oma digitaalset jalajälge kasu saamise eesmärgil teiste asutustega nagu näiteks valitsused.

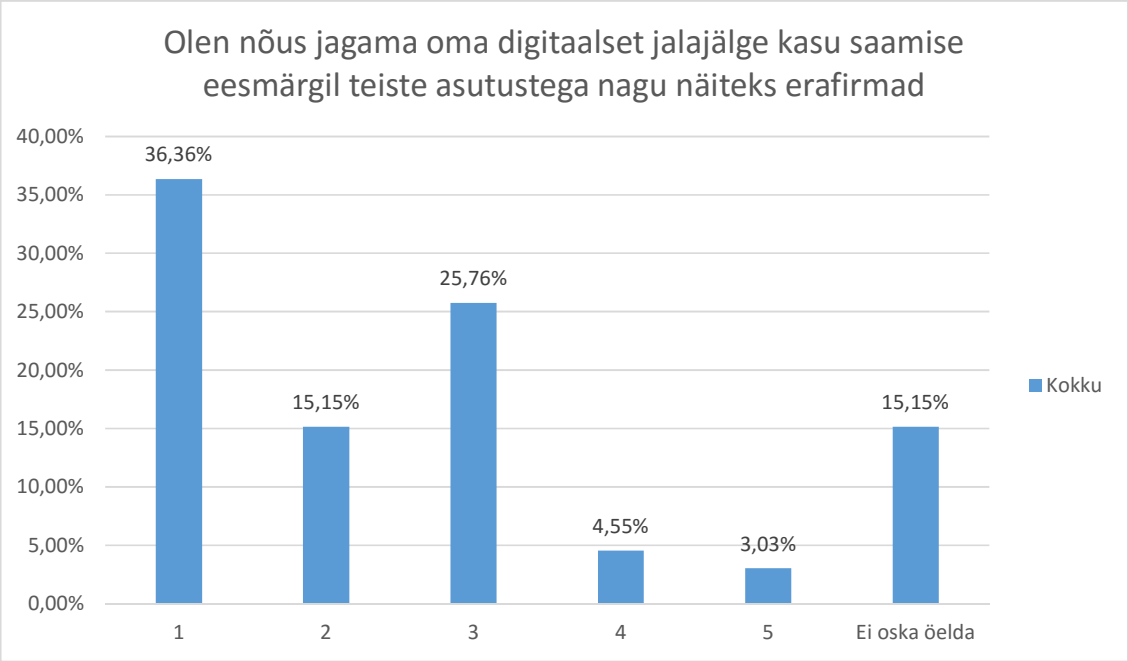

Diagramm 11. Olen nõus jagama oma digitaalset jalajälge kasu saamise eesmärgil teiste asutustega nagu näiteks erafirmad.

Küsimusele „Milliste meetodite abil on võimalik digitaalset jalajälge vähendada“ vastas 63,60% vastajatest Andmete krüpteerimine. 59,10% küsitluses osalenutest vastas virtuaalne privaatvõrk (VPN) ja turvalisema tarkvaraplatvormi valiku poolt. Anonümiseerija (nt Tor) poolt oli 53,00% vastajatest ja veebilehitseja privaatse režiimi poolt 51,50%. Võrselt 50,00% vastustest said puhverserver (proxy) ja veebilehitseja turvalisust tõstev lisand. Veel sai ajutiste failide kustutamine valitud 40,90% vastajate seast ja 5,70% kasutajatest lisasid enda arvamusi juurde. Küsimusele vastata ei osanud 22,70% vastajatest. Antud küsimuse vastustest saab järeldada, et küsitluses osalenutest ei teadnud suur hulk vastanutest milliseid meetmeid on võimalik rakendada digitaalse jalajälje vähendamiseks.

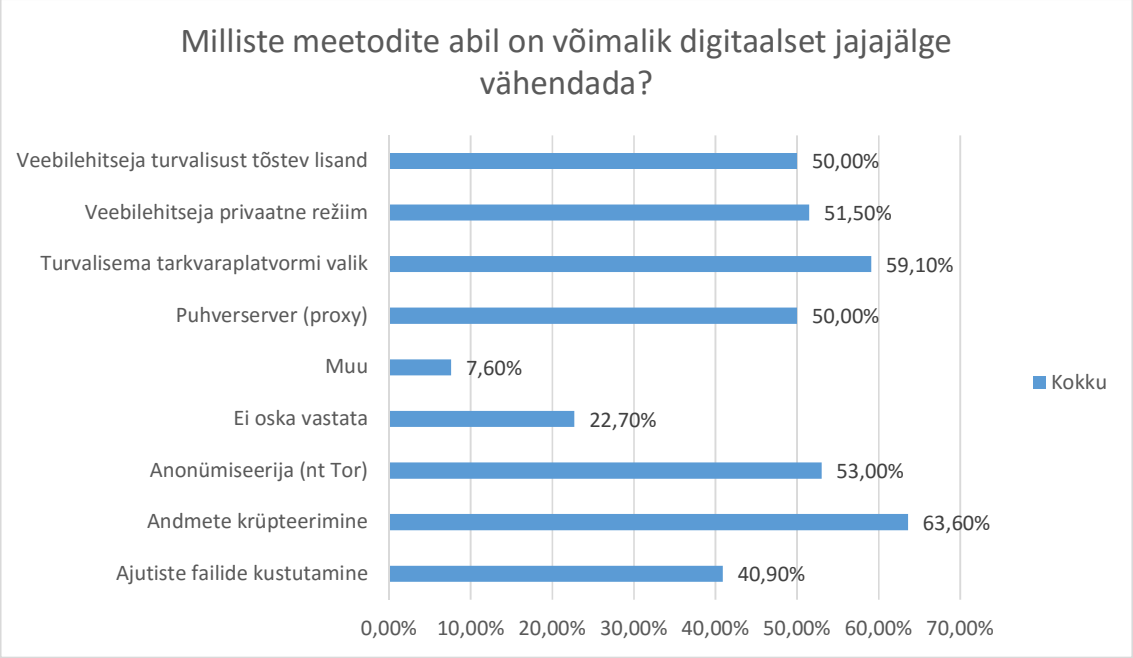

Diagramm 12. Milliste meetodite abil on võimalik digitaalset jajajälge vähendada?

Küsimusele „Kui efektiivne on antud lahendus on digitaalse jalajälje vähendamiseks“ leidsid küsitluses osalenud, et kõige efektiivsem lahendus on muuta kasutusharjumusi. Teine efektiivsem lahendus, mida vastajad valisid on andmete krüpteerimine. Veel peeti digitaalse jalajälje vähendamiseks efektiivseks puhverserverit, anonümiseerijat nagu näiteks Tor, turvalisema tarkvaraplatvormi valikut ja virtuaalset privaatvõrku. Vähem efektiivseks peeti veebilehitseja privaatset režiimi, ajutiste failide kustutamist ning kõige ebaefektiivsemaks peeti veebilehitseja turvalisust tõstvat lisandit.

Samuti ei osanud väga suur osa vastajatest antud küsimustele vastata ning kõige vähem teati puhverserverit, anonümiseerijat nagu näiteks Tor ja virtuaalset privaatvõrku. Antud küsimuse vastustest saab eeldada, et küsitlusele vastanutest ei teadnud väga suur osa eelnimetatud lahendustest midagi kuna tihti valiti efektiivsetele lahendustele vastuseks mitte efektiivne ning suur hulk vastanutest ei osanud öelda kas eelnimetatud lahendused on efektiivsed.

Küsimusele „Kui oled kasutanud varem mõnda meetodit, siis millist ning mis oli peamine põhjus“ vastas 43,94% küsitlusel osalenutest, kus 9,09% kasutajad vastasid et ei ole varem mõnda meetodit kasutanud ning seega on 34,85% kasutajatest varem kasutanud mõnda eelnevat meetodit. 6,06% küsimusele vastajatest on kasutanud varem Tor-i digitaalse jalajälje vähendamiseks. 9,09% vastajatest on kasutanud varem puhverserverit ja 7,56% VPN-i ning nende kasutuste peamiseks põhjuseks toodi välja regioonide piirangute vältimiseks.

