TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Johan Skytte poliitikauuringute instituut

Krista Valli

KOOLINOORTE HARJUMUSED PAROOLIDE LOOMISEL JA KASUTAMISEL NING VÕIMALUSED TURVALISEMATE VALIKUTE SUUNAS NÜGIMISEKS

Juhendaja: Leonore Riitsalu, PhD

Kaasjuhendaja: Madis Raaper, MA

Tartu 2019

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite seisukohad, ning kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..

/*töö autori allkiri*/

Kaitsmine toimub ……../*kuupäev*/ kell ……../*kellaaeg*/ ……../*aadress*/ auditooriumis ……./*number*/.

Retsensent: …….. /*nimi*/ (……./*teaduskraad*/), …….. /*amet*/

Magistritöö autor soovib tänada oma juhendajaid Leonore Riitsalu ja Madis Raaper-it pühendatud aja, töö ning eriti kannatlikkuse eest.

LÜHIKOKKUVÕTE

Tänapäeva infoühiskonnas alustavad lapsed aina nooremana arvuti ja interneti kasutamist, mis pakuvad võimalusi silmaringi arendamiseks ja vaba aja veetmiseks. Kuid lisaks positiivsetele külgedele, ohustavad noori ka erinevad küberriskid.

Selleks, et end nende ohtude eest kaitsta, peavad lapsed nendest teadlikud olema ning oskama internetis võimalikult turvaliselt navigeerida.

Üheks lihtsamaks lähtepunktiks on tugev parool ning selle turvalisuse hoidmine. Käesolev magistritöö uurib koolinoorte harjumusi paroolide loomisel ning kasutamisel. Selleks on autor läbi viinud küsitluse erinevates Eesti koolides koolides 9-16aastaste õpilasete hulgas.

Autori poolt läbi viidud küsitlusest selgus, et koolinoored on enamasti teadlikud ohtudest, mis kaasnevad nõrga parooli kasutamisel. Samuti on neile tuttavad soovitused, milline peaks turvaline salasõna olema. Sellest hoolimata valivad nad tihti siiski nõrga parooli ning ei uuenda seda regulaarselt.

Lahendusena pakub autor välja käitumisökonoomika teadmiste abil koolinoorte nügimist turvalisemate valikute suunas. Selleks on analüüsitud erinevaid siiani kasutatud nügimisstrateegiaid ning uuringuid. Samuti on ettepanekuks kasutada ära käitumisökonoomika teadmised ning võimalused koolinoorte teadlikkuse tõstmiseks tugevate paroolide koostamisel ning nende turvalisuse hoidmisel, ja seeläbi muuta selline tegevus harjumuseks aina nooremas eas.

Koolinoorte paroolide loomist ning nende turvalisuse hoidmist on uuritud vähe ning Eestis pole senini ühtegi sellekohast uuringut avaldatud. Seega on käesoleva magistritöö üheks ajendiks selle tühimiku täitmine ning sisend edasiste uuringute läbi viimiseks.

SISUKORD

SISSEJUHATUS

2015. aastal avaldatud PISA *(Program for International Student Assessment)* uuringu andmete kohaselt teevad Eesti õpilased arvutitega ja internetiga tutvust aina nooremas eas. 48% küsitletud õpilastest hakkab arvutit kasutama 6 aastaselt või varem. Internetti on kasutanud neist 32%. Küsitlusele vastanud Eesti 15-aastastest kooliõpilastest on kodus arvuti 79%-l, mida nad saavad koolitööde tegemiseks kasutada ja 89%-l õpilastest on kodus internetiühendus[1].

Kuigi internet pakub õpilastele tänapäeval palju võimalusi silmaringi avardamiseks ning aja veetmiseks, varitsevad seal neid ka erinevad ohud. Näiteks võivad lapsed tahtmatult ning enda ebaturvalise käitumise ehk halva küberhügieeni tõttu, sattuda ebatsensuursetele veebilehekülgedele, suhelda pahatahtlike võõrastega, avaldada isiklikke andmeid ning kogeda küberkiusamist[2].

Nii rahvusvahelisel kui ka Euroopa Liidu tasandil ei ole küberkiusamist üheselt defineeritud[3]. Küll aga on välja toodud faktoreid, mis on küberkiusamise korral alati esindatud. Nendeks on erinevate tehniliste seadmete (nt mobiiltelefon, tahvelarvuti, veebikaamera jne) kasutamine. Näiteks toimub e-kirjade, SMS-ide jms kaudu sõimamine ja ähvardamine. Samuti võib kiusamine aset leida erinevates portaalides ja suhtluskeskkondades alandavate kommentaaride kirjutamise ja/või mõnitamise näol[4]. Üks levinumaid küberkiusamise viise on libakontode tegemine, kuhu pannakse üles halvustavat, ebaõiget, tihti ka ebatsensuurset informatsiooni kiusatava kohta või võetakse üle kiusatava konto[5], mis on nõrga parooli või selle jagamise tulemusel lihtsam. Suur osa küberkiusamise ohvritest on käitunud internetis ebaturvaliselt ning näiteks jaganud oma

---

[1]Täht, K. (2015) Õpilaste eluga rahulolu ning sellega seotud tegurid PISA 2015 uuringu näitel, Tartu Ülikool. Kättesaadav arvutivõrgus: https://www.innove.ee/wp-content/uploads/2017/11/%C3%95pilaste-rahulolu-PISA-2015.pdf (09.02.2019)

[2]Catalina, G., jt. (2014) Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet The risks faced by adolescents on the Internet: minors as actors and victims of the dangers of the Internet. *Revista Latina de Comunicación Social*, 69, lk 462-485.

[3]Euroopa Parlament, (2016) Cyberbullying among Young People. Kättesaadav arvutivõrgus: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf (28.10.2018)

[4]Garaigordobil, M., Martínez-Valderrey, V. (2014) Effect of Cyberprogram 2.0 on Reducing Victimization and Improving Social Competence in Adolescence. *Revista de Psicodidáctica,* 19, 2, lk 289-305.

[5]Peled, Y. (2019) Cyberbullying and its influence on academic, social, and emotional development of undergraduate students. Heliyon, 5, 3.

parooli teistega[6]. EU Kids Online'i uuringust selgub, et kuna Eestis on 9–16aastased lapsed ühed suurimad internetikasutajad Euroopas, siis on nad ka suurema tõenäosusega kokku puutunud *online*-riskidega[7], mille alla kuulub muuhulgas küberkiusamine. Kui eelmainitud raportis oli aastal 2010 11-16aastaste laste seas tõenäosus küberkiusamisega kokku puutuda 7%, siis 2014. aastal oli see tõusnud 12 protsendini. Tegelikkuses on see arv ilmselt suurem ning kasvab aastatega.

Küberohtude vältimiseks ei piisa vaid tehnilistest lahendustest, turvalisuse hoidmisel on kõige olulisem siiski inimene ise ning hea küberhügieen. Küberturvalisuse hoidmiseks ja parandamiseks on tähtis mõista inimeste motivatsiooni ning mõjutajaid, mis loovad nende harjumused ja seeläbi ka küberhügieeni[8], mille üheks osaks on tugev parool ning selle turvalisuse hoidmine[9].

Selleks, et kaitsta lapsi küberkiusamise eest, tuleks teada saada nende käitumismaneeridest internetis ning suunata neid tegema turvalisemaid valikuid. Siinkohal tuleb kasutusele käitumisökonoomika üks vahenditest – „nügimine", mille eesmärgiks on lihtsate muudatuste abil mõjutada meid ümbritsevas maailmas inimeste poolt tehtavaid otsuseid ja käitumist neile endile soodsas suunas. Mõjutamine toimub käskude, keeldude, sunni ja liigsete kuludeta[10]. Antud teooria on ka käesoleva magistritöö lähtepunktiks.

Käitumisökonoomika uurib, kuidas inimesed teevad otsuseid ning mis mõjutab nende valikuid[11]. Ühendkuningriigi valitsuses käitumisökonoomikaga tegelev organisatsioon *The Government Office for Science* on oma raportis öelnud, et küberturvalisuse

---

[6]Hinduja, S., Patchin, J. W. (2014). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Thousand Oaks, CA: Corwin.

[7]Helsper, E. J., Kalmus, V., jt. (2013) Country classification: opportunities, risks, harm and parental mediation. Kättesaadav arvutivõrgus: http://eprints.lse.ac.uk/52023/1/Helsper_Country_classification_opportunities_2013.pdf (28.10.2018)

[8]Clarke, N., Furnell, S. (2012) Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31, 8, lk 983-988.

[9]Oravec, J. A. (2017) Emerging "cyber hygiene" practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. 2017 IEEE International Professional Communication Conference (ProComm).

[10]Strauss-Raats, P. (2013) Kuidas töötajaid soodsas suunas mõjutada? Tööinspektsiooni infokiri. Kättesaadav arvutivõrgus: https://www.ti.ee/fileadmin/user_upload/failid/dokumendid/Meedia_ja_statistika/Teavitustegevus/Infokirjad/2013/infokiri_nr_28/detsember2013_tookeskkond1.pdf (29.10.2018)

[11]Mullainathan, S., Thaler, R. (2015) Behavioral Economics. International Encyclopedia of the Social & Behavioral Sciences (Second Edition), lk 437-442.

parandamine läbi käitumisökonoomia vajab kindlasti edasist uurimist[12], mis näitab, et tegemist on uudse lähenemisega küberturvalisuse valdkonnas.

Küberturvalisuse ning küberteadlikkuse teema on üheks prioriteediks nii riigi kui ka Euroopa Liidu tasandil. Majandus- ja Kommunikatsiooniministeerium on „Küberturvalisuse strateegia 2019-2022“ dokumendis rõhutanud, et ühiskonnas on siiani küberturvalisuse alane teadlikkus ebapiisav ning eesmärgiks seatakse iga koolilõpetaja baasteadmiste omandamist küberohtudega toimetulekuks[13]. Samuti on Justiitsministeeriumi poolt koostatud eelnõus „Kriminaalpoliitika põhialused aastani 2030“ välja toodud soov, et eranditult kõik lasteaiad, üldharidus- ja kutsekoolid võtaksid 2030. aastaks kasutusele tõenduspõhise kiusamisvastase programmi, mis peab hõlmama ka küberkiusamist[14]. Euroopa Liidu suunis on, et iga liikmesriik peab küberteadlikkuse tõstmisse suhtuma täie tõsidusega[15].

Antud uurimistöö eesmärk on uurida koolinoorte harjumusi paroolide loomisel ning kasutamisel. Samuti analüüsib autor käitumisökonoomika kasutamise võimalusi, mis suurendaks koolinoorte teadlikkust küberturvalisust ning seeläbi vähendada küberkiusamise ohvriks langemise riski. Käesoleva töö raames on koolinoor 9 kuni 16-aastane.

Käitumisökonoomia kasutamise võimalusi koolinoorte küberturvalisuse osas varasemalt Eestis uuritud ei ole. Seega annab käesolev uurimistöö uut infot käitumisökonoomia rakendamise võimalustest, millest võiks olla abi küberkiusamise vähendamisel ning koolinoorte teadlikkuse tõstmisel.

Kuna küberturvalisus on lai valdkond ning lähtudes uurimistöö mahu piirangutest, keskendub käesolev magistritöö koolinoorte paroolide loomise ning kasutamise praktikale ning sellega seonduvate riskide teadlikkusele.

---

[12]Government Office for Science. (2014). Using behavioural insights to improve the public' s use of cyber security best practices. Kättesaadav arvutivõrgus: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (29.10.2018).
[13]Majandus- ja Kommunikatsiooniministeerium. (2018). Küberturvalisuse strateegia 2019-2022.
[14]Justiitsministeerium. (2018). Kriminaalpoliitika põhialused aastani 2030. Eelnõu. Seletuskiri.
[15]Euroopa Komisjon. (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

Selleks, et saavutada antud töö eesmärk, on püstitatud järgmised uurimisküsimused:

1. Millised on koolinoorte harjumused paroolide loomisel ja kasutamisel?
2. Millised vahendeid on varasemalt kasutatud, et nügida inimesi turvalisemate paroolide suunas?

Käesolev töö koosneb sissejuhatusest, teoreetilise raamistiku moodustava kirjanduse ülevaatest, metoodika peatükist, autoripoolsete järelduste peatükist ning kokkuvõttest. Magistritöö teoreetilise osa esimeses pooles selgitatakse käitumisökonoomikas kasutatud nügimise olemust. Samuti keskendutakse kübervaldkonna erinevatele mõistetele ning antakse ülevaate strateegiatest, mis on loodud salasõnade turvalisemaks muutmiseks.

Töö teine osa keskendub kübervaldkonna erinevatele mõistetele ning aspektidele, mis on antud uurimise jaoks olulised ning selgitab, kuidas paroolide turvalisus on kübervaldkonnaga seotud. Samuti toob autor välja seni läbi viidud uuringud inimeste paroolide loomise ning kasutamise harjumuste kohta. Samas peatükis on tutvustatud ka, milliseid vahendeid on kasutatud inimeste turvalisemate paroolide suunas nügimiseks.

Kolmas peatükk annab ülevaate antud magistritöö eesmärgi saavutamiseks valitud uurimismetoodikast, uurimuse valimist ning andmete analüüsi selgitusest.

Magistritöö neljas osa analüüsib koolinoorte seas tehtud küsitluse tulemusi, mille alusel kaardistati nende harjumused ning teadlikkus paroolide loomisel ja kasutamisel. Samuti tuuakse välja järeldused ja antakse autoripoolsed soovitused olukorra parandamiseks.

Magistritöö lisas esitatakse ankeetküsitluse küsimused.

Magistritöö vormistamise aluseks on võetud Tartu Ülikooli Johan Skytte poliitikauuringute instituudi kirjalike tööde koostamise ja vormistamise juhend[16].

[16]Tartu Ülikooli Johan Skytte poliitikauuringute instituudi kirjalike tööde koostamise ja vormistamise juhend. Kättesaadav arvutivõrgus: https://skytte.ut.ee/et/oppimine/oppematerjalid-juhendid-1 (03.01.2019).

1. KÜBERHÜGIEEN JA PAROOLIDE TURVALISUS

Käesoleva peatükk on jagatud kolmeks alapeatükiks.

Esimene alapeatükk selgitab antud töös kasutatud kübervaldkonna termineid. Eelkõige keskendub autor küberhügieeni defineerimisele, kuna see on uurimistöö eesmärgist lähtudes olulisel kohal. Samuti toob autor välja, kuidas on paroolide loomine ning kasutamine seotud küberhügieeniga. Kasutatud on nii Eesti kui teiste riikide õigusakte ja küberturvalisuse strateegiaid ning eesti- ja inglise keelseid teaduskirjanduse väljaandeid ja teadusartikleid, kus on antud mõistet selgitatud.