Veel on 7,56% vastanutest muutnud oma kasutusharjumusi ja 4,54% veebilehitseja privaatset režiimi. 1,51% vastajatest on kastutanud veebilehitseja turvalisust tõstvat lisandit ja võtnud kasutusele turvalisema platvormi ning 6,06% küsimusele vastajat on varem andmeid krüpteerinud. Lisaks on 4,54% vastanuid kustutanud ajutisi faile. Antud küsimuse vastustes saab välja lugeda, et ligikaudu üks kolmandik vastajatest on midagi ette võtnud oma digitaalse jalajälge vähendamiseks ning osa, kes on mõnda meetodit kasutanud, on seda teinud rohkem riiklikest piirangutest mõõda saamiseks, mitte oma digitaalse jalajälje vähendamiseks.

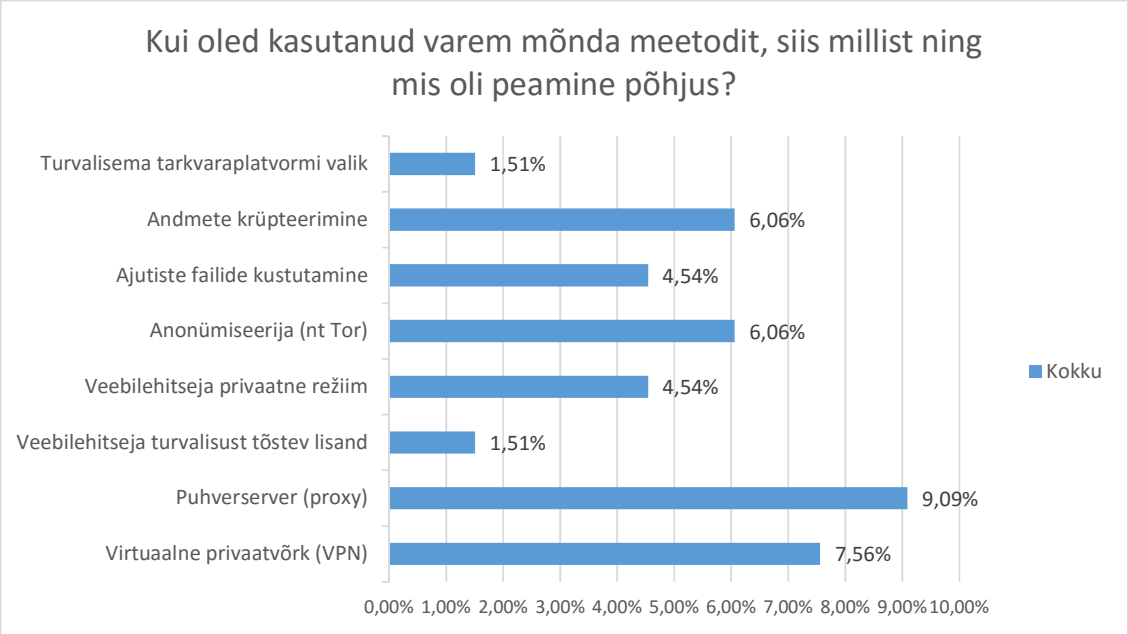

Diagramm 13. Kui oled kasutanud varem mõnda meetodit, siis millist ning mis oli peamine põhjus?

Küsimusele „Millisel määral nõustud, et järgmised operatsioonisüsteemid tagavad võimalikult väikese digitaalse jalajälje“ leidsid küsitluses osalenud, kes ei valinud ei oska vastata vastuseks, et kõige rohkem tagab arvuti kasutamise puhul operatsioonisüsteem Linux võimalikult väikese digitaalse jalajälje ning sellele järgnevad Apple OS X ja Microsoft Windows vastavalt. Mobiilsete operatsioonisüsteemide osas arvatakse, et võimalikult väikese digitaalse jalajälje jätab IOS ning enamus leidsid, et Android üldjuhul ei aita tagada võimalikult väikese digitaalse jalajälje.

Küsimuse vastustest saab järeldada, et enamus kasutajad ei ole kursis sellega, milline operatsioonisüsteem võimalikult väikese digitaalse jalajälje ning need, kes oskasid vastata leidsid, et arvutimaalimas on usaldusväärseim operatsioonisüsteem Linux ning vähem usaldusväärseim Microsoft Windows ning mobiilses maailmas peetakse iOS operatsioonisüsteemiks, mis aitab tagada võimalikult väikese digitaalse jalajälje.

Küsimusele „Millisel määral usaldad tasulist tarkvara rohkem kui vabavara digitaalse jalajälje vähendamiseks“ vastasid 7,58% osalenutest, et eelistavad tasulist tarkvara kindlalt vabavarale digitaalse jalajälje vähendamiseks. 16,67% usaldavad tasulist tarkvara rohkem, kui vabavara digitaalse jalajälje vähendamiseks. 43,94% küsitlusel osalenutest üldiselt usaldavad tasulisi lahendusi digitaalse jalajälje vähendamiseks rohkem kui vabavaralisi lahendusi. 22,73% osalenutest usaldavad natuke rohkem tasulist tarkvara ja 9,09% vastanutest ei usalda tasulist tarkvara rohkem, kui vabavaral põhinevaid lahendusi.

Küsimuse vastusest saab järeldada, et küsitluses osalenud on rohkem nõus usaldama tasulisi lahendusi vabavaralistele digitaalse jalajälje vähendamiseks, kuigi vabavaralistel lahendusel on kasutajal võimalik tarkavaral silma peal hoida, vaadates läbi tarkvara lähtekoodi ning soovi korral seda ise muutes. Selliseid omadused tasulistel lahendustel tavaliselt puuduvad ning kasutajad võivad sattuda arendaja tiimi eksituse ohvriks, vigade parandamiseks pole kasutajal midagi muud teha kui võtta arendusmeeskonnaga ühendust ning loota, et viga eemaldatakse. Seega on toimumas jää murenemine ehk tasapisi hakatakse aru saama omandvara probleemides ning aina rohkem on hakatud usaldama vabavara.

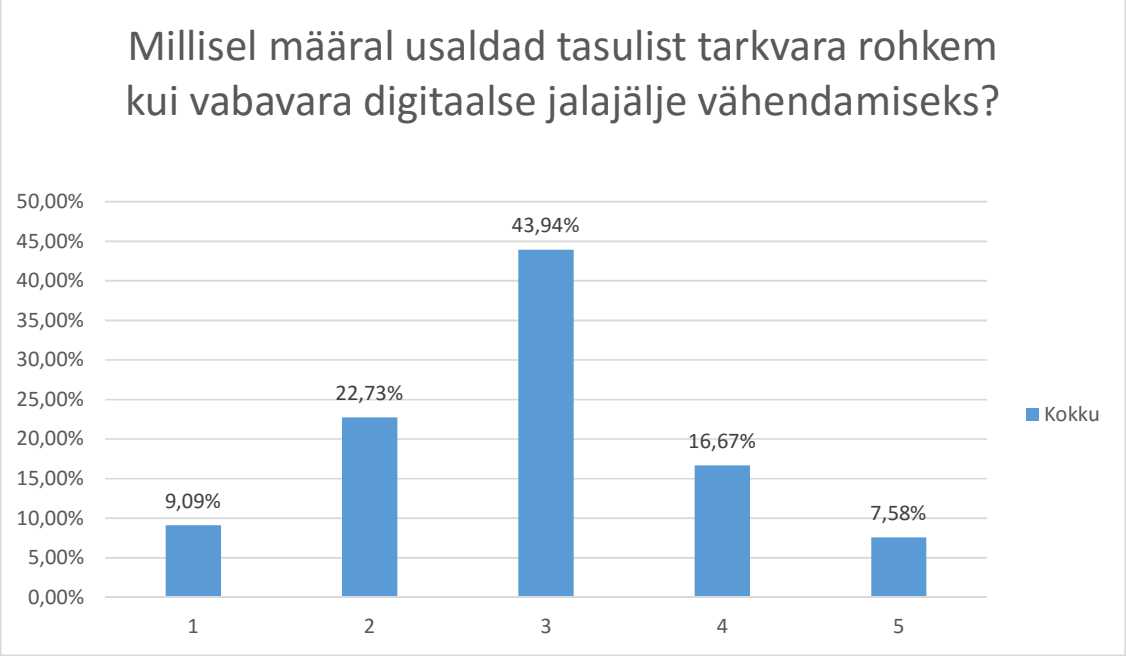

Diagramm 14. Millisel määral usaldad tasulist tarkvara rohkem kui vabavara digitaalse jalajälje vähendamiseks?

„Kui oled muutnud kasutusharjumusi siis millised“ küsimusele vastas 83,30% vastajatest, et on isikliku info jagamisega internetis ettevaatlikumad ning 66,70% on sotsiaalvõrgustiku seadeid muutnud või nendest loobunud. 42,40% küsitlusel osalenutest on võtnud kasutusele veebilehitseja privaatse režiimi. 40,90% küsimuse vastajatest ei jäta kasutajanimesid, salasõnasid veebilehitsejale enam meelde ja 30,30% on kasutanud registreerimisel võltsitud andmeid. Lisaks on 21.20% vastajatest võtnud kasutusele alternatiivseid otsingumootoreid ja 25,80% otsustanud turvalisema e-postiteenuse kasuks. Küsitlusel osalenutest on 18.20% andmeid krüpteerinud ja 10.60% vahetanud operatsioonisüsteemi turvalisema vastu. 1,50% on võtnud kasutusele veebilehitseja privaatse režiimi. Kasutusharjumusi ei ole muutnud 9,10% vastanutest.

Antud küsimuse vastustest saab järeldada, et suurim osa vastanutest on infojagamisega ettevaatlikum, kuid tekib oluline konflikt eelneva küsimusega „kui oled kasutanud varem mõnda meetodit, siis millist ning mis oli peamine põhjus“, kuna eelneval küsimusel ei olnud kasutusharjumusi muutnud 18,18% vastanutest aga „Kui oled muutnud kasutusharjumusi siis millised“ küsimusel ei olnud kõigest 9,10% kasutusharjumusi muutnud.

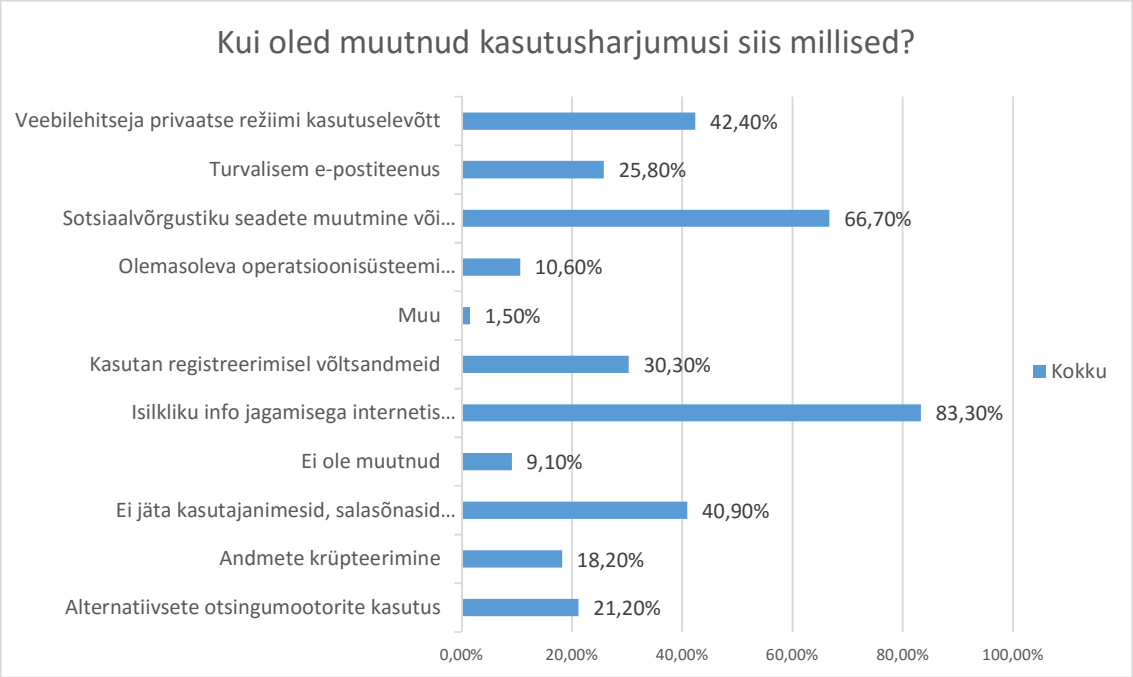

Diagramm 15. Kui oled muutnud kasutusharjumusi siis millised?

„Mind motiveerib erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kasutusele võtma see kui nende kasutamine oleks võimalikult kerge“ küsimusele vastasid 39,39%, et nõustuvad täielikult väitega „mind motiveerib erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kasutusele võtma see kui nende kasutamine oleks võimalikult kerge“. 27,27% küsitluses osalenutest nõustusid osaliselt väitega ja 28,79% vastanutest jäid neutraalseks ehk ei osanud seisukohta võtta. Kõigest 1,52% osalenutest väga ei nõustunud väitega ja 3,03% vastanutest ei nõustunud üldse väitega et mind motiveerib erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kasutusele võtma see, kui nende kasutamine oleks võimalikult kerge.

Küsimuse vastustest saab seega järeldada, et enamus on siiski motiveeritud võtma kasutusele erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kui nende kasutamine oleks võimalikult kerge.

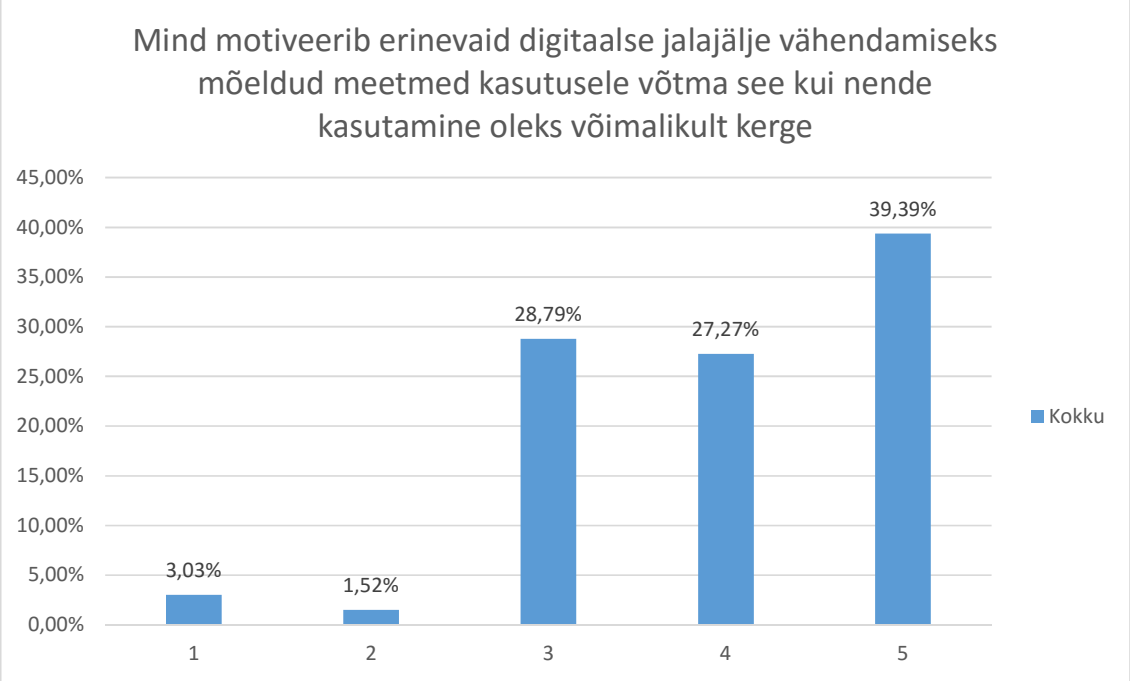

Diagramm 16. Mind motiveerib erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kasutusele võtma see kui nende kasutamine oleks võimalikult kerge.