Teine alapeatükk toob välja paroolide loomise ning kasutamisega seotud levinumad probleemid. Samuti antakse ülevaade nende probleemide vähendamise headest tavadest ja parimatest praktikatest.

Kolmandas alapeatükis annab autor ülevaate senini läbi viidud lastega seotud uuringutest, mis on seotud paroolide loomise ning nende kasutamisega.

1.1. Küberhügieeni mõiste

Andmekaitse ja infoturbe leksikoni kohaselt on eesliite *küber-* vaste „küberneetiline“, mis vastupidiselt laialt levinud arusaamale, ei tule sõnast küberneetika, vaid küberpunk. Küberpunk kujutab endast tulevikuühiskonda, mis on üle võetud arvutite poolt[17].

Kübervaldkonna mõistete puhul kasutatakse eesliidet *küber-*, mis on Majandus- ja Kommunikatsiooniministeeriumi poolt defineeritud kui eesliidet, mis tähistab võrgu- ja infosüsteeme[18].

2018. aastal vastu võetud Eesti Küberturvalisuse seadus ei defineeri eraldi eesliidet *küber-*, vaid on selgitatud küberintsidendi mõistet kui süsteemis toimuvat sündmust, mis

[17]Andmekaitse ja infoturbe leksikon. Kättesaadav arvutivõrgus: https://akit.cyber.ee/term/9143 (24.03.2019).
[18]Majandus- ja Kommunikatsiooniministeerium. (2018). Küberturvalisuse strateegia 2019-2022.

ohustab või kahjustab süsteemi turvalisust.[19]. Seaduse kohaselt võrdub *küber* mõistega *süsteem*, mis on välja toodud järgnevalt:

„**Võrgu- ja infosüsteem** – elektroonilise side võrk elektroonilise side seaduse § 2 punkti 8 tähenduses, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringuga või edastatakse eelnimetatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks;“

Tabelis 1 on välja toodud Majandus- ja Kommunikatsiooniministeeriumi dokumendis Küberturvalisuse strateegia 2019-2022 leitav uuendatud kübervaldkonna terminite loetelu.

Tabel 1. Terminid ja definitsioonid 2018

Nr.	Termin	Definitsioon	Kommentaar
Põhimõisted			
1.	**Küber-**	Eesliide, mis tähistab võrgu- ja infosüsteeme.	Näiteks küberturvalisuse seaduse mõistes on võrgu- ja infosüsteem elektroonilise side võrk, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub digitaalsete andmete töötlemine.
2.	**Küberturvalisus**	Seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest.	Inglise keeles defineeritakse antud terminit (cybersecurity) samuti turvalisuse tagamisena. Eesti keeles kasutatakse sellises kontekstis terminit „küberturve“.

[19]Küberturvalisuse seadus. -RT I, 22.05.2018, 1.

3.	**Küberturve**	Võrgu- ja infosüsteemide turvalisuse tagamine.	Teiste sõnadega on küberturve meetmete rakendamine küberturvalisuse saavutamiseks.
4.	**Küberjulgeolek**	Seisund, kus riigi julgeolek on kaitstud võrgu- ja infosüsteemide kaudu tekkivate ohtude eest.	Eesti keeles on kasutusel kaks mõistet – turvalisus ja julgeolek. Inglise keeles sellist vahet ei tehta (security). Seetõttu võiks „küberjulgeoleku“ tõlge olla inglise keeles „National Cybersecurity“.
Olulisemad küber- eesliite abil moodustatud mõisted			
5.	**Küberhügieen**	Üksikisiku või organisatsiooni elementaarsed toimingud vältimaks võrgu- ja infosüsteemide kaudu tekkivate ohtude realiseerumist.	

Allikas: Majandus- ja Kommunikatsiooniministeerium[20]

Lisaks mõistete defineerimisele on oluline ka eristada, kuidas küberoskuste omandamine sõltub inimese oskuste asemest ning kuidas on liigitatud küberhügieen:

- **Kodaniku tase:** küberhügieen (elementaarne turvameetmete oskus on osa tavapärasest digipädevusest, näiteks hea ja turvalise salasõna valimine);
- **Professionaali tase:** küberturvalisus (IT spetsialisti tase, näiteks kaitstakse asutusi küberrünnakute eest);
- **Eksperdi tase:** küberkaitse/-sõda (küberruum on viies ruum, kus toimub kaitsetegevus lisaks maale, merele, õhule ja kosmosele).[21]

Eelnevast lähtuvalt on koolinoorte paroolide loomise ning kasutamise harjumused osa küberhügieenist.

[20]Majandus- ja Kommunikatsiooniministeerium. (2018). Küberturvalisuse strateegia 2019-2022.
[21]Lorenz, B., Kikkas, K. (2019). Digitaalne kirjaoskus infoühiskonnas. Kättesaadav arvutivõrgus: https://entk.ee/wp-content/uploads/2019/02/1-2-birgy-ja-kaido.pdf (01.04.2019).

Hea küberhügieeni praktika hulka kuulub muuhulgas:

- Tulemüüri kasutamine;
- Tundmatute allikate poolt saadetud manuste mitte avamine;
- Tugevate paroolide kasutamine ning nende mitte jagamine;
- Viirusetõrje kasutamine;
- Tarkvara regulaarne uuendamine;
- Kahtlaste veebilehekülgede mitte külastamine.[22]

Vastavalt käesolevas töös püstitatud eesmärgile, keskendub autor paroolide loomise ja kasutamisega seotud probleemidele, kuna erinevalt eelmainitud küberhügieeni praktikatest, on paroolide loomine ja kasutamine koolinoorte puhul enamasti igapäevane tegevus ning seetõttu on hooletu ning ebaturvalise paroolide kasutamise korral oht küberkiusamise ohvriks langeda tunduvalt suurem, kui muude küberhügieeni praktikate korral. Tulemüüride, viirusetõrjete ja tarkvarauuendustega on koolinoortel kokkupuuteid tunduvalt vähem.

Autori hinnangul on tugevate paroolide loomine ning nende turvalisuse hoidmine üheks inimese jaoks lihtsamini kontrollitavaks viisiks hea küberhügieeni tagamisel. See aga eeldab teadlikkust tugevate salasõnade koostamise põhimõtetest ning nende turvalisuse hoidmise viisidest.

1.2. Paroolide loomise ning kasutamise probleemid ja head tavad

Nagu Eesti Vabariigi president Kersti Kaljulaid oma kõnes Euroopa Kaitseagentuuri aastakonverentsil "Turvalisus digiajastul: Euroopa koostöö lisaväärtus" välja tõi, ei taga ainuüksi Euroopa Liidu loodud või ka siseriiklikud küberkaitse ning -strateegiate dokumendid inimeste ohutut navigeerimist internetist. Endiselt on siinkohal oluline üksikisik ning elementaarne küberhügieen[23].

[22]Cain, A. A. jt. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, lk 36-45.
[23]Kaljulaid, K. (2017). Keynote speech at the European Defence Agency Annual Conference "Security in the digital age: the added value of European cooperation". Kättesaadav

Parool on kõige sagedasem ning kasutajasõbralikum isiku autentimisviis internetis[24].

Üheks suurimaks probleemiks on parooli lihtsus selle kombinatsiooni mõttes. Juba aastaid on kõige levinumad salasõnad „123456“ ja „password“[25] (eesti keeles „parool“). Erinevate uuringute kohaselt on inimesed tegelikult teadlikud, milline peaks tugev parool olema, kuid erinevatel põhjustel kasutatakse tihti siiski nõrka[26].

Parooli koostamisel tuleks vältida sõnu, mille kirjapilt on otse sõnaraamatust võetud. Samuti ei tohiks see olla liiga lühike. Üldtuntud tava on, et parooli pikkus võiks olla vähemalt 8 tähemärki[27]. Mitmetes allikates soovitatakse aga vähemalt 12-kohalist salasõna. Isiklike andmete kasutamine salasõna koostamisel on suur turvarisk, kuna see lihtsustab parooli ära arvamist[28]. Soovitatav on kasutada kombinatsioone, mis koosneb erisuuruses tähtedest, numbritest ning sümbolitest. Kõige enam kasutatavad sümbolid paroolide koostamisel on ! ja @, kuna neid on klaviatuuril mugav sisestada[29]. Seega oleks soovitatav kasutada muid variante.

Tugev salasõna üksi ei kaitse kasutajat, kui kasutaja ei suuda seda meelde jätta ning kirjutab selle üles. Riski maandamiseks võiks kasutada tehnikat, mis kujutab endast meeldejääva lause sõnade esimeste tähtede kombineerimist muude sümbolite ja numbritega. Näiteks, kui võtta aluseks lause: „Kui mina alles noor veel olin, lapsepõlves mängisin...“, siis selle esimeste tähtede kombinatsiooniks tuleks „Kmanvolm“. Samuti tuleks lisada ka sümboleid ning numbreid. Pealtnäha tundub olevat suvaline tähtede

arvutivõrgus: https://www.president.ee/en/official-duties/speeches/13766-keynote-speech-at-the-european-defence-agency-annual-conference-qsecurity-in-the-digital-age-the-added-value-of-european-cooperationq-/index.html (13.03.2019)

[24]Denham, N., jt. (2016). Secure modular password authentication for the web using channel bindings. *International Journal of Information Security*, 15, 6, lk 597-620.

[25]The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius. Kättesaadav arvutivõrgus: https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705 (13.03.2019).

[26]Glassmann, M, Vandenwauver, M. (2009). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 3, lk 233-244.

[27]Infosüsteemide turvameetmete süsteem ISKE. M 2.11 Paroolide kasutamise reeglid. Kättesaadav arvutivõrgus: https://iske.ria.ee/8_03/ISKE_kataloogid/7_Kataloog_M/M2/M_2.11 (13.03.2019).

[28]Hainsalu, O. (2017). Kuidas valida hea parool, mis ei unune? *Digi*, 150, 7. Kättesaadav arvutivõrgus: https://dea.digar.ee/cgi-bin/dea?a=d&d=AKdigi201710.2.29.4 (13.03.2019).

[29]Shen, C. jt. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, 61, lk 130-141.

kombinatsioon, kuid kasutajale peaks see siiski lihtsalt meelde jääma, kuna tema jaoks on tegemist loogilise jadaga[30].

Sarnaseks praktikaks on ka väljendite täispikk kasutamine, asendades mõningad tähed numbrite ja sümbolitega. Kasutades juba eelpool mainitud lauset, võiks parool välja näha selline: „Ku1_m1n2_2ll3s_n0oR_v33l_0l1n%“[31].

Kuna inimesed ei suuda mitmeid paroole meeles pidada, siis on tavapärane, et erinevatel veebilehekülgedel kasutatakse samu salasõnu ning neid ei uuendata regulaarselt, mis omakorda suurendab andmete varguse ohvriks langemise tõenäosust[32].

Kokkuvõtvalt on eksperdid andnud paroolide loomisel ja kasutamisel järgmisi soovitusi:

- Mitte kasutada sõnaraamatust leitavaid fraase, kuna salasõna tuvastamise programmides on sõnaraamatu liides, mis võib vaste leida sekunditega;
- Mitte jagada teiste inimestega enda paroole, kuna see võimaldab konto kaaperdamist;
- Salasõna ei tohiks üles kirjutada, kui just ei olda kindel, et see on turvalises kohas ning teistele mitte leitav;
- Erinevatel kontodel peaks olema ka erinev salasõna. Vastasel juhul on ühe konto salasõna teada saamisel ka teised kontod haavatavad;
- Paroole tuleks regulaarselt vahetada. Soovitavalt kord kuus;
- Parool peaks olema vähemalt 8-kohaline tähtede, numbrite ning sümbolite kombinatsioon;
- Paroolide koostamisel peaks kasutama süsteemi, mis võimaldab seda paremini meelde jätta (vt näidet lk 11).[33]

Olles teadlik tugeva parooli loomise ning kasutamise põhimõtetest, saab inimene vähendada riski kokku puutuda küberohtudega. Kuigi teadmised on olulised, ei garanteeri

[30]Furnell, S. (2007). An assessment of website password practices. *Computers & Security*, 26, (7-8), lk 445-451.
[31]Goodin, D. (2012). Why passwords have never been weaker—and crackers have never been stronger. Ars Technica. Kättesaadav arvutivõrgus: https://arstechnica.com/information-technology/2012/08/passwords-under-assault/ (13.03.2019).
[32]Florencio, D., Herley, C. (2007). A Large-Scale Study of Web Password Habits. *The 16th international conference on World Wide Web*, lk 657-666.
[33]Furnell, S. (2001). Cybercrime: vandalizing the information society. *Web Engineering International Conference*, lk 8-16.

need turvalisust, kui neid ei rakendata või ei saa turvaline käitumine internetis harjumuseks. Seetõttu on autori hinnangul oluline tutvustada lastele eelmainituid printsiipe turvalise käitumise kinnistamiseks juba siis, kui nad esimest korda internetti kasutama hakkavad.

1.3. Ülevaade varasematest uurimustest

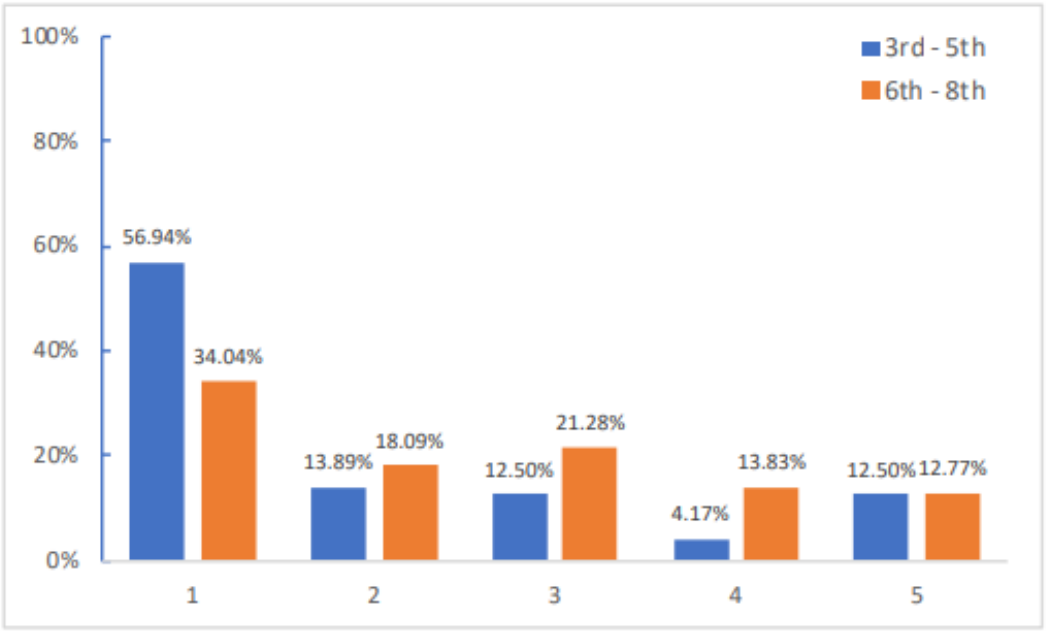
Varasemalt on läbi viidud uuringuid[34][35] saamaks teada täiskasvanute harjumusi paroolide loomisel ning nende turvalisuse hoidmisel, kuid laste seas on sellekohaseid uuringuid vähe läbi viidud või ole neid avalikustatud. Üheks põhjuseks võib olla see, et kuna uuringu sihtgrupiks on lapsed, kehtivad uuringu läbi viimisel ja avaldamisel ranged eetilised piirangud[36]. Samuti mängib aasta või kaks laste vanuses suurt rolli uuringu protsessis – näiteks võib noorema lapse tähelepanu olla erinevate faktorite korral kergemini hajutatav kui vanemal[37]. Seega on vajalik uuringuid läbi viia kitsastes vanusevahemikes, mis nõuab rohkem aega ning ressursse.