„Tunnen muret kui vähetuntud või tuntud asutus huvitub minu digitaalse jalajälje vastu“ küsimusele vastas 43,94%, et tunneb väga suurt muret kui vähetuntud asutus huvitub minu digitaalsest jalajäljest ning 25,76% kui tuntud asutus tunneb huvi minu digitaalse jalajälje vastu. Vähetuntud asutuse osas tunneb muret 21,21% vastanutest ja tuntud 19,70%. 22,73% ja 37,88% vastanutest tundsid teatud määral muret vähetuntud ja tuntud asutuste osas ning 7,58% küsitluses osalenutest tundsid nii vähetuntud kui ka tuntud asutuse osas muret, kui eelnevad oleks huvitatud nende jalajäljest ja üldse ei tundnud muret vähetuntud asutuste huvi nende digitaalse jalajälje vastu 4,55% ja tuntud asutustes 9,09%.

Andmetest saab järeldada, et küsitluses osalenud tunnevad rohkem muret, kui vähetuntud asutus oleks nende digitaalsest jalajäljest huvitatud ja vähem muret tuntud asutuste osas. Lisaks on hulk vastajaid, kes ei muretse üldse selle üle, kes nende digitaalse jalajälje vastu huvi tunnevad.

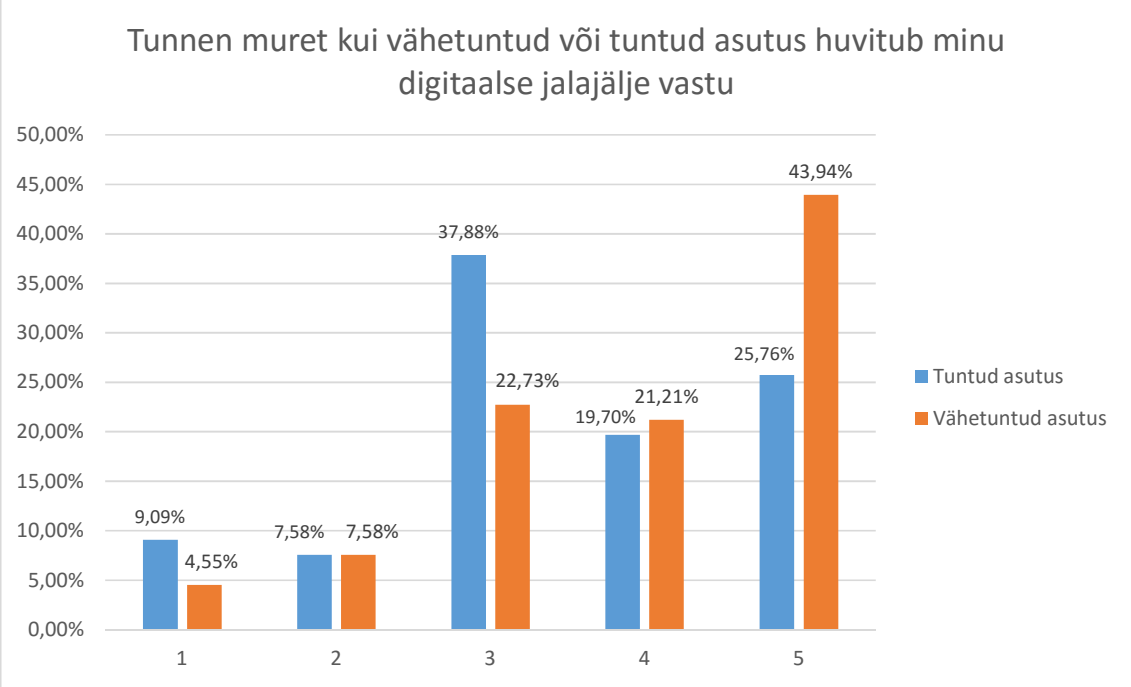

Diagramm 17. Tunnen muret kui vähetuntud või tuntud asutus huvitub minu digitaalse jalajälje vastu.

Küsimusele „Püüan vähendada digitaalset jalajälge kui mulle on tekitatud kahju“ vastasid 56,06% küsitluses osalenud et kindlasti püüavad vähendada oma digitaalist jalajälge kui kahju on tekitatud. 30,30% vastajatest püüavad vähendada kahju saamisel digitaalset jalajälge ning kõigest 6,06% on enam-vähem väitega nõus. Väitega eriti nõus polnud 3,03% vastajatest, ning üldse ei nõustunud väitega „püüan vähendada digitaalset jalajälge kui mulle on tekitatud kahju“ 4,55% osalenutest. Küsimuse vastustest saab järeldada, et küsitluses osalenud üldiselt püüaksid oma digitaalset jalajälge vähendada kahju tekkimise tagajärjel.

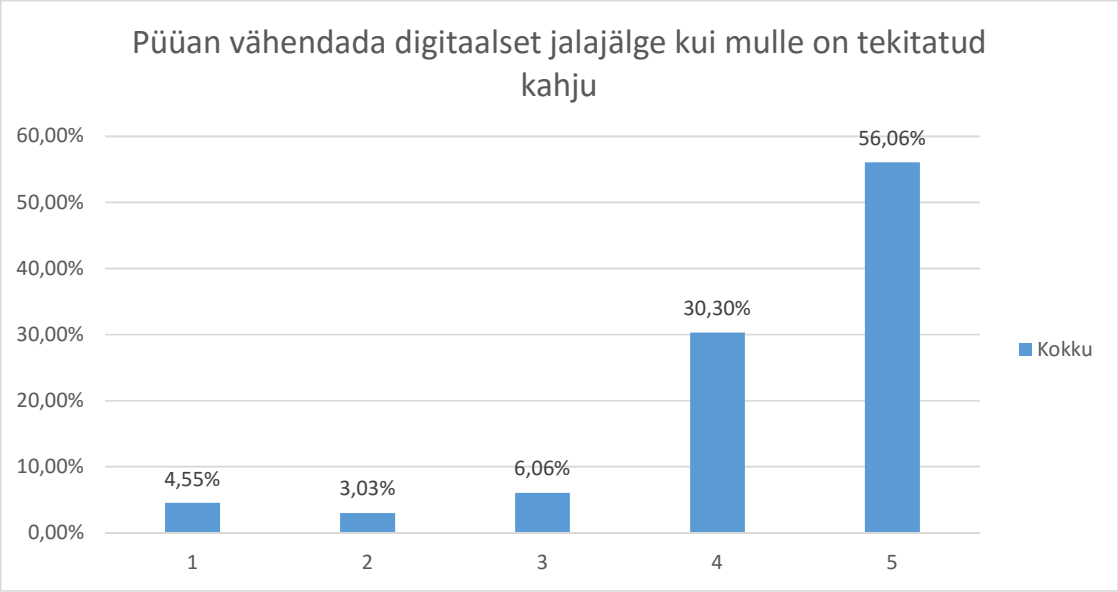

Diagramm 18. Püüan vähendada digitaalset jalajälge kui mulle on tekitatud kahju.

Küsimusele „Mis motiveeriks vähendama enda digitaalset jalajälge“ vastas 95,50% osalenutest et neid motiveerib isiklik kahju digitaalse jalajälje vähendamiseks. 66,70% leidsid, et teadmine, et digitaalse jalajälge abil suunatakse sinu mõttemaailma on motivatsioon ja 63,60% teadmine, et isiklike andmeid töödeldakse ettevõtte kasu eesmärgil. Sihitud reklaamide saamine motiveeriks digitaalset jalajälge vähendama 54,50% osalenutest ja 50,00% riigiasutuse pilt nende huvidest. Kõigest 3,00% vastanutest vastasid, et neil puudub motivatsioon digitaalse jalajälje vähendamiseks ja 1,50% vastanutest pakkus oma motiivi.