Aastal 2019 avaldatud kahes Ameerika Ühendriigi koolis läbi viidud uuringus jagati õpilased kahte vanusegruppi: 3.–5. klass, kuhu kuulusid lapsed vanuses 8-12, ning 6.-8. klass, mille vanusevahemik oli 11-15 aastat. Uuringu esialgsed tulemused näitasid, et kuigi koolinoored on teadlikud tugeva parooli vajalikkusest, valivad nad tihti siiski nõrga salasõna. Tulemused küll paranevad vanemate laste seas, kuid nõrga parooli osakaal on siiski suur. Noorema vanusegrupi puhul oli näha, et vanemad aitavad paroole välja mõelda või loovad neid lastele ise (69.32%)[38].

Joonisel 1 on välja toodud paroolide tugevusastmed 1-5 ning õpilaste prontsentide jaotus vastavalt nendele. Skaalal 1-5 vastab „1“ kõige nõrgemale ning „5“ kõige tugevamale paroolile. Kõige nõrgema tugevusastmega paroole esines noorema grupi laste seas

[34] Duggan, G. B., jt. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, 70, 6, lk 415-431.
[35]Chouseinoglou, O., jt. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, lk 83-93.
[36]Höysniemi, J., jt. (2003). Half-Day Tutorial: Evaluating Interactive Products for and with Children. *Human-Computer Interaction*, lk 1027-1028.
[37]Alexander, K., jt. (1997). Guidelines for usability testing with children. *Interactions*, lk 9-14.
[38]Choong, Y-Y., jt. (2019). Case Study – Exploring Children's Password Knowledge and Practices. *Proceedings 2019 Workshop on Usable Security (USEC)* Internet Society.

ligikaudu 57% ning vanema grupi hulgas 34%. Tugevat parooli kasutas nii nooremas kui vanemas vanusegrupis ligikaudu 13%.



Joonis 1. Paroolide tugevus[39]

Samuti selgus, et vanemas grupis oli 50% vastanutest jaganud enda parooli sõpradega.

Meeri Kuustemäe poolt 2015. aastal kaitstud magistritöö „6. ja 9. klassi õpilaste hinnangud enda digipädevustele[40]“ uuris, kuidas lapsed hindavad enda toimetulekut digitehnoloogiaga. Digipädevus on mainitud magistritöös jagatud nelja valdkonda: informatsioon, kommunikatsioon, sisuloome, ohutus ja probleemide lahendamine. Salasõnade loomine ning kasutamine kuulub ohutuse valdkonda[41]. Antud uuringus oli üks väide paroolide jagamise kohta: „Minu paroolid on ainult minule teada“. Küsitluses osalejad pidid märkima, kas väide kehtib, ei kehti nende kohta või ei oska öelda. Uurimuses tulemusena selgus, et 83% vastajatest hoiab salasõnad enda teada, 8% ei

[39]Ibid.
[40]Kuustemäe, M. (2015). 6. ja 9. klassi õpilaste hinnangud enda digipädevustele. Magistritöö, Tartu Ülikool.
[41]Ibid.

osanud vastata ning 6%-l vastajatest on oma salasõna jaganud. Siinkohal ei olnud täpsustatud, kellele parooli jagati.

Eeltoodust lähtuvalt arvab töö autor, et on suur vajadus edasiste ning laiemate uuringute järele, mille sihtgrupiks on lapsed.

2. KÄITUMISÖKONOOMIKA TEADMISTE ABIL NÜGIMINE

Käesolev peatükk on jagatud kolme alapeatükki.

Esimene alapeatükk selgitab käitumisökonoomia üht meetodit – nügimist. Samuti tuuakse välja kriteeriumid, millele nügimise strateegia peab vastama.

Teine alapeatükk annab ülevaate nügimise kasutamisest erinevates valdkondades ning selgitab, miks need võiksid toimida.

Kolmas alapeatükk keskendub praktikale, mis on loodud nügimismeetodit kasutades küberhügieeni parandamise eesmärgil. Eelkõige paroolide loomise ning kasutamise valdkonnas.

2.1. Nügimise mõiste ning strateegia välja töötamise tingimused

Kuigi inimesed võivad olla teadlikud turvalise käitumise põhimõtetest internetis, siis erinevatel põhjustel neid alati ei järgita. Põhjuseks võib olla see, et inimesed alahindavad riski kokku puutuda küberohtudega või ei hooma nad ebaturvalise käitumise tagajärgi. Kõige sagedasem põhjus nõrga parooli kasutamisel on aga lihtsalt ajapuudus või mugavus.[42]

Inimeste käitumise parandamiseks neile kasulikumas suunas on proovitud nügimist. Richard H. Thaler ning Cass R. Sunstein selgitavad nügimist järgnevalt:

„Nügimine tähendab valikuarhitektuuri ükskõk millist külge, mis juhib inimeste käitumist soovitud suunas, keelamata talle samas muid võimalusi ning muutmata oluliselt majanduslikke stiimuleid. Et sekkumist pidada vaid nügimiseks, peaks seda olema lihtne ja odav vältida. Nügimine ei ole võimu kasutamine, puuvilja asetamine pilgu tasandile läheb kirja nügimisena, rämpstoidu keelamine aga mitte.“[43]

[42]West, R. (2008). The Psychology of Security. *Communications of the ACM*, 51, 4, lk 34–41.
[43]Sunstein, C. R., Thaler R. H. (2018). Nügimine. viis toetada valikuid, mis viivad tervise, jõukuse ja õnneni. Tallinn: Tänapäev.

Näiteks ei ole nügimine see, kui veebilehekülgel keelata nõrkade paroolide sisestamist, kus süsteem takistab levinud ning nõrkade salasõnade nagu „123456“ või „*password*“ valimist kasutaja poolt vaatamata sellele, et nende kasutamine võib inimesele tuua kahju, mida teatud tüüpi paroolide keelamisega on proovitud vältida.[44]

Nügimise kasutamine inimeste valikute suunamiseks on saanud ka palju kriitikat selle libertaarse paternalismi omaduste pärast, mis tähendab, et nii riigil kui ka eraettevõttel on võimalus sekkuda inimeste otsuste tegemisse, et mõjutada nende käitumist neile kasulikumas suunas[45]. Kritiseerijad aga usuvad, et see võib viia olukorrani, kus inimeste suunamine muutub manipulatsiooniks ning lõpuks isegi karistamiseks. Selle illustreerimiseks on toodud näiteks tubakatooted. Kui algul on riigi poolt levitatud tagasihoidlikke hoiatussilte tänavatel, et suitsetamine on tervisele kahjulik, siis mingist hetkest hakati korraldama ründavaid teavituskampaaniaid. See viis omakorda tubakaaktsiisi tõstmise ning suitsetamise avalikus kohtades keelustamiseni. Arvustajate hinnangul ei ole ka välistatud, et suitsetaja hakkab tundma end paranoiliselt ning eeldab, et tubakatoodete regulatsioon karmistub või sigaretid lausa keelustatakse.[46]

Samuti peetakse ohuks nügimise kasutamist isiklike huvide saavutamiseks ning seetõttu ebaeetiliseks[47].

Põhikriteeriumid nügimise eetilisuse tagamisel on:

- Nügimine peab olema läbipaistev ning mitte eksitav;
- Inimesele peab nügimisega suunatavast valikust loobumine olema võimalikult lihtne;
- Nügimine ei tohi olla materiaalselt kulukas;
- Peab olema uskumus, et nügitava suunamine teatud valiku juurde on temale kasulik.[48]

[44]Renaud, K., Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies, 120, lk 22-35.
[45]Glaeser, E. L. (2006). Paternalism and Psychology. *The University of Chicago Law Review* 73, 1, lk 133-156.
[46]Sunstein, C. R., Thaler R. H. (2018). *Nügimine. viis toetada valikuid, mis viivad tervise, jõukuse ja õnneni.* Tallinn: Tänapäev.
[47]Turow, J. (2011). *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven: Yale University Press.
[48]Sunstein, C. (2015). The Ethics of Nudging. *Yale Journal on Regulation*, 32, 2, lk 413-450.

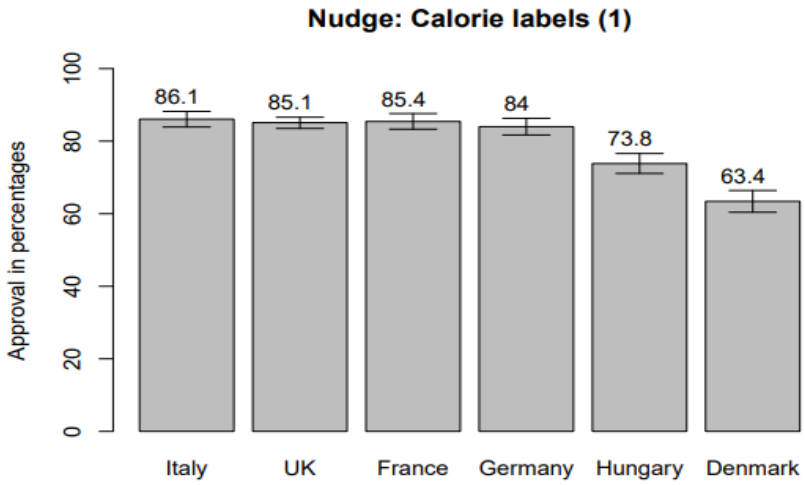
Tõstatatud on ka üldine küsimus - kes ikkagi lõpuks teab ja otsustab, mis on inimestele parim. Igaüks peaks saama elada nagu ta seda soovib, kui see ei riiva kellegi teise õiguseid[49].

Nügimise eetilisuse ning ühiskonna kasu vahel on aga kohati küsitav tasakaal. Kui nügimise tulemusena manipuleeritakse keskkonda ning selle eesmärk on mittesoovitava tegevuse valimise tegemine raskeks või võimatuks, võib vaielda, et see on ebaeetiline, kuna on limiteeritud mittesoovitatate tegevuste tegemise võimaluste hulk. Näiteks kiirusetõke („lamav politseinik“) tänaval vähendab kiiruse ületamise võimalust autojuhi poolt ning ohtu nii teistele liiklejatele kui ka autojuhile endale, mis on ühiskonna huvides[50].

Kokkuvõttes on riigi eesmärk muuta läbi nügimise inimese elu paremaks ja turvalisemaks ning eesmärgiks seatud tulemuste saavutamiseks ning eetilisuse tagamiseks tuleks seda teha vaid põhjaliku eeltöö järgselt[51].

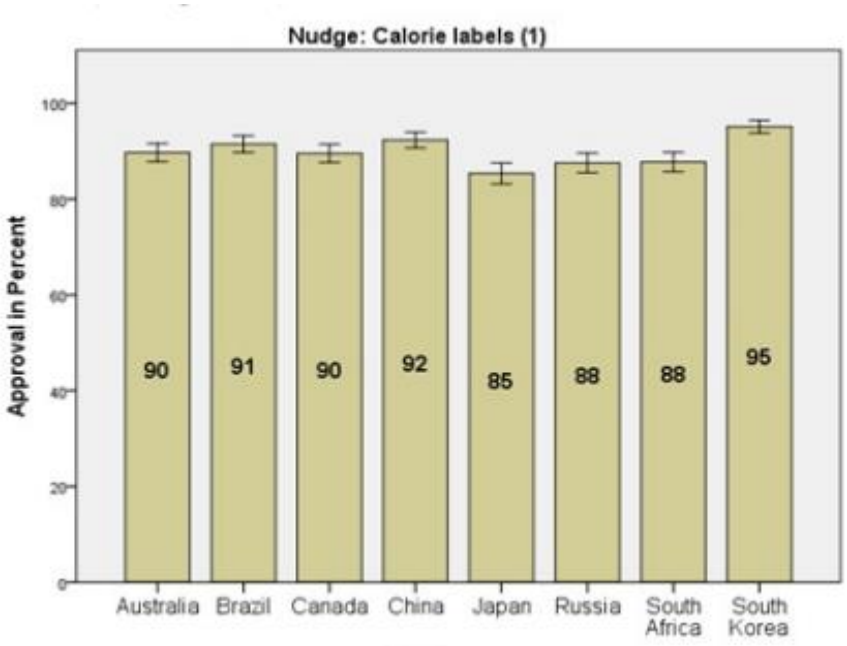
Informatiivset nügimist, mis soodustab tervislikke eluviise, nagu näiteks valitsuste poolt kehtestatud nõuet, et toodete pakenditel peab olema välja toodud kalorite hulk, peetakse inimeste poolt positiivseks sekkumiseks. Kuigi sellist nõuet võib pidada erafirmade jaoks piiravaks, oli kuues Euroopa riigis läbi viidud uuringu tulemusel, toetus nügimisele keskmiselt 78% (joonis 2.)[52].

[49]Child, J. W. (1994). Can Libertarianism Sustain a Fraud Standard? *Ethics*, 104, 4, lk 722-738.
[50]Renaud, K., Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies*, 120, lk 22-35.
[51]Benartzi, S., jt. (2017). Should Governments Invest More in Nudging? *Psychological Science*, 28, lk 1041-1055.
[52]Ibid.



Joonis 2. Toetus informatiivsele nügimisele Euroopas[53]

Samuti oli kalorite hulga illustreerimise nõude pooldajate hulk suur väljaspool Euroopat – keskmiselt 90% (joonis 3).



Joonis 3. Toetus informatiivsele nügimisele väljaspool Euroopat[54]

[53]Reisch, L. A., Sunstein, C. R. (2016). Do Europeans like nudges? *Judgment and Decision Making*, 11, 4, lk 310–325.

[54]Rauber, J., jt. (2017). Behavioral Insights All Over the World? Public Attitudes Toward Nudging in a Multi-Country Study. Kättesaadav arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921217 (10.05.2019).

Üldjuhul on inimeste toetus nügimisele positiivne nii kaua, kuni selle soovitud tulemus on vastavuses nende huvide ning väärtustega. Nügimine ei ole enamikele vastuvõetav, kui selle tulemusena võetakse inimeselt raha tema teadmata ning nõusolekuta. Samuti ei soosita alateadlikke reklaame, mille eesmärgiks on küll suitsetamise või ülesöömise vähendamine, kuid mis nii kiirelt näiteks kinoekraanilt üle käib, et inimene ei jõua seda teadvustada. Antud juhul seostatakse neid reklaame manipulatsiooniga.[55]

2.2. Nügimise kasutamine praktikas

Nügimist on kasutatud mitmetes erinevates valdkondades, millest peamised on inimeste tervise- ning finantskäitumine.

Näiteks on kasutatud nügimist vähi sõeluuringutes osalevate inimeste arvu suurendamiseks. Eestis juba toimivat sõeluuringutes osalemise kutsete saatmist on proovitud ka Ühendkuningriigis. Eesmärk oli suurendada inimeste osalust just madalama sissetulekuga ning etnilise vähemuse esindajate hulgas, kuna nende sõeluuringutes osalemine oli kesine. Lisaks kutse edastamisele, saadeti inimestele mingi aja möödudes ka meeldetuletus ning see edastati vastavalt valimile SMS-i, telefonikõne või posti teel[56].

Siinkohal on oluline just meeldetuletuse sisu. Saksamaal läbi viidud uuring näitas, et kui saadetakse teade sisuga: „Viimaste uuringute kohaselt käis eelmisel aastal vähi sõeluuringus vaid üks viiendik meestest (ainult 18 %!)“, siis hindas sõnumi saaja enda tõenäosust uuringutele minemisel ka madalalt (30.8%). Mehed, kellele saadeti teade: „Viimased uuringud Saksamaal näitavad, et vähi sõeluuringutel osales eelmisel aastal kaks kolmandik meestest (lausa 65%!)“, hindasid ka tõenäosust ise uuringutes osalemist kõrgemalt (46.2%)[57].

Käesoleva näite puhul nügiti inimesi sõnumi raamistamise (*framing*) põhimõttel. Kahneman-i ja Tversky poolt kasutusele võetud raamistamise efekt seisneb teoorias, et

[55]Reisch, L. A., Sunstein, C. R. (2016). Do Europeans like nudges? *Judgment and Decision Making,* 11, 4, lk 310–325.
[56]Duffy, S. W., Myles, J. P., Maroni, R. (2016). Rapid review of evaluation of interventions to improve participation in cancer screening services. *Journal of Medical Screening*, 24, 3, lk 127-145
[57]Decker S., Sieverding M., Zimmermann F. (2010). Information about low participation in cancer screening demotivates other people. *Psychol Sci*, 21(7), lk 941-943

probleemi või teate sisu erinev sõnastamine mõjutab tihti ka inimese otsust, mis ei pruugi olla alati ühesugune, vaid oleneb just selle edastamisest[58].

Antud juhul on kasutatud ettekirjutavat *(injunctive)* sotsiaalset normi, mis annab inimesele mõista, et teatud käitumine on „normaalne" ning seetõttu ka mõistlik[59]. Tihti eristavad inimesed õiget ja valet käitumist teiste eeskujul. Siinkohal on oluline selgitada antud teooria kahte aspekti. Määramatuse faktor, mis seisneb selles, et kui inimene tunneb end ebakindlalt, on tõenäolisem, et ta võtab eeskuju teiste käitumisest. Sarnasuse faktor tähendab seda, et inimesed käituvad sageli nii nagu teised inimesed, kellega nad end samastuvad.[60]

Näiteks kasutatakse komöödiasarjades võltsnaeru, mis paneb ka vaatajad naerma, kuna see tundub tänu ette antud käitumismallile õige. Samuti võib tuua näiteks teeninduskohtades jootraha purgi nägemine. Kui klient näeb, et purgis on raha, tekib tal tunne, et ka tema peaks purki raha lisama. Olgugi, et purgis olev raha võidi panna just kliendi mõjutamise eesmärgil ka klienditeenindaja enda poolt[61].

Lihtsaid nügimisvõtteid kasutavad kauplused igapäevaselt. Mitmed tooted on klienti ostma meelitamiseks paigutatud läbimõeldult ning sihilikult. Näiteks kaup, mida seostatakse impulsiivsete ostudega (närimiskumm, šokolaad, ajakirjad jne), sätitakse kassa kõrvale, et inimene neid märkaks, kui tähtsamad tooted on juba leitud[62].

Samasugust taktikat on kasutatud ka positiivsemas suunas – tervislikumate valikute tegemisel. On tõenäoline, et õpilaste seas suureneb puuviljade tarbimine, kui need paigutada koolisööklates nähtavamale kohale[63].

---

[58]Kahneman, D., Tversky, A. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 211 (4481), lk 453-458.

[59]Ammi, M. jt. (2017). Using social injunctive norms to nudge usersto build green houses / El empleo de normasprescriptivas sociales para animar a los usuarios aconstruir casas ecológicas. *Psyecology Revista Bilingüe de Psicología Ambiental / Bilingual Journal of Environmental Psychology*, 8 (3), lk 297-322

[60]Cialdini, R. B. (2006). Influence: The Psychology of Persuasion, *Harper Business.*

[61]Sunstein, C. R., Thaler R. H. (2018). *Nügimine. viis toetada valikuid, mis viivad tervise, jõukuse ja õnneni.* Tallinn: Tänapäev.

[62]Miller, C. jt. (2012). Measuring the Food Environment: A Systematic Technique for Characterizing Food Stores Using Display Counts. *Journal of Environmental and Public Health*, 2012, lk 1-6

[63]Marcano-Olivier, M. jt. (2019). A low-cost Behavioural Nudge and choice architecture intervention targeting school lunches increases children's consumption of fruit: a cluster randomised trial. International Journal of Behavioral Nutrition and Physical Activity, 16, lk 20

Kuna tänapäeval teevad inimesed tihti erinevaid ning tähtsaid valikuid ja otsuseid küberkeskkonnas, siis on oluline uurida nügimise võimalusi ka tehnikaseadmetes[64].

Tabel 2 kirjeldab valikutearhitektuuri põhimõtteid ning toob vastavad näited, mida on Thaler, Sunstein ja Balz loonud kübervaldkonnas rakendamiseks. Efektiivse valikuarhitektuuri välja töötamiseks saab kasutada vastavalt eesmärgile erinevaid mõjutamise vahendeid. Üheks populaarsemaks ning ka edukamaks nendest on vaikimisi seadete kasutamine[65]. Selle aluseks on põhimõte, et inimesed valivad tihti kergema vastupanu teed mineku, kuna see nõuab nendelt vähem pingutust.

Tabel 2. Nügimise põhimõtted, kirjeldused ja näited tehnikaseadmete puhul

Nügimise põhimõte	**Kirjeldus**	**Näide**
Vaikimisi seaded *(defaults)*	Valikud on seadistatud vaikimisi.	Vaikimisi valikute muutmine eesmärgiga suurendada tõenäosust, et inimesed annavad oma nõusoleku organidoonorlusega liitumiseks. Inimene peab ise muutma valikuid, kui ei ole nõus olema organidoonor.
Vigade eeldamine	Süsteem eeldab, et inimesed eksivad, ning on võimalikult andestatav.	Sularahaautomaat nõuab, et inimene võtab enne raha kätte saamist pangakaardi välja. Selle tulemusena ei unusta inimene kaarti masinasse.
Kaardistamise mõistmine	Info kaardistamine, mis aitab inimesel erinevaid valikuid paremini mõista.	Digikaamera megapikslite numbrilise kirjelduse asemel näidata visuaalselt, milleks kaamera võimeline on. Näiteks reklaamida koos

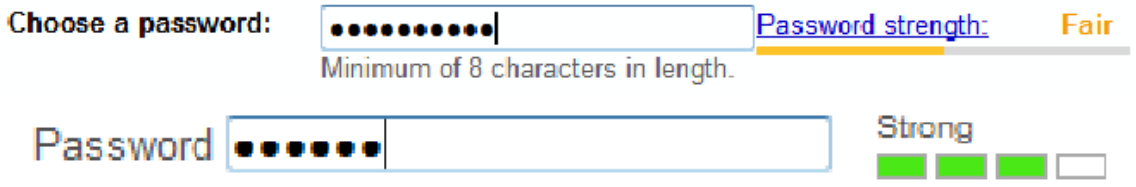
[64]Brocke, J., jt. (2016). Digital Nudging. *Business & Information Systems Engineering*, 58, 6, lk 433–436.
[65]Sunstein, C. R. (2017). Nudges that fail. *Behavioural Public Policy*, 1, 1, lk 4-25.

		kvaliteetse pildiga väljatrüki piirsuurust.
Tagasiside andmine	Süsteem annab inimesele teada, kui ta on teinud midagi hästi või valesti.	Elektroonilised teemärgised, mis annavad inimesele naeru- või kurva näoga märku kiiruse ületamisest või sellest kinni pidamisest.
Keeruliste valikute struktureerimine	Kõikide valikute kirjeldamine lubades inimesel vajadusel kompromisse.	Internetipoodide kaubavaliku filtreerimise võimalused lihtsustamaks kasutaja jaoks toote valimise ning ostmise protsessi.
Stiimulid	Stiimulite esile tõstmine, et tõhustada nende mõju.	Telefonid, mis kuvavad jooksvalt kõne maksumust.

Allikas: Balz, J. P, jt. (2010). Choice Architecture[66] (autori tõlgitud)

2.3. Tugevama parooli loomise ja kasutamise suunas nügimine

Mitmed eksperdid peavad tekstilist parooli nõrgaks, kuna sama salasõna kasutatakse tihti erinevatele kontodele ligi pääsemiseks[67]. Joonisel 4 on näha ühe lahendusena tugevuse mõõtjat (*password strength meter – PSM, edaspidi PSM*).

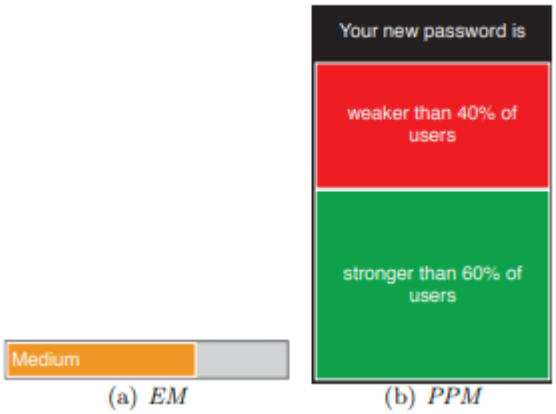


[66]Balz, J. P, jt. (2010). Choice Architecture. Kättesaadav arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509 (10.05.2019).
[67]Han, W., jt. (2018). Shadow Attacks based on Password Reuses: A Quantitative Empirical View. IEEE Transactions on Dependable and Secure Computing, 15, lk 309 – 320

Joonis 4. Gmail-i ja Yahoo parooli tugevuse mõõtja[68]

Küll aga näitavad erinevad uuringud, et PSM-i kohaselt on mõni nõrk parool hoopis tugev. 2010. aastal avaldatud uuring näitas, et PSM ei ole alati usaldusväärne[69]. Eelkõige sellepärast, et pikk sõna näitab PSM-i kasutades automaatselt parooli tugevust. Praktikas aga see nii ei pruugi olla.

Hästi disainitud ning välja töötatud PSM aitab kasutajat suunata turvalisema parooli loomiseni[70]. Ameerika Ühendriikides läbi viidud eksperiment näitas, et hea PSM-i rakendamise korral on tõenäolisem, et inimene muudab enda salasõna tugevamaks[71]. Antud juhul kasutati sotsiaalseid norme, mille puhul kasutajale antakse info tema parooli tugevusest võrdluses teiste kasutajatega. Joonisel 5 on vasakul algeline PSM, mis näitab, kas sisestatud parool on nõrk, keskmine või tugev. Paremal on välja toodud mõõdik, mis näitab, kas sisestatud salasõna on nõrgem kui 40% kasutajatel või tugevam kui 60% kasutajatel.



Joonis 5. PSM nügimine[72]

[68]Egelman, S., jt. (2013). Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, lk 2379-2388
[69]Weir, M., jt. (2010). Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. *Proceedings of the 17th ACM conference on Computer and communications security,* lk 162-175
[70]Egelman, S., jt. (2013). Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* lk 2379-2388
[71]Ibid
[72]Ibid

Eksperimendi tulemused näitasid, et parooli tugevuse mõõtja suunab inimesi tugevamat salasõna looma, kuid seda vaid juhul, kui peab looma uue salasõna. Uue ning tugevama parooli valis 77,5%.

Sotsiaalsete normide näitamine mõjub, kuna inimesed teevad meelsamini seda, mida peetakse õigeks ning mida enamik inimestest ka tegelikult teeb[73].

Samuti lähtub inimene oma tegevuses soovist end kaitsta. Kui inimene tunneb end ohustatuna, teeb ta sellest lähtuvalt vastavaid valikuid *(Protection Motivation Theory – PMT).* Aastal 2019 avaldati sellel teoorial läbi viidud uuringu tulemused. Uuringu eesmärk oli vaadelda, kas internetikeskkonnas teavituste erinev kujutamine suunab kasutajaid turvalisemaid valikuid tegema. Uuringus osales 2024 internetikasutajat Saksamaalt, Rootsist, Poolast, Hispaaniast ja Ühendkuningriigist[74].

Osalejad jagati nelja gruppi – üks kontrollgrupp *(control group)* ning kolm erinevaid tegevusi läbi viivat sekkumisgruppi *(treatment group).* Uuringus osalejatel paluti navigeerida ohutult internetipoe kodulehel ning selle käigus ilmus nendele (vastavalt gruppi kuulumisele) teavitus.

Joonisel 6 on välja toodud erinevate sihtgruppide teavitused, mis neile ilmusid internetipoe koduleheküljel.

[73]Sunstein, C. R., Thaler R. H. (2018). Nügimine. viis toetada valikuid, mis viivad tervise, jõukuse ja õnneni. Tallinn: Tänapäev

[74]Bavel, R., jt. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123, lk 29-39.

Kontrollgrupi teavitus

Navigeeri ohutult.

Sekkumise grupp I teavitus

Navigeeri ohutult.