Vastuste andmetest saab järeldada, et kõige rohkem motiveerib küsitluses osalenuid digitaalset jalajälge vähendama isiklik kahju ning ülejäänud autori pakutud vastustest üle poolte olid motiveeritud digitaalse jalajälje vähendama. Seega enamus küsitlusel osalenutel on olemas motivatsioon digitaalse jalajälje vähendamiseks.

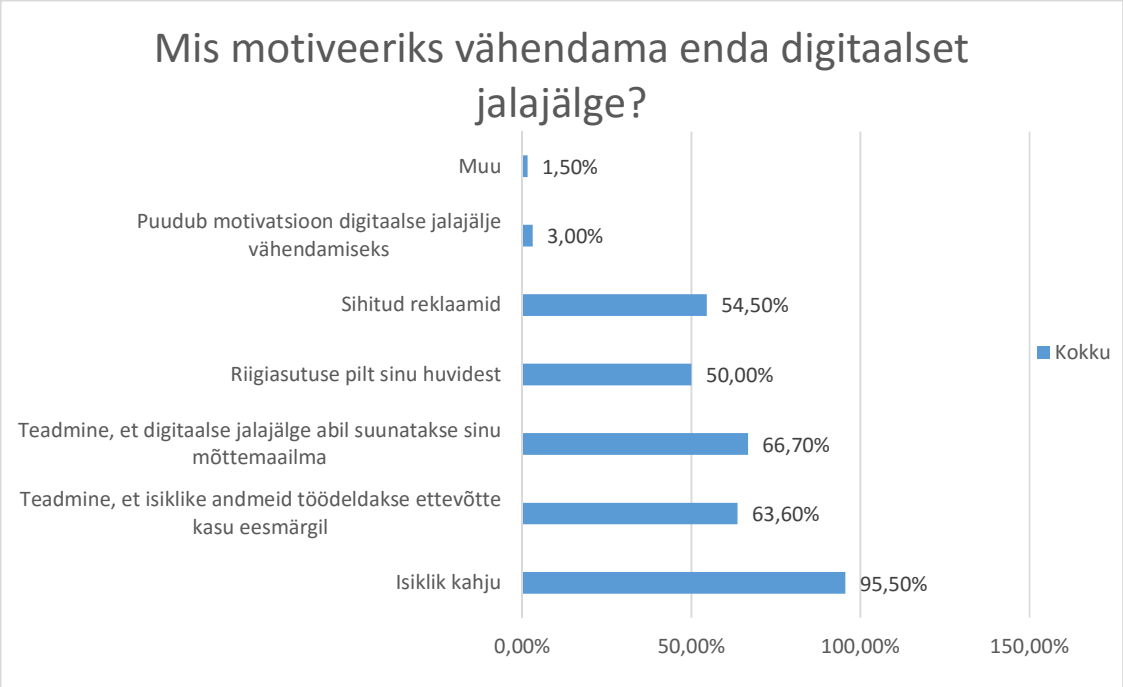

Diagramm 19. Mis motiveeriks vähendama enda digitaalset jalajälge?

Küsimusele „Privaatsust internetis ei ole olemas“ vastas 43,94% osalejatest, et nõustuvad täielikult väitega, et privaatsust internetis ei ole olemas ja 27,27% nõustusid väitega osaliselt. Neutraalse ehk kindlat seisukohta ei võtnud 24,24% vastajatest ja 4,55% leidis, et osaliselt ei nõustu väitega, et privaatsust internetis ei ole olemas ning ükski vastajatest ei valinud vastuseks 1 ehk üldse ei nõustu väitega privaatsust internetis ei ole olemas. Küsimuste vastustest saab järeldada, vastajad üldiselt pooldavad väidet „privaatsust internetis ei ole olemas“ ja kipuvad arvama, et privaatsust internetis ei saagi olla.

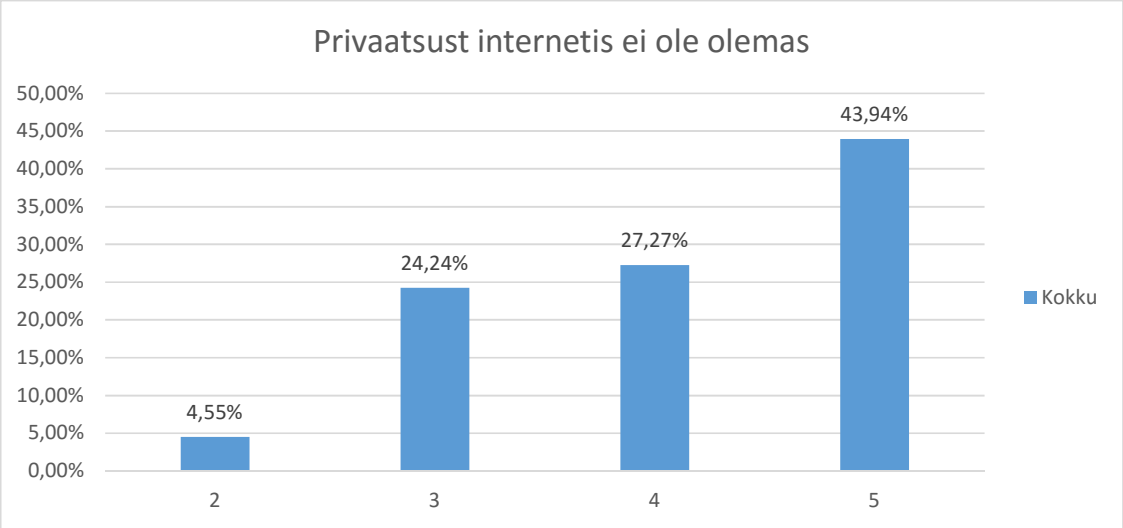

Diagramm 20. Privaatsust internetis ei ole olemas.

Küsimusele „Olen nõus muutma oma kasutusharjumusi vähendamaks digitaalset jalajälge“ olid 33,33% vastajatest täiesti nõus ja 36,36% osaliselt nõus muutma oma kasutusharjumusi digitaalse jalajälje vähendamiseks. Neutraalse ehk seisukohta ei osanud öelda 18,18% osalenutest ning 9,09% ei ole väga nõus ja 3,03% ei olnud üldse nõus oma kasutusharjumusi muutma digitaalse jalajälje vähendamiseks. Küsimuse vastustest on siiski valdav enamus nõus muutma oma kasutusharjumusi digitaalse jalajälje vähendamiseks ning üldiselt väike protsent vastajatest ei olnud nõud oma kasutusharjumusi muutma digitaalse jalajälje vähendamiseks.

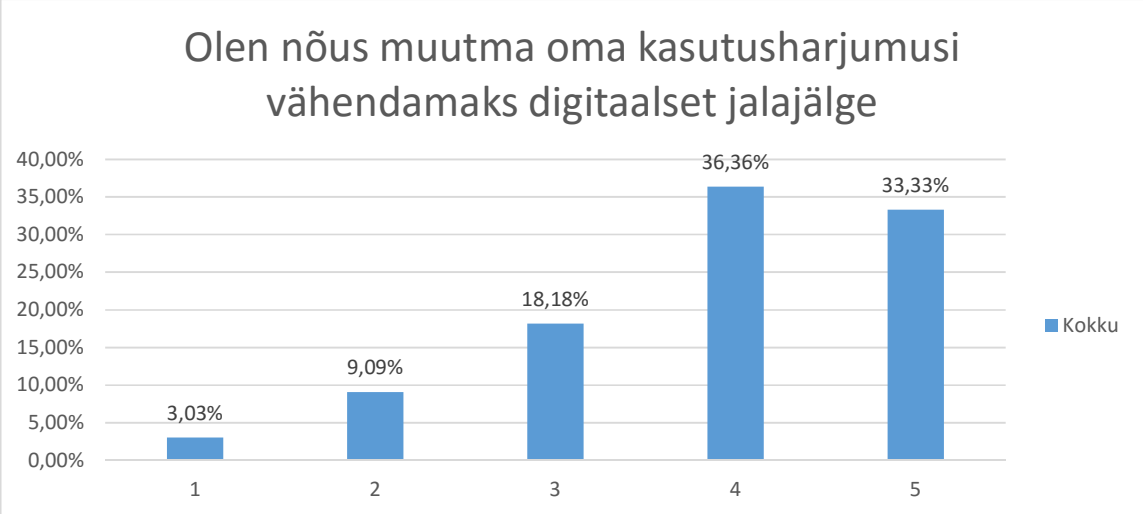

Diagramm 21. Olen nõus muutma oma kasutusharjumusi vähendamaks digitaalset jalajälge.