Küberrünnakute ohvriks langemise riski saad kergesti vähendada, kui kasutad turvalist internetiühendust, logid end peale kasutamist välja ning valid tugeva parooli (suurte ning väikeste tähtede, arvude ja sümbolite kombinatsioon).

Sekkumise grupp II teavitus

Navigeeri ohutult.

Vastasel juhul võivad lekkida sinu isiklikud andmed või arvuti nakatuda viirusega.

Sekkumise grupp III teavitus

Navigeeri ohutult.

Küberrünnakute ohvriks langemise riski saad vähendada, kui kasutad turvalist internetiühendust, logid end peale kasutamist välja ning valid tugeva parooli (suurte ning väikeste tähtede, arvude ja sümbolite kombinatsioon).

Vastasel juhul võivad lekkida sinu isiklikud andmed või arvuti nakatuda viirusega.

Joonis 6. Kontrollgrupi ja sekkumise gruppide teavitused[75] (autori tõlgitud)

Kontrollgrupi teavitus sisaldas vaid meeldetuletust ohtutult navigeerida.

I sekkumisgrupi teavitus sisaldas peale meeldetuletuse veel nõuannet, kuidas end kergesti küberünnakute eest kaitsta. Nõuande eesmärk on kasutajale sisendada enesekindlust *(self-efficacy),* et tema suudab end ise ohtude eest kaitsta[76].

[75]Maddux, J. E., Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19, 5, lk 469-479.
[76] Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: Worth Publishers.

II sekkumisgrupi teavitus hoiatas, et nende tegevus/tegevusetus internetis võib kaasa tuua küberrünnaku.

III sekkumisgrupi teavitus oli kombinatsioon I ja II sekkumisgrupi sõnumitest. Varasemate uuringute kohaselt on inimesed vastuvõtlikumad enda käitumises muudatusi tegema, kui on välja toodud nende haavatus ning neid varitsev võimalik oht[77].

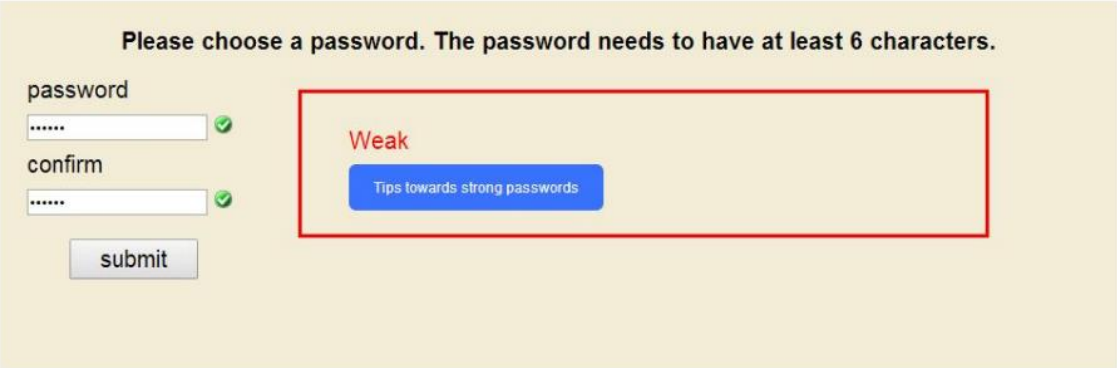
Uuringu tulemused näitasid, et osalejad, kellele tuli internetipoes teavitus (koos või ilma küberrünnaku hoiatuseta), kuidas end võimaliku küberohu eest kaitsta, navigeerisid ka turvalisemalt. 21.8% II sekkumisgrupist lõpetasid eksperimendi, kui neile tuli teade, et nende mitteturvaline käitumine võib kaasa tuua küberohu riski.

Kokkuvõttes oli edukas sekkumine see, kui internetikasutajaid teavitada, kuidas end võimalike küberohtude eest kaitsta ning teavitada, mis nende tegevus endaga kaasa tuua võib.

Kombineeritud vahendite kasutamine paroolide tugevuse mõõtja disanimisel osutus kõige efektiivsemaks ka järgnevas uuringus, kus lisaks infole salasõna tugevusest lisati ka hoiatussõnum või viide tugeva parooli loomise soovitusele[78].

Joonisel 7 on toodud uuringus kasutatud PSM, mis näitas, kas sisestatud salasõna oli nõrk, keskmine või tugev. Samuti oli öeldud, et parool peab koosnema vähemalt kuuest tähemärgist ning lisatud oli viide „Nipid tugeva parooli koostamiseks“. Uuringu läbiviijad aga tõdesid, et olla kindel, kas inimesed ka lugesid viidatud nippidele või vajutasid sellele lihtsalt uurimise keskkonna tõttu, oleks vaja läbi viia täiendavaid katseid, mis samuti annaksid ka ülevaate nende nõuannate mõjust.

[77]Griffin, R. J., jt. (2000). Protection Motivation and Risk Communication. *Risk Analysis*, 20, 5, lk 721-734.
[78]Khern-am-nuai, W., jt. (2017). Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment. *Proceedings of the 50th Hawaii International Conference on System Sciences*, lk 587-596.



Joonis 7. PSM koos viitega[79]

Töö autor arvab, et eelnevalt välja toodud lähenemisi võiksid kasutada või vähemalt testida selle mõju noorte seas populaarsed veebileheküljed. Oluline on järgida kasutajasõbralikkust ning eetilisust.

[79]Ibid.

3. METOODIKA

Käesolevas peatükis antakse ülevaade uurimistöö valimist, andmete kogumise meetodist ja andmete analüüsist.

Magistritöö eesmärgi saavutamiseks kasutab autor kvantitatiivset uurimismeetodit. Kvantitatiivne uurimismeetod võimaldab analüüsida võimalikult suurt valimit. Autor on koostanud küsitluse, kus on lisaks suletud küsimustele ka avatud vastustega küsimused, mistõttu kasutatakse ka kvalitatiivse uurimismeetodit.

3.1. Valim ja andmete kogumine

Küsitlusele vastajad on valitud vastavalt sissejuhatuses mainitud küberkiusamise uuringus osalejate vanusegrupile, milleks on 9-16 aastased koolinoored üle Eesti.

Andmete kogumiseks koostas töö autor ankeetküsitluse internetis *Google Docs* keskkonnas, kuna see võimaldas õpilastele kiiremat ning mugavamat vastamist. Samuti lihtsustas see autoril andmete kogumist, kuna isetäidetava ankeetküsitlusega on võimalik saada andmestik võimalikult suurelt hulgalt õpilastelt ning analüüsimist. *Google Docsi* eelistati ka, kuna küsimustik avaldatakse populatsiooni suhtes üheaegselt ning küsimustele on võimalik vastata vastajale sobival ajal. Küsitluse laiali saatmine ning vastuste kogumine toimus märts 2019. Küsitluse pealkirjaks oli „Paroolide loomine ning kasutamine“.

Ankeet ning uuringu eesmärgi kirjeldus saadeti laiali e-posti teel kõikidesse põhikoolidesse, mille kodulehelt autor võis välja lugeda, et koolis on arvutiõpe või -huviring. Enamasti on informaatika koolides valikaine, kuid ühel või teisel viisil on see õppekavasse või huviringidena sisse toodud[80].

Autor saatis välja 148 kirja ning lisas selgitusena juurde soovituse vastata küsitlusele arvutiõppe või -huviringi tunnis, kuna sellisel juhul oli õpetajal vajadusel võimalus

[80]Lorenz, B., Kikkas, K. (2019). Digitaalne kirjaoskus infoühiskonnas. Kättesaadav arvutivõrgus: https://entk.ee/wp-content/uploads/2019/02/1-2-birgy-ja-kaido.pdf (01.04.2019).

õpilastele selgitada ning täpsustada küsimusi. Samuti andis see võimaluse diskussiooniks paroolide turvalisuse teemal.

Tagamaks vastajate anonüümsus, ei olnud küsitluses vaja märkida kooli nime ega klassi. Magistritöö seisukohalt oli oluline eelkõige õpilase vanus ja sugu.

Küsitlusele vastas 1105 õpilast, millest valimisse mahtus 1077. Valimist jäid välja õpilased, kelle vanus ei olnud vahemikus 9 – 16. Esines juhtumeid, kui kirjutati vanuseks näiteks 9000 või muu suvaline number. Ühel juhul kirjutati vanuse lahtrisse enda nimi. Sellised vastused välistasid valimisse kuulumise.

3.2. Andmete analüüs

Küsitluse algandmeteks tuli vastajal märkida sugu ning vanus.

Kuna erinevate uuringute kohaselt on tüdrukud kogenud rohkem küberkiusamist kui poisid, siis on küsitud ka vastajate sugu[81], eesmärgiga vaadelda, kas vastuste põhjal on näha soolisi erinevusi küberkäitumises paroolide loomise ning kasutamise suhtes.

Küsitlus koosnes 18 küsimusest, millest 15 olid vastusevariantidega ning kolm avatud vastustega küsimused.

Google Docs platvorm, mille abil küsimustik koostati ning andmed koguti, võimaldas andmed esitada vajadusel protsentuaalselt ja diagrammi kujul. Samuti oli platvormi standardfunktsionaalsusena andmete Excelisse teisendamine, mistõttu polnud andmete käsitsi sisestamine vajalik. Tulemuste näitlustamiseks on kasutatud tabeleid ja diagramme.

[81]Luik, P., Naruskov, K. (2015). Küberkiusamise fenomeni tajumine Eesti õpilaste seas: sooline võrdlus kiusamise kriteeriumite ja liikide alusel. *Eesti Haridusteaduste Ajakiri*, 3, (2), lk 186–215.

3.3. Uuringuga seotud eetilised probleemid

Kuna autori poolt koostatud valimisse kuulusid koolinoored vanuses 9 – 16 aastat, siis oli oluline tagada küsitluse eetilisus, kuna tegemist oli haavatava sihtgrupiga. Antud valimi küsitlemisel tuleb läheneda teisiti kui täiskasvanutega[82]. Seetõttu ei maininud autor ka küsitluses sõna „küberkiusamine“, et mitte tuua esile võimalikke negatiivseid tundeid. Ankeedi pealkirjaks valiti neutraaluse eesmärgist lähtuvalt „Paroolide loomine ning kasutamine“. Oluline oli ka koostada ankeet, kus küsimuste sõnastused olid selged ning üheselt mõistetavad. Samuti oli autor arvamusel, et küsitlusele vastamise asukohaks tuttava keskkonna valimine, antud juhul õppeklass, loob eelduse vastaja võimalike pingete maandamiseks, mis võivad tekkida võõra ruumiga. Koolinoorte vastamismugavuse eesmärgil valiti ka ankeeküsitlus, mis oli täidetav arvutis. Küsitluses järgiti uuringu vastavust eetikanõuetele. Kõikidel küsitluses osalejatel tagati anonüümsus ning neil ei olnud küsitlustele vastamine kohustuslik. Igal küsitlusele vastajal oli õigus katkestada oma osalus uuringu mistahes etapis.

[82]Punch, S. (2002). Research with Children: The Same or Different from Research with Adults? *Childhood*, 9, 3, lk 321-341.

4. TULEMUSED JA ARUTELU

Käesolev peatükk käsitleb uurimuse tulemusi ning arutelu.

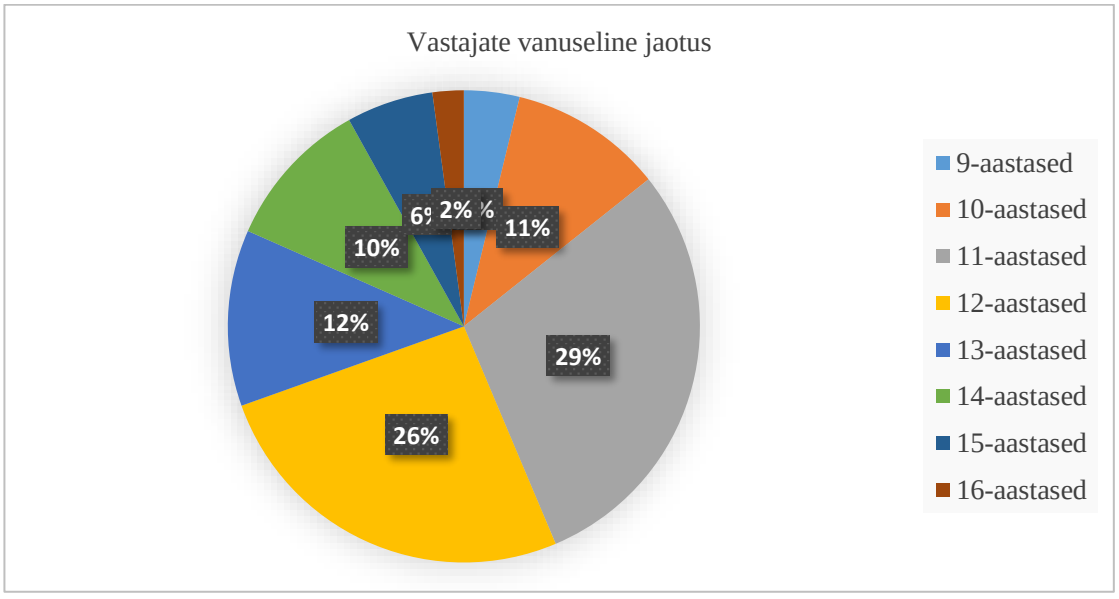
Esimene alapeatükk toob välja küsitluse tulemused küsimuste kaupa.

Teises alapeatükis tehakse tulemuste põhjal järeldused, kuidas koolinoored loovad ning kasutavad paroole. Samuti antakse soovitusi, kuidas neid suunata turvalisemate valikute poole.

4.1. Küsitluse tulemused

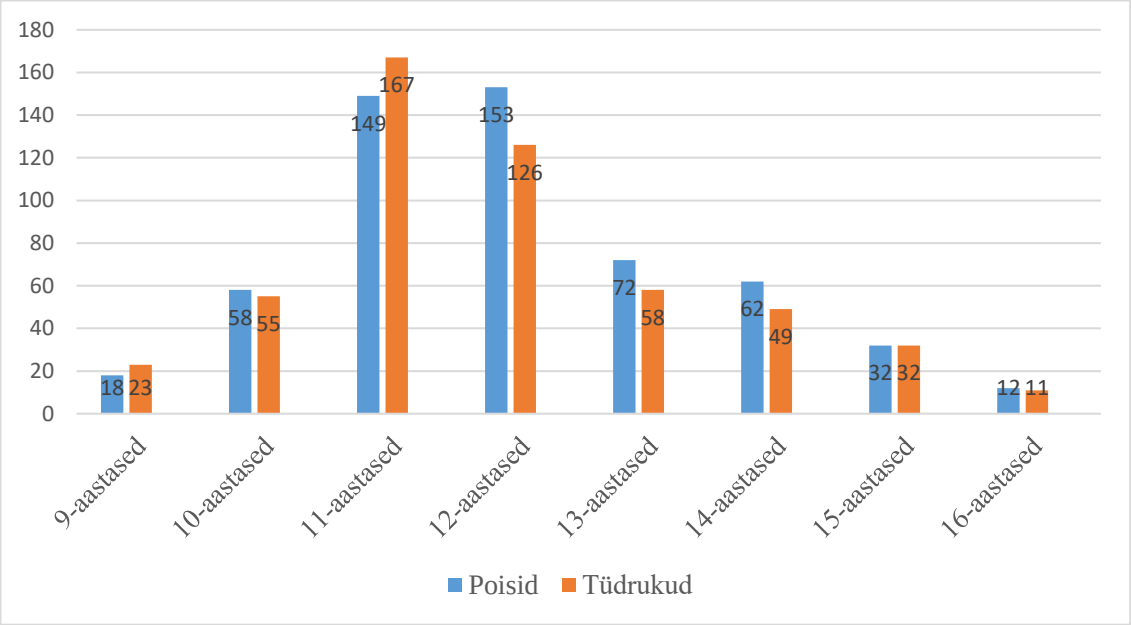
Küsitlusele vastas 1077 õpilast, neist 556 poissi, mis moodustab valimist 52% ja 521 tüdrukut, vastavalt 48%.

Joonisel 8 on välja toodud ankeedile vastajate vanuseline jaotus. Kõige rohkem oli vastajate hulgas 11-aastaseid – 316 (29%) ja 12-aastaseid vastavalt 279 (26%).



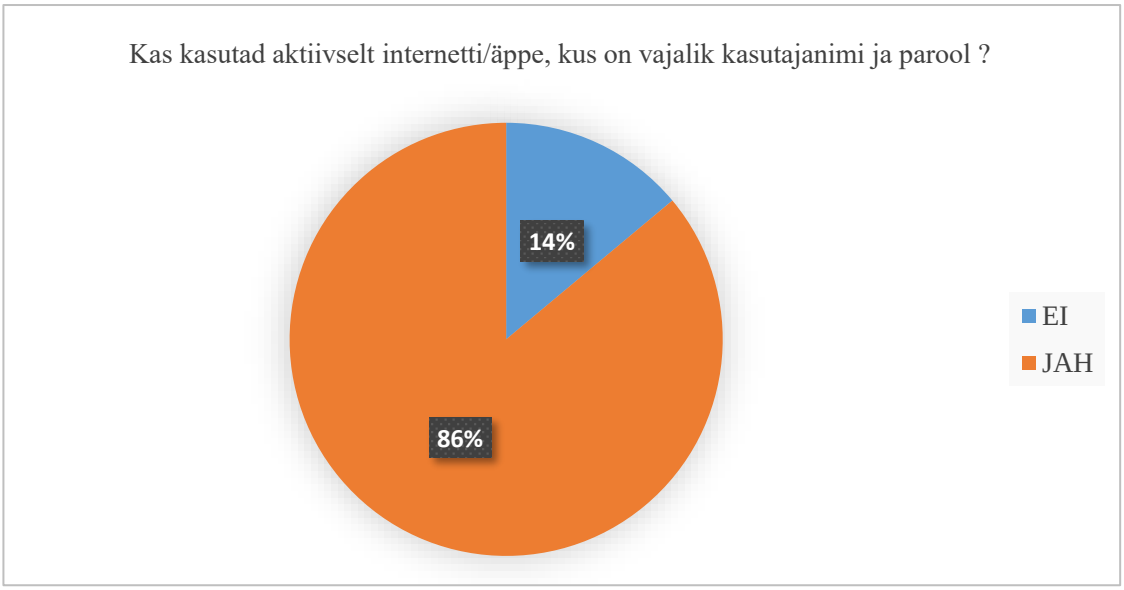
Joonis 8. Vastajate vanuseline jaotus

Sooliselt ja vanuseliselt jagunesid vastajad alljärgnevalt (Joonis 9):



Joonis 9. Vastajate sooline ja vanuseline jaotus

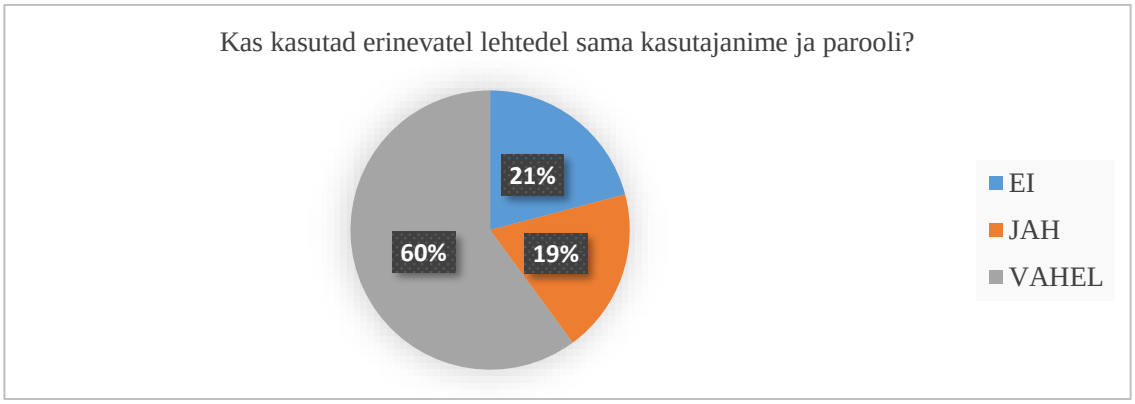
Järgnevalt uuriti kasutajanime ning parooli nõudvate veebilehtede ja äppide kasutamist. Selgus, et 9-16 aastased kasutavad aktiivselt internetti (Joonis 10). Aktiivseid interneti ja/või äppide kasutajaid oli 86% vastanutest, sealjuures poisid ja tüdrukud jagunevad selles osas võrdselt – mõlemad 43%.



Joonis 10. Interneti/äppide aktiivne kasutamine

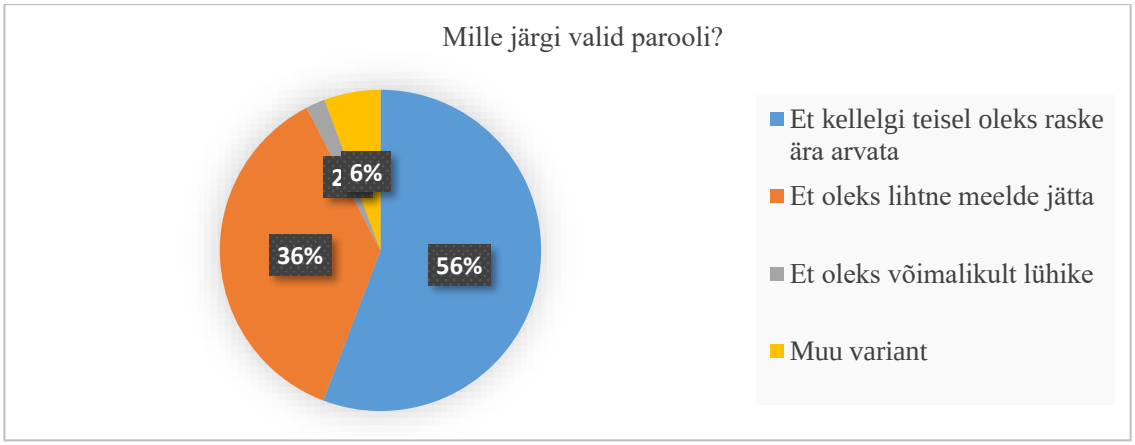
Kuna valdav enamus kasutavad aktiivselt internetti ja/või äppe, kus on vajalik registreerida end kasutajanime ja parooli kasutades, siis on oluline, et koolinoored oleksid teadlikud turvalise salasõna loomise põhimõtetest.

Uuringus selgus, et 60% (647 õpilast) vastanutest kasutab vahel erinevatel lehtedel sama kasutajanime ja paroole. 21% vastanutest teeb seda pidevalt ning 19% ei kasuta samu paroole (Joonis 11). Märkimisväärseid erinevusi poiste ja tüdrukute vahel ei ole.



Joonis 11. Sama kasutajanime ja parooli kasutamine

Küsitluses uuriti ka parooli valimise põhjuseid (Joonis 12). Selgus, et kõige sagedasem põhjus parooli valikul oli teiste suutmatus parooli ära arvata. Nii vastas 601 õpilast (56% vastanutest). Populaarsuselt järgmine parooli valimise põhjus oli võime parooli ise meelde jätta – 394 õpilast (36% vastanutest). Väike osa (2%) vastanutest valib paroole salasõna pikkuse järgi. Nii tegutseb 61 vastanut.

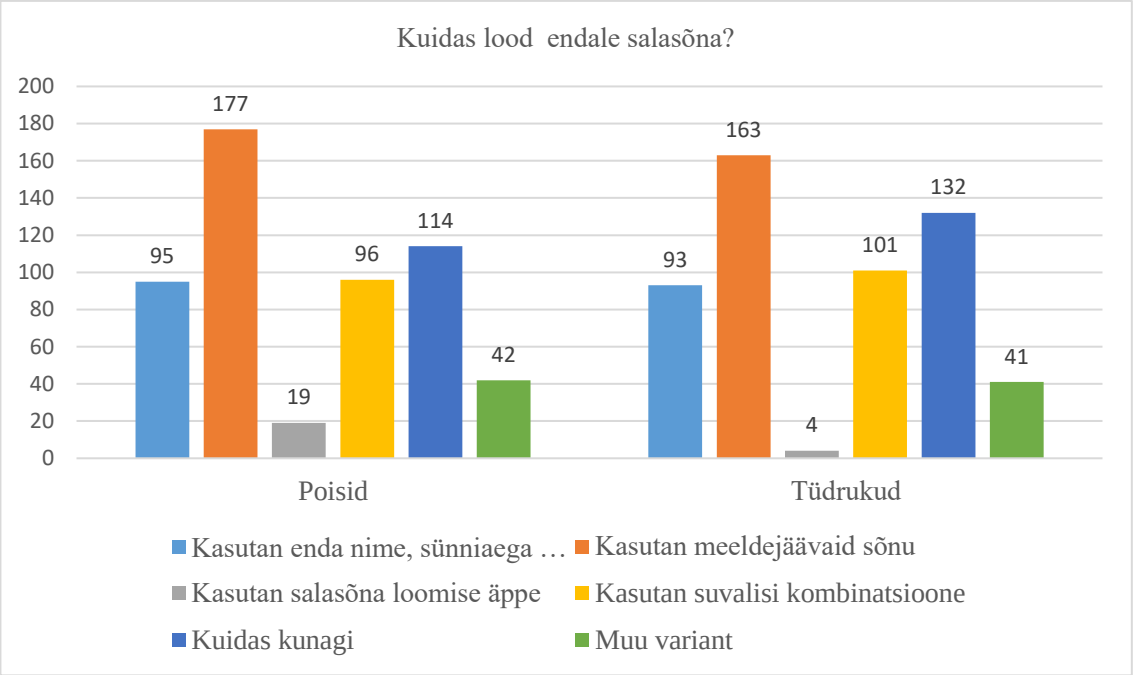


Joonis 12. Parooli valimise põhjused

6% vastajatest oli parooli valikul mõni muu põhjus, millest toodi muuhulgas välja järgmised põhjendused:

- *mis oleks hästi pikk ja hästi keeruline, aga meelde peab jätma;*
- *keskmise pikkusega aga raske;*
- *et seostan millegiga mis on mulle tähtis;*
- *võimalikult pikk ja raske (numbrid, suured tähed);*
- *kirjutan suvaliselt ja siis õpin selle pähe (nt DFJEUIVJE3478FeDER);*
- *ma räägin oma emaga ja otsustame koos;*
- *panen parooliks midagi, mida pole loogiliselt võimalik võtta;*
- *ma valin numbrid ja panen need oma süsteemi järgi paika;*
- *ma tavaliselt panen kedagi või midagi tähtsat oma elust;*
- *ma lihtsalt mõtlen mõned sõnad välja ja kasutan neid paroolina;*
- *et oleks lühike, aga teistele raske.*

Uurides salasõna loomise viise, selgus, et kõige sagedamini kasutatakse meeldejäävaid sõnu (340 vastajat) ning juhuslikke viise (246 vastajat) vastavalt 32% ja 23% õpilastest. 17% vastanutest kombineerib oma parooli enda nimes, sünniajas või muudest isiklikest andmetest. Suvaliste kombinatsioonide meetodit kasutab 18% (197 vastajat). Muid variante kasutab 83 (8%) õpilast ning salasõna loomise äppe kasutab vaid 23 (2%) õpilast. Joonisel 13 on välja toodud erinevate salasõna loomise viiside kasutamise soolises lõikes, kus on näha, et suuri erinevusi poiste ja tüdrukute osas ei ole.