5.3. Järeldused

Küsitlusel osalenud puudus osaliselt informatsioon antud valdkonna kohta, kuna tihti ei olutud oma esitatud vastustest kindlad. Küsimuste analüüsimise käigus ilmnesid sisse lõhed vastuste vahel. Näiteks küsimuse milliste meetodite abil on võimalik digitaalset jalajälge vähendada valisid 59,10% vastajatest turvalisema tarkvaraplatvormi ja kui efektiivne on antud lahendus on digitaalse jalajälje vähendamiseks oli Turvalisema tarkvaraplatvormi valikust ei oska vastata 30,30% vastajatest ning 4 ja 5 ehk nõustumise valisid 36,36%.

Sama lugu on ka küsimuste millisel määral nõustud, et järgmised operatsioonisüsteemid tagavad võimalikult väikese digitaalse jalajälje operatsioonisüsteemi Linux vastajatest 39,39% valinud ei oska vastata ja 4 ja 5 ehk nõustumise valisid 28,79%. ning küsimuse millisel määral usaldad tasulist tarkvara rohkem, kui vabavara digitaalse jalajälje vähendamiseks vahel, kus viimasel olid ebakindlad 43,90% ja 24,3% vastajatest usaldas omandvara rohkem kui vabavara ning 31,8% ei usalda omandvara rohkem.

Uuringu alusel saab järeldada, et vastajad teavad mis on digitaalne jalajälg ja on üldiselt mures privaatsuse pärast internetis, kuna suur osa vastajatest leiab, et privaatsust internetis ei ole olemas. Üldiselt ollakse teadlikud, et digitaalne jalajälge saab piirata ning lisaks teatakse mõnda meetodit digitaalse jalajälje vähendamiseks ja osaktakse nimetada mõned infod mida digitaalne jalajälg sisaldab ning millised on nende tagajärjed. Osad vastajad on ka digitaalse jalajälje vahetamiseks midagi ette võtnud kuid enamus seda siiski teinud pole.

Lisaks kiputakse usaldama rohkem valisusi oma digitaalse jalajäljega kui erafirmasid ning tuntakse rohkem muret selle üle, kui vähetuntud asutused tunneksid huvi nende digitaalse jalajälje kohta ning kiputakse rohkem tuntuid asutusi usaldama. Veel motiveerib suur hulk vastajaid erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmeid kasutusele võtma see kui nende kasutamine oleks võimalikult kerge ning vastajad püüavad kõige rohkem nõus vähenema digitaalset jalajälge kui neile on tekitatud kahju selle alusel.

Kokkuvõte

Töö käigus selgitas autor, mis on digitaalne jalajälg ja mida mõistetakse vabavara all. Digitaalne jalajälg on kogum andmeid, mis eksisteerib tänu kasutaja tegevustele digitaalses maalimas, mida on võimalik seostada kindla kasutajaga. Vabavara on tarkvara, mis on tasuta kättesaadav ning avatud lähtekoodiga. Töö käigus leidis autor vastused kõikidele püstitatud uurimisküsimustele.

Töös toodi välja millist infot ja kuidas kasutajate kohta on võimalik saada, tuues esile veebilehitseja küpsised, otsingumootorid, seadme sõrmejälje ning asukoha jälgimise. Kõik eelnimetatud tekitavad kasutaja kohta digitaalse jalajälje, mida on võimalik kasutaja endaga siduda nagu näiteks ligikaudne asukoht, isiklikud hobid ja huvid, kasutajanimed ning salasõnad, vanuse grupp, e-postiaadress, nimi, foto või terviseandmed.

Autor tutvustas lugejale, kuidas oleks võimalik vähendada digitaalset jalajälge erinevate vabavaraliste tarkvarade abil, milleks osutusid VPN teenuse pakkuja nagu OpenVPN. Veel oli võimalik digitaalset jalajälge vähendada andmete krüpteerimise kaudu, kasutades vabavaralisi lahendusi nagu GNU Privacy Guard ja Veracrypt. Lisaks eelnimetatutele on digitaalse jalajälje vähedamiseks võimalik kasutada Tor veebilehitsejat. Olemasolevatele veebilehitsejatele on olemas vabavaralisi lisandid, mis aitavad digitaalset jalajälge vähendada nagu näiteks HTTPS Everywhere, AdBlock Plus, Disconnect, NoScript ja ScriptSafe ning Privacy Badger. Lisaks on võimalik vahetada olemasolev operatsioonisüsteem turvalisusele ja privaatsusele pühenduva operatsioonisüsteemi vastu.

Antud lahendustega peab kasutaja muutma oma kasutusharjumusi, kuna eelnimetatud lahendused võivad interneti kiirust aeglustada ning mõni lahendus võib veebilehe kasutuskõlbmatuks muuta, ning kasutajal tuleb ise uurida, millised allikaid blokeerida ning milliseid mitte, et veebileht korralikult kuvaks ja töötaks.

Antud töös viis autor läbi uuringu, kus leiti, et uuringus osalenud on üldiselt väga kahtlevad ega teadvusta digitaalse jalajälje ohtusid. Autor järeldas, et vastajad teavad mis on digitaalse jalajälje definitsioon ja oskavad osaliselt nimetada, mida digitaalne jalajälg võib sisalda. Üldjuhul ollakse mures privaatsuse pärast internetis. Üldiselt ollakse teadlikud, et digitaalne jalajälge saab piirata ning teatakse mõnda tuntud meetodit digitaalse jalajälje vähendamiseks.

Uuringus osalejad usaldasid rohkem valisusi oma digitaalset jalajälge kasutama kui erafirmasid ning muretseksid rohkem, kui vähetuntud asutused tunneksid huvi nende digitaalse jalajälje vastu. Veel motiveerib suurt hulka vastajaid digitaalse jalajälje vähendamiseks mõeldud meetmeid kasutusele võtma see, kui nende kasutamine oleks võimalikult kerge ning osalenud püüavad kõige rohkem vähendada digitaalset jalajälge kui neile on tekitatud selle läbi kahju.

Küsitluses osalenud on hetkel rohkem nõus usaldama tasulisi lahendusi kui vabavara digitaalse jalajälje vähendamiseks, kuigi vabavaralistel lahendusel on kasutajal võimalik tarkavara toimimist jälgida ja teha sellese muudatusi. Selliseid omadused tasulistel lahendustel reeglina puuduvad, ning kasutajad võivad sattuda arendustiimi eksituse ohvriks. Seega on toimumas jää murenemine ehk tasapisi hakatakse aru saama omandvara probleemidest ning aina rohkem on hakatud usaldama vabavara.

Summary

In this bachelor's thesis, the author explained what a digital footprint is, and the meaning of open source software. A digital footprint is a collection of data which exists due to a user's activities in the digital world, which can be associated with a certain user. Open source software is any software, which is free to use, and with an open source. In this thesis the author found the answers to all of the stated questions.

This bachelor's thesis talks about the possible ways to acquire info about the user and which type of info, while highlighting cookies, browsers along with monitoring a devices fingerprint and location. All of which create a digital footprint, which can be tied to the user themselves, and acquire information, like for example, the user's approximate location, personal interests and hobbies, usernames and passwords, age, e-mail address, name, photograph or health.

The author introduced the reader to the ways on how to reduce one's digital footprint with the use of different open source software, like the VPN service provider OpenVPN. Another way to reduce one's digital footprint is by encrypting data using open source software like GNU Privacy Guard or Veracrypt and by using the Tor browser. Web browsers come with free add-ons, which also help reduce a user's digital footprint, like HTTPS Everywhere, AdBlock Plus, Disconnect, NoScript, ScriptSafe and also Privacy Badger. Also user can switch operating systems for more security and privacy focused one.