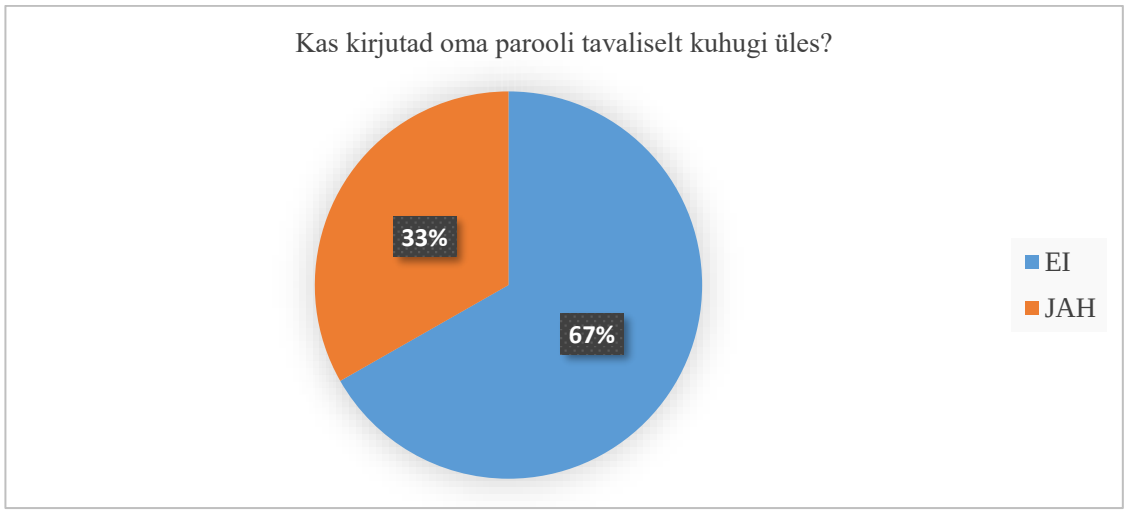


Joonis 13. Salasõna loomine

Kui vastati eelmisele küsimusele salasõna loomise kohta "Muu variant", siis pakuti muuhulgas välja järgnevaid vastuseid:

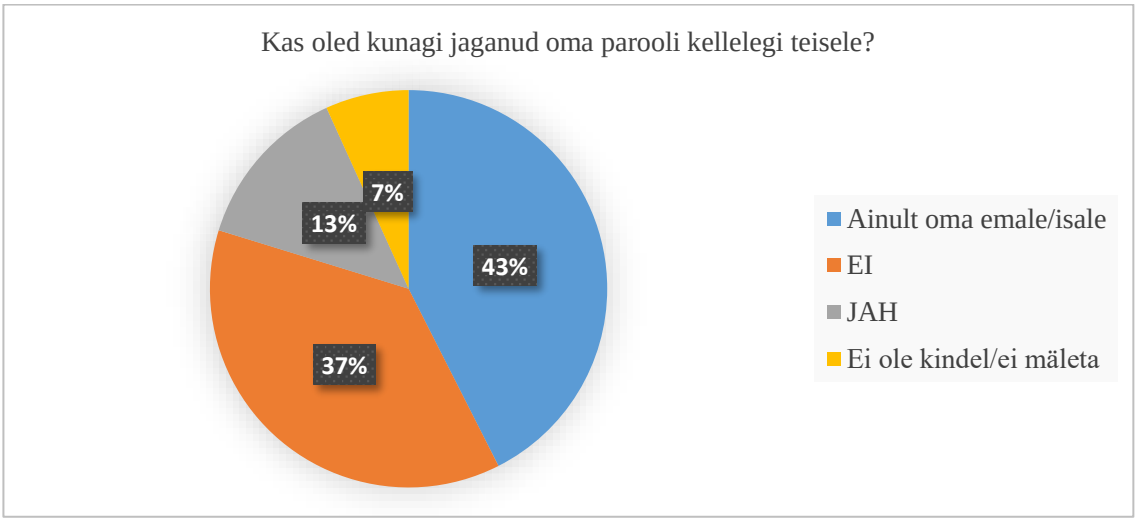
- *mõtlen koos emaga salasõna välja*;
- *kasutan numbreid ja saan kokku ühe lause;*
- *panen oma lemmikmänguasjade nimed, sest neid nimesid keegi ei tea;*
- *kasutan nii suvalisi kombinatsioone kui ka muid isiklikke andmeid;*
- *ma teen enda pärisnime veidi lühemaks;*
- *minul on samasugune parool nagu minu emal, sest kui on vaja siis saab ta minu netiseadmesse ligipääsu;*
- *lasen vennal tähed ja numbrid kokku panna;*
- *arutan ema/isaga;*
- *enda nimi koos numbriga;*
- *kuulan ema vastuseid ja valin sobiva.*

Uuringus küsiti ka, kas õpilased kirjutavad tavaliselt oma parooli kuhugi üles (Joonis 14). 719 õpilast (67% vastajatest) vastas sellele küsimusele eitavalt ning 358 (33% vastajatest) jaatavalt.



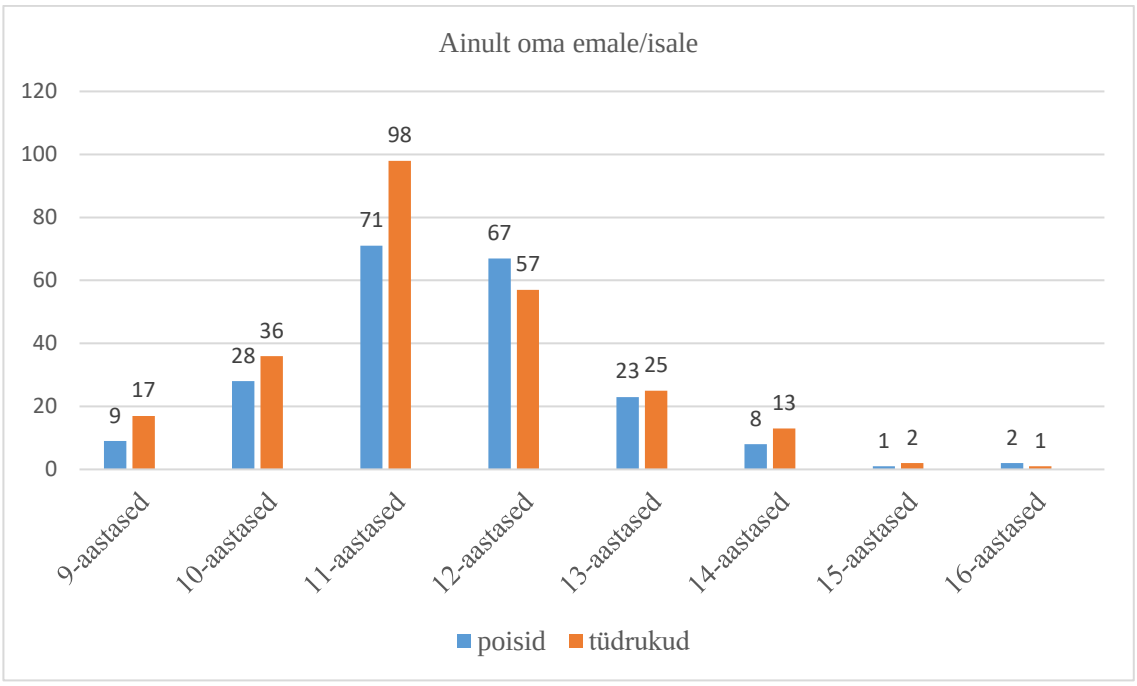
Joonis 14. Parooli üles kirjutamine

Lisaks selgus uuringust, et peaaegu pooled vastanud õpilastest (43%) on kunagi jaganud oma parooli ema või isaga. 401 õpilast (37%) ei ole kunagi parooli kellegi teisega jaganud, 145 vastajat (13%) on paroole jaganud ning 73 õpilast (7%) ei ole oma paroolide jagamises kindlad või ei mäleta seda (Joonis 15).



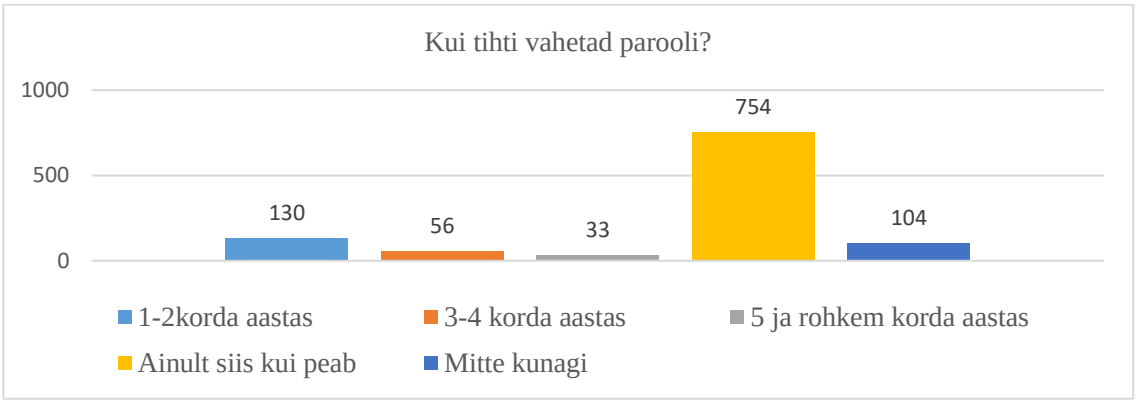
Joonis 15. Parooli jagamine

Oma vanematega jagavad paroole (Joonis 16) kõige rohkem 11-aastased tüdrukud – neid on 98 (9%), siis sama vanad poisid – 71 (7%). Kõige väiksemate arvudega on 15-16 aastased.



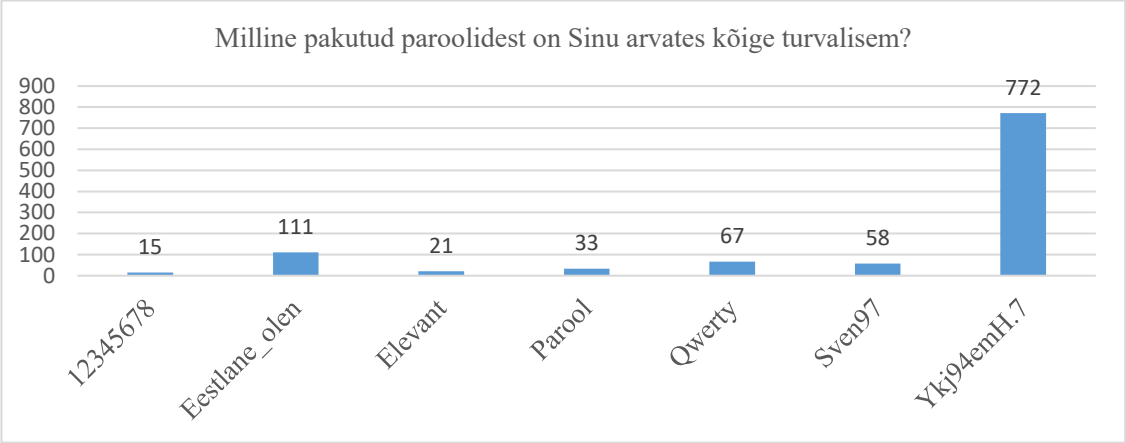
Joonis 16. Parooli jagamine emale/isale

Uuringus selgus, et suurem osavastajatest vahetab paroole (Joonis 17) vaid siis, kui peab – 754 (70%) vastajat. 130 (12%) õpilast vahetab paroole 1-2 korda aastas ning 104 (10%) õpilast ei tee seda enda sõnul kunagi. 3-4 korda aastas vahetab paroole 56 (5%) vastajat ning üle 5 korra aastas 33 (3%) õpilast.



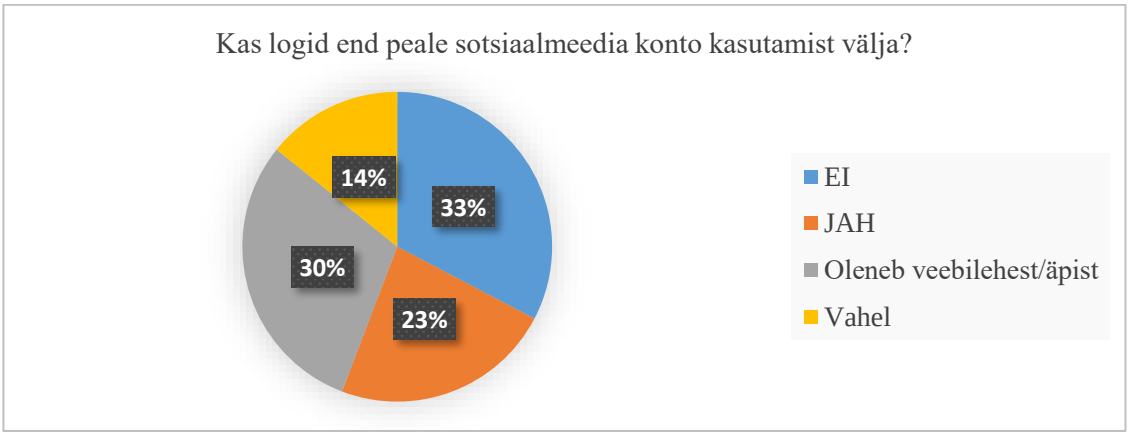
Joonis 17. Parooli vahetamine

Uuringus esitleti õpilastele valikut erinevatest paroolidest ning paluti nimetada üks parool, mida nad peavad enda arvates kõige turvalisemaks (Joonis 18). Selgus, et konkurentsitult peeti turvaliseimaks parooliks Ykj94emH.7. Seda arvamust jagas 71% (772 õpilast) vastanutest. 111 (10%) vastajat pidas kõige turvalisemaks parooliks Eestlane_olen_ja eestlaseks_j22n ning ülejäänuid variante peeti kõige turvalisemaks vähem.



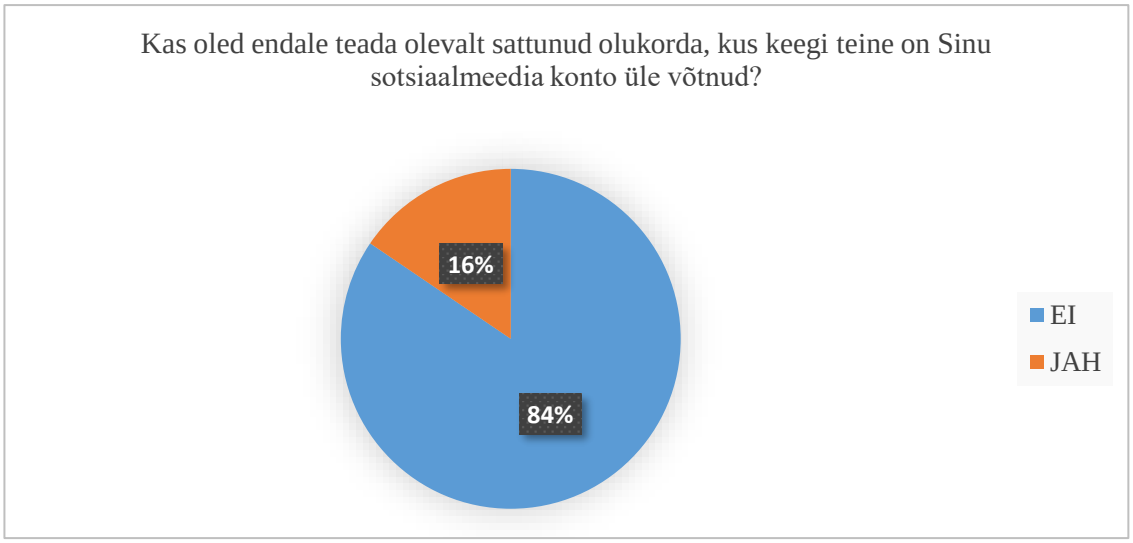
Joonis 18. Parooli turvalisus

Küsitluse tulemusena selgus, et sotsiaalmeedia kontolt kasutamise lõppemisel välja logimine tavapärane ei ole (Joonis 19). 352 vastajat (33%) ei tee seda, 323 vastajat (30%) teeb seda vastavalt kasutavale veebilehele/äpile ning 153 õpilast (14%) teeb seda vahel. Vaid 249 õpilast (23%) logib enda sõnul end peale sotsiaalmeedia konto kasutamist alati välja.