In this bachelor's thesis the author carried out a survey, where the author found that the surveys participants are on average extremely cautious and don't give out information. The author concluded that the participants knew the definition of digital footprint, and what it could consist of. The participants are worried about their privacy on the internet. Overall the participants were aware, that their digital footprint could be contained, and knew some of the well-known methods on how to do so.

The survey's participants had more trust in the government, rather than Companies with their digital footprint, and were more concerned about less-known companies taking interest in their digital footprint. The leading motivation for the participants to use digital footprint reducing methods, is the ease of doing so and previously caused harm due to the user's digital footprint.

The majority of the survey's participants were willing to trust non open source software more than open source software for reducing their digital footprint, despite open source software having the option for the user to keep an eye on the software, and make changes to it. Non free open source software usually lacks the option to do so, and the user could get end up as a victim to a development team's mistake. Currently more people are becoming aware of the downsides of non-open source software, and towards open source software has started to grow.

Kasutatud kirjandus

1. About Adblock Plus. (kuupäev puudub). Adblock Plus. Loetud 18. märts 2016 aadressil https://adblockplus.org/en/about
2. About Device Fingerprint/Deviceprint. (kuupäev puudub). Darkwavetech. Loetud 20. veeburar 2016 aadressil http://darkwavetech.com/device_fingerprint.html
3. About this Add-on (27.04.2016). BetterPrivacy. Loetud 27. aprill 2016 aadressil https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
4. Ads Take a Step Towards "HTTPS Everywhere". (17.04.2015). Google Security Blog. Loetud 18. märts 2016 aadressil https://security.googleblog.com/2015/04/ads-take-step-towards-https-everywhere.html
5. Browser Hygiene: The Importance of Clearing Cache and Cookies. (kuupäev puudub). Loetud 23. aprill 2016 aadressil http://helpcenter.verticalresponse.com/articles/VR2/Browser-Hygiene-The-Importance-of-Clearing-Cache-and-Cookies
6. Clean Your System and Free Disk Space. (kuupäev puudub). Bleachbit. Loetud 23. aprill 2016 aadressil https://www.bleachbit.org/
7. Data Encryption in Transit Guideline. (kuupäev puudub). Berkeley. Loetud 24. märts 2016 aadressil https://security.berkeley.edu/data-encryption-transit-guideline
8. Disconnect. (15.01.2015). Disconnect. Loetud 6. märts 2016 aadressil https://github.com/disconnectme/disconnect
9. Disconnect. (kuupäev puudub). Disconnect. Loetud 18. märts 2016 aadressil https://disconnect.me/help#subdesktop-browser-extensions
10. Hansen, R, J. 2015. GnuPG Frequently Asked Questions. Loetud 26. märts 2016 aadressil https://www.gnupg.org/faq/gnupg-faq.txt
11. Hoffman, C. (2014). HTG Explains: What is HTTPS and Why Should I Care?. Loetud 20. märts 2016 aadressil: http://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/
12. How does third-party ad serving work? (kuupäev puudub). Allaboutcookies. Loetud 5. märts 2016 aadressil http://www.allaboutcookies.org/ad-serving/
13. How nsa proof are vpn providers?. (10.2013). Torrentfreak. Loetud. 4. märts 2016 aadressil https://torrentfreak.com/how-nsa-proof-are-vpn-providers-131023/

14. How to protect against device fingerprinting. (2014). Device fingerprinting Demo. Loetud 20. veeburar 2016 aadressil http://fingerprinting.comyr.com/
15. How Virtual Private Networks Work. (13.10.2008). Cisco Loetud. 5. märts 2016 aadressil http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html
16. Idrassi, M. (14.11.2014). Veracrypt Introduction. Loetud 27. märts 2016 aadressil https://veracrypt.codeplex.com/wikipage?title=Introduction
17. Inception. (kuupäev puudub). Torproject. Loetud 5. märts 2016 aadressil https://www.torproject.org/about/torusers.html.en
18. Introduction. (20.03.2016). Openvpn Loetud 4. märts 2016 aadressil https://community.openvpn.net/openvpn/wiki/HOWTO#Introduction
19. Is your browser safe against tracking? (kuupäev puudub). Panopticlick. Loetud 20. märts 2016 aadressil https://panopticlick.eff.org/
20. Licenses. (09.02.2016). Gnu. Loetud 6. veeburar 2016 aadressil https://www.gnu.org/licenses/licenses.html
21. Location tracking. (kuupäev puudub). American Civil Liberties Union. Loetud 4. märts 2016 aadressil https://www.aclu.org/issues/privacy-technology/location-tracking
22. Lookup IP Address Location. (kuupäev puudub). Whatismyipaddress. Loetud 4. märts 2016 aadressil http://whatismyipaddress.com/ip-lookup
23. Networkadvertising. (Kuupäev puudub). Opt Out of Interest-Based Advertising. Loetud 6. märts 2016 aadressil: http://www.networkadvertising.org/choices/
24. Noscript. (kuupäev puudub). Noscript. Loetud 18. märts 2016 aadressil https://noscript.net/features
25. Noscript faq. (kuupäev puudub). Noscript. Loetud 18. märts 2016 aadressil https://noscript.net/faq#qa3_3
26. Not all issues are Adblock Plus bugs. (kuupäev puudub). Adblock Plus. Loetud 18. märts 2016 aadressil https://adblockplus.org/en/bugs
27. OpenVPN Community Software. (kuupäev puudub). OpenVPN Community. Software Loetud 4. märts 2016 aadressil https://openvpn.net/index.php/open-source/335-why-openvpn.html
28. Prabhu, V. (2015). 3 Search Engines that don't track user data like Google. Loetud 20. märts 2016 aadressil: http://www.techworm.net/2015/10/worried-about-privacy-forget-google-and-try-these-search-engines.html

29. Privacy Badger FAQ. (kuupäev puudub). Privacy Badger. Loetud 24. märts 2016 aadressil https://www.eff.org/privacybadger
30. Qubes OS. (kuupäev puudub). Tour. Loetud 26. aprill 2016 aadressil https://www.qubes-os.org/tour/
31. Rouse, M. (11.2014). Encryption. Loetud 26. märts 2016 aadressil http://searchsecurity.techtarget.com/definition/encryption
32. Scriptno. (6.09.2011). ScriptSafe. Loetud 18. märts 2016 aadressil https://code.google.com/archive/p/scriptno/
33. Tails. (kuupäev puudub). About. Loetud 26. aprill 2016 aadressil https://www.qubes-os.org/tour/
34. The Open Source Definition. (22.03.2007). Open Source Initiative. Loetud 20. veeburar 2016 aadressil https://opensource.org/osd
35. Tor: Overview. (kuupäev puudub). Torproject. Loetud 4. märts 2016 aadressil https://www.torproject.org/about/overview.html.en
36. Use of Cookies on About Cookies Website (kuupäev puudub). Aboutcookies. Loetud 6. märts 2016 aadressil http://www.aboutcookies.org/legal-notices/cookies/
37. Watching Them Watching Me: Browser Extensions'Impact on User Privacy Awareness and Concern. (2016). Torproject. Loetud 8. aprill 2016 aadressil https://www.internetsociety.org/sites/default/files/blogs-media/watching-them-watching-me-browser-extensions-impact-on-user-privacy-awareness-and-concerns.pdf
38. What is a cookie? (kuupäev puudub). Allaboutcookies. Loetud 5. märts 2016 aadressil http://www.allaboutcookies.org/cookies/
39. What is a Digital Footprint. (22.03.2007). Internetsociety. Loetud 7. veeburar 2016 aadressil http://www.internetsociety.org/sites/default/files/flash/What_is_a_Digital_Footprint/presentation_content/external_files/What_is_a_Digital_Footprint.pdf
40. What is Free Software? (11.04.2016). Gnu. Loetud 13. aprill 2016 aadressil https://www.gnu.org/
41. Why is Tor so slow?. (kuupäev puudub). Torproject. Loetud 4. märts 2016 aadressil https://www.torproject.org/docs/faq.html.en#WhySlow
42. Why you should use a VPN. (kuupäev puudub). Perfect privacy Loetud. 4. märts 2016 aadressil https://www.perfect-privacy.com/why-vpn/

43. Wigmore, I. (05.2014). Digital footprint. Loetud 7. veeburar 2016 aadressil http://whatis.techtarget.com/definition/digital-footprint

Lisad

Lisa1

Küsimustik

Digitaalne jalajälg

Olen Risto Ruuben ning olen lõpetamas Tallinna ülikoolis informaatika eriala. Seoses lõputööga olen läbi viimas uuringut teemal "Digitaalse jalajälje vähendamine vabavara abil", mille eesmärk on anda ülevaade kui teadlikud ollakse privaatsusest internetis ja kas kasutatakse meetmeid selle kaitseks. Kõik küsitluses osalenud jäävad anonüümseteks ning vastamiseks kulub orienteeruvalt kuni 10 minutit.

* Kohustuslik

1. **Digitaalne jalajälg on:** *
Märkige ainult üks ovaal.

- ◯ jälg, mis on digitaalne
- ◯ kõikvõimalik informatsioon, mida inimene on enda kohta internetti maha jätnud
- ◯ internetiteenus, mis jätab maha jälje
- ◯ Ei oska vastata

2. **Digitaalset jalajälge saab piirata.** *
Millisel määral nõustud antud väitega?
Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

3. **Internetti kasutades jääb maha digitaalne jalajälg, mille alusel on võimalik varastada kasutaja identiteet.** *
Millisel määral nõustud antud väitega?
Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

4.

Tunnen muret oma privaatsuse pärast internetis. *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

5.

Millist infot on võimalik internetist kasutaja kohta saada? *

Märkige kõik sobivad.

- [ ] Füüsiline asukoht
- [ ] Isiklikud hobid ja huvid
- [ ] Kasutajanimed ning salasõnad
- [ ] Vanus
- [ ] E-postiaadress
- [ ] Nimi
- [ ] Tervisega seotud info
- [ ] Foto
- [ ] Ei oska vastata
- [ ] Muu: _____

6.

Millisel viisil on võimalik kasutaja kohta infot koguda? *

Märkige kõik sobivad.

- [ ] Veebilehitseja küpsised
- [ ] Otsingumootorid
- [ ] Mobiilseadmete rakendused
- [ ] Seadme sõrmejälg
- [ ] Erinevad veebilehed
- [ ] Rakendused
- [ ] Veebilehitseja lisand
- [ ] Sotsiaalvõrgustik
- [ ] Pahavara kasutades
- [ ] Ei oska vastata
- [ ] Muu: _____

7.

Kuidas on võimalik kahju tekitada kogutud andmetega? *

Märkige kõik sobivad.

- [ ] Sihitud reklaamid
- [ ] Identiteedivargus
- [ ] Rämpspostitajad
- [ ] Rahaline kahju
- [ ] Füüsiline kahju
- [ ] Andmete hävimine või avalikuks tulek
- [ ] Jälitamine, manipuleerimine
- [ ] Ei oska vastata
- [ ] Muu: .....

8.

Olen nõus jagama oma digitaalset jalajälge kasu saamise eesmärgil teiste asutustega nagu näiteks valitsused ning erafirmad? *

Kasu saamine: näiteks pakutakse tasuta teenust.

Märkige ainult üks ovaal rea kohta.

	1	2	3	4	5	Ei oska öelda
Valitsus	◯	◯	◯	◯	◯	◯
Erafirma	◯	◯	◯	◯	◯	◯

9.

Milliste meetodite abil on võimalik digitaalset jajajälge vähendada? *

Märkige kõik sobivad.

- [ ] Virtuaalne privaatvõrk (VPN)
- [ ] Puhverserver (proxy)
- [ ] Veebilehitseja turvalisust tõstev lisand
- [ ] Veebilehitseja privaatne režiim
- [ ] Anonümiseerija (nt Tor)
- [ ] Ajutiste failide kustutamine
- [ ] Andmete krüpteerimine
- [ ] Turvalisema tarkvaraplatvormi valik
- [ ] Ei oska vastata
- [ ] Muu: .....

10. **Kui efektiivne on antud lahendus on digitaalse jalajälje vähendamiseks?** *

Märkige ainult üks ovaal rea kohta.

	1	2	3	4	5	Ei oska vastata
Virtuaalne privaatvõrk (VPN)						
Puhverserver (proxy)						
Veebilehitseja turvalisust tõstev lisand						
Veebilehitseja privaatne režiim						
Anonümiseerija (nt Tor)						
Ajutiste failide kustutamine						
Andmete krüpteerimine						
Kasutusharjumuste muutmine						
Turvalisema tarkvaraplatvormi valik						

11. **Kui oled kasutanud varem mõnda meetodit, siis millist ning mis oli peamine põhjus?**

12. **Millisel määral nõustud, et järgmised operatsioonisüsteemid tagavad võimalikult väikese digitaalse jalajälje?** *

Märkige ainult üks ovaal rea kohta.

	1	2	3	4	5	Ei oska vastata
Microsoft Windows						
Linux						
Apple OS X (Mac)						
Android						
iOS						

13. **Millisel määral usaldad tasulist tarkvara rohkem kui vabavara digitaalse jalajälje vähendamiseks?** *

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu						nõustun täielikult

14.

Kui oled muutnud kasutusharjumusi siis millised? *

Märkige kõik sobivad.

- [ ] Veebilehitseja privaatse režiimi kasutuselevõtt
- [ ] Alternatiivsete otsingumootorite kasutus
- [ ] Kasutan registreerimisel võltsandmeid
- [ ] Turvalisem e-postiteenus
- [ ] Sotsiaalvõrgustiku seadete muutmine või nendest loobumine
- [ ] Isilkliku info jagamisega internetis ettevaatlikum
- [ ] Olemasoleva operatsioonisüsteemi vahetamine turvalisema vastu
- [ ] Andmete krüpteerimine
- [ ] Ei jäta kasutajanimesid, salasõnasid veebilehitsejale enam meelde
- [ ] Ei ole muutnud
- [ ] Muu: .....

15.

Mind motiveerib erinevaid digitaalse jalajälje vähendamiseks mõeldud meetmed kasutusele võtma see kui nende kasutamine oleks võimalikult kerge. *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

16.

Tunnen muret kui vähetuntud või tuntud asutus huvitub minu digitaalse jalajälje vastu. *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal rea kohta.

	1	2	3	4	5
Vähetuntud	◯	◯	◯	◯	◯
Tuntud	◯	◯	◯	◯	◯

17.

Püüan vähendada digitaalset jalajälge kui mulle on tekitatud kahju. *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

18. **Mis motiveeriks vähendama enda digitaalset jalajälge?** *

Märkige kõik sobivad.

- [ ] Isiklik kahju
- [ ] Teadmine, et isiklike andmeid töödeldakse ettevõtte kasu eesmärgil
- [ ] Teadmine, et digitaalse jalajälge abil suunatakse sinu mõttemaailma
- [ ] Riigiasutuse pilt sinu huvidest
- [ ] Sihitud reklaamid
- [ ] Puudub motivatsioon digitaalse jalajälje vähendamiseks
- [ ] Muu: _____

19. **Privaatsust internetis ei ole olemas.** *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

20. **Olen nõus muutma oma kasutusharjumusi vähendamaks digitaalset jalajälge.** *

Millisel määral nõustud antud väitega?

Märkige ainult üks ovaal.

	1	2	3	4	5	
üldse ei nõustu	◯	◯	◯	◯	◯	nõustun täielikult

21. **Asutus, kus hetkel töötad/õpid?** *

Märkige ainult üks ovaal.

- ◯ haridusasutus
- ◯ kohalik omavalitsus
- ◯ eraettevõte
- ◯ Ei soovi avaldada
- ◯ Muu: _____

22. **Sugu?** *

Märkige ainult üks ovaal.

- ◯ Naine
- ◯ Mees

23.

Vanus? *

Märkige ainult üks ovaal.

- ◯ alla 16
- ◯ 17-26
- ◯ 27-39
- ◯ 40-59
- ◯ üle 60