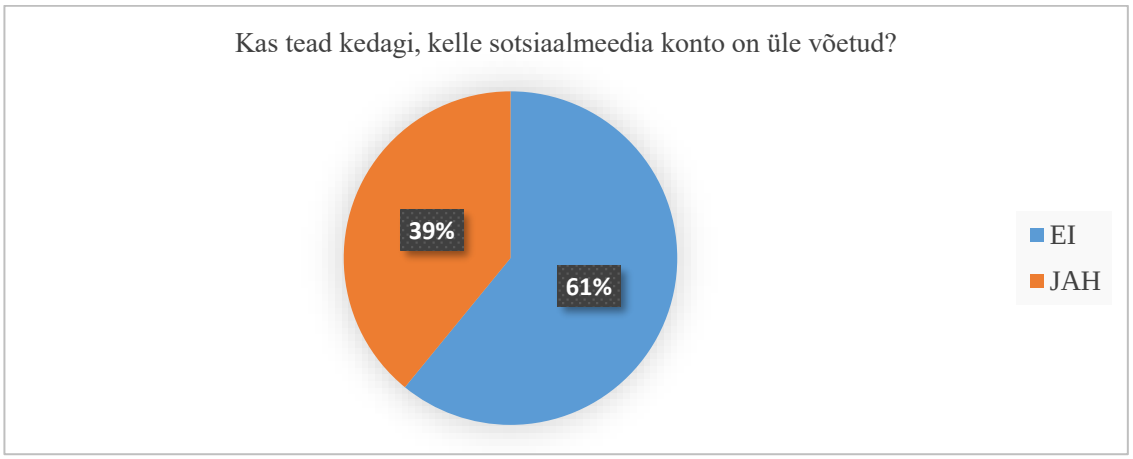
Joonis 19. Välja logimine

Küsitlusest selgus, et suurem osa küsitlusele vastanud õpilastest ei ole enda teada sattunud olukorda, kus keegi teine on nende sotsiaalmeedia konto üle võtnud (Joonis 20). Eitavalt vastas sellele 910 õpilast (84%) ning konto ülevõtmise kogemus on enda sõnul 167-l õpilasel (16%).



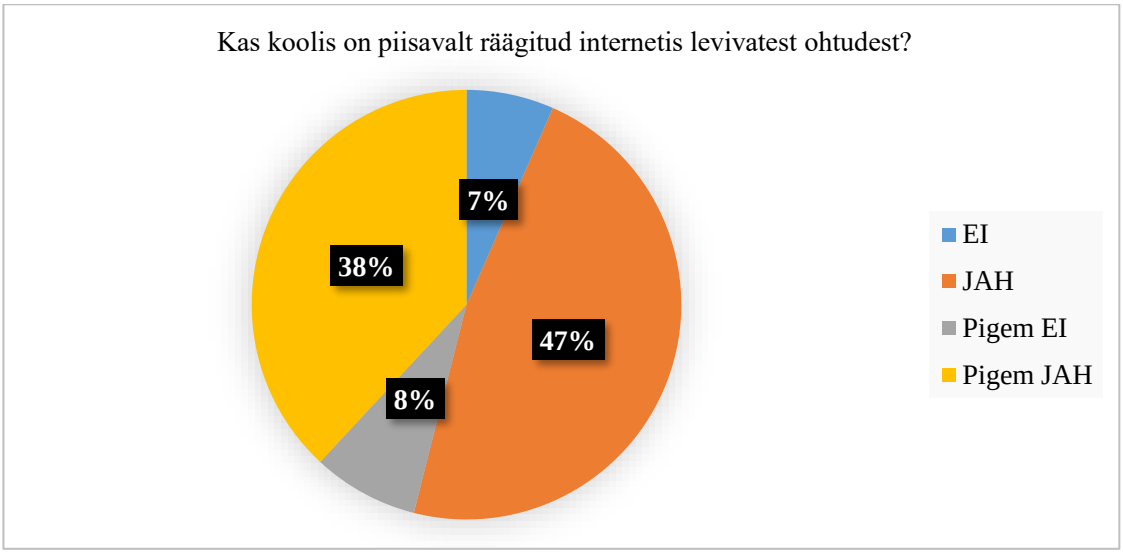
Joonis 20. Isikliku konto üle võtmine

Kui suur osa küsitlustele vastanud õpilastest vastas eitavalt enda konto kaaperdamise kohta, siis tunduvalt rohkem oli neid, kes teadsid kedagi, kelle konto on üle võetud. 656 (61%) õpilasel ei olnud ühtegi tuttavat, kelle sotsiaalmeedia konto on kaaperdatud ning 421 õpilast (39%) teadsid kedagi, kellega on see juhtunud (Joonis 21).



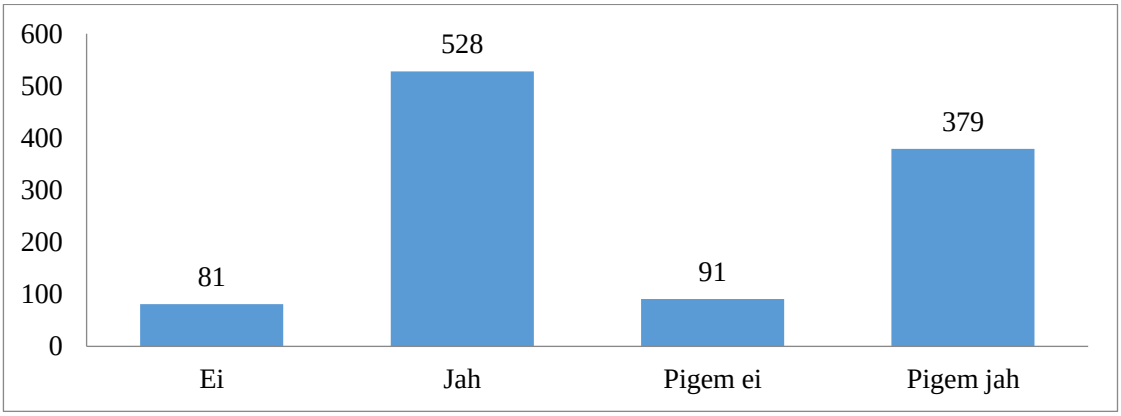
Joonis 21. Tuttava konto üle võtmine

Uurides, kas koolides räägitakse internetis levivatest ohtudest õpilaste arvates piisavalt, selgus, et suurema osa vastanute meelest seda tehakse (Joonis 22). 510 (47%) õpilase arvates seda tehakse ning 410 (38%) õpilase hinnangul pigem tehakse. 86 õpilast (8%) arvasid, et koolides ei tehta tõhusat tööd internetiohtude tutvustamiselt ning 71 õpilast (7%) arvas, et internetis levivatest ohtudest nende koolis kindlasti ei räägita.



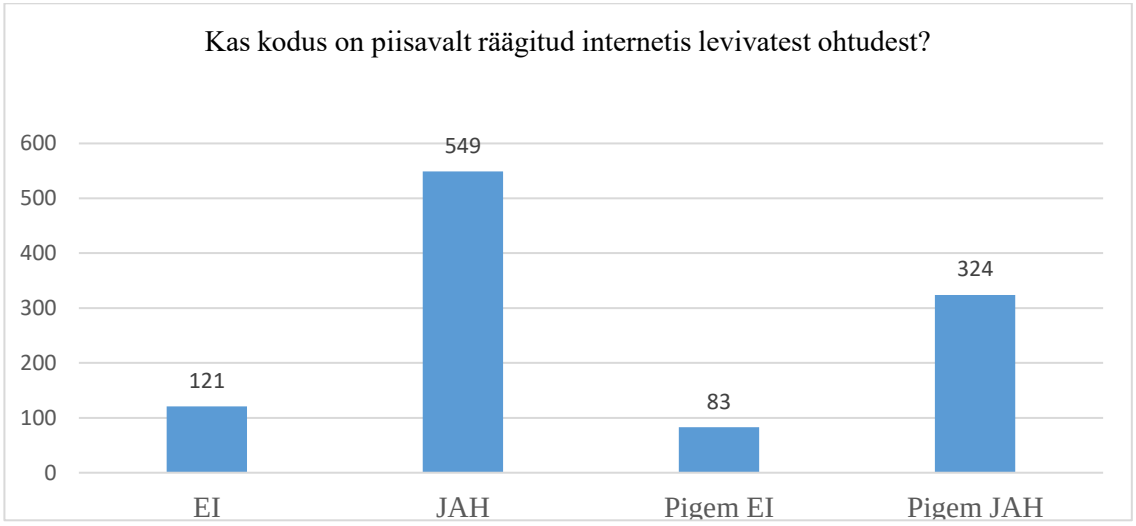
Joonis 22. Internetiohtude tutvustamine koolides

Sarnaselt oldi nõus, et koolis räägitakse lisaks internetis levivatele ohtudele ka sellest, kuidas nende ohtude eest end kaitsta (Joonis 23). 528 (49%) õpilast pidasid ohtude vastu kaitsmise tutvustamist piisavaks, „pigem jah“ vastas 379 (35%). Ebapiisavaks pidas 81 (8%) õpilast ning „pigem ei“ vastas 91 (8%).



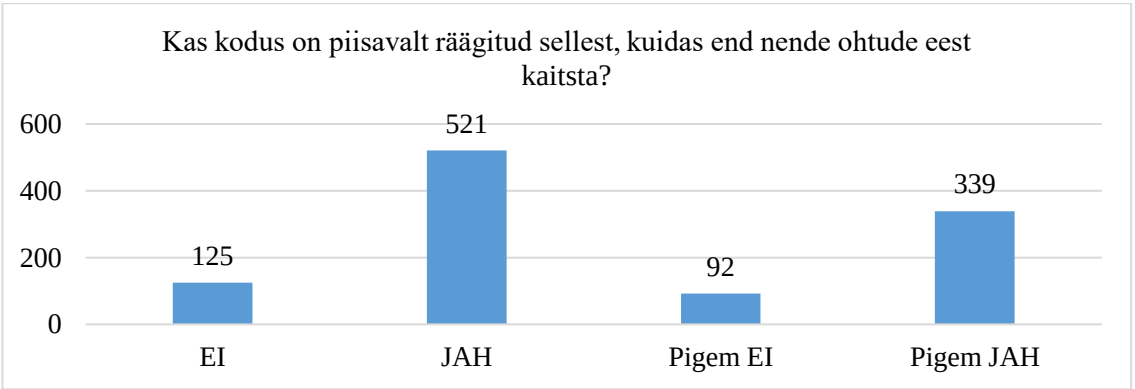
Joonis 23. Enda kaitsmise võimaluste tutvustamine koolides

Samuti uuriti, kas õpilaste kodudes räägitakse piisavalt internetis levivatest ohtudest (Joonis 24). Selgus, et ka kodudes on tehtud selgitustööd. 549 (51%) õpilast vastasid sellele küsimusele jaatavalt ning pigem jaatavalt vastas 324 (30%) õpilast. 83 (8%) õpilase kodus pigem ei räägita internetis levivatest ohtudest ning 121 (11%) õpilase kodus ei tehta seda üldse.



Joonis 24. Internetiohtude tutvustamine kodudes

Sarnased tulemused tulid ka, kui uuriti, kas lisaks kodus räägitud internetis levivatest ohtudest räägitakse ka sellest, kuidas nende ohtude eest end kaitsta (Joonis 25). Jaatavalt vastas 521 (48%) õpilast ning pigem jaatavalt 339 (31%) õpilast. 92 (9%) õpilase arvates neile kodus internetiohtude kohta selgitustööd ei jagata ning 125 (12%) õpilase arvates ei tehta seda kindlasti.



Joonis 25. Enda kaitsmise võimaluste tutvustamine kodudes

Vastustest küsimustele 14-17 võib järeldada, et tegelikult on küsitluses osalenud õpilaste koolides ja kodudes tehtud. Lisaks uuriti õpilaste arvamusi suurimate ohtude kohta juhul, kui keegi on nende (sotsiaalmeedia) konto kaaperdanud. Suurimateks ohtudeks pakkusid õpilased:

- *Et ta saab kõik minu andmed teada.*
- *Postitab väga naeruväärseid pilte ja kiusab*
- *Avaldab rõvedaid pilte*
- *Et hakatakse minu isiklikke asju, mis sellel kontol on, igale poole jagama*
- *Et hakatakse raha nõudma*
- *Saadetaks minu konto peal n2iteks viiiruseid.*
- *Et hakatakse asju rääkima, mis pole tõsi*
- *Et keegi ei taha enam minuga rääkida, kuna mu konto on igasuguseuid roppusi täis*
- *saadakse isiklikud andmed teada näiteks mu elukoha*
- *ta võib näha kõiki pilte või sõnumeid*
- *Raha, failide varastamine.*
- *parooli muutmine*
- *Saadab teisetele ebasündseid pilte või kirjutab solvanguid minu nime alt.*
- *avaldab paroolid ja pildid*
- *Võib hakkata teistele koledaid sõnumeid saata nt Facebookis sõpradele.*
- *Viirused.*

88 (8%) õpilast ei osanud konto kaaperdamise korral ühtegi ohtu nimetada. Enamik vastanutest pidas suurimaks ohuks isiklike piltide jagamist ning maine kahjustamist.

Lisaks paluti küsitluses osalenud õpilastel lisada muid mõtteid või probleeme salasõnade loomise või kasutamise kohta. Ankeetides toodi välja järgmised mõtted ja probleemid:

- *Kui sa tõesti ei tea, millist parooli endale panna, siis saab kasutada mingeid kellaaegu, sest keegi ei tea mis kell sa selle parooli panid ning siis mingid suvalised sõnad, mis ei ole sinuga seotud;*
- *Et kasutajaid kaitsta, siis peab looma samale kasutajale 5 parooli ja verification teisele kontole, et nad teaksid, et konto omanik on õige;*
- *Enamik inimesi kasutab enda isiklikke andmeid – probleem;*
- *Koolis võiks sellest rohkem rääkida;*
- *Kui lood endale konto, siis pead seda turvaliselt hoidma;*
- *Salasõna peaks olema minu arust vähemalt 10 tähemärki ning suur algustäht ja mingid suvalised numbrid;*
- *Osad lapsed kasutavad oma nimesid või sünniaegu paroolina ja seda on lihtne ära arvata;*
- *Ei tohi jagada oma parooli.*

4.2. Arutelu, järeldused ja soovitused

Uuringus selgus, et küsitluses osalenud koolinoored on aktiivsed interneti ja äppide, kus nõutakse ka kasutajanime ja parooli, kasutajad. Samas ei ole kasutajanimede ja paroolide kasutamine nii turvaline, kui võiks.

Uurides koolinoorte harjumusi paroolide loomisel ja kasutamisel, leiti, et enamus koolinoori kasutab erinevatel veebilehtedel sama parooli. Vaid 21% küsitlusele vastanutest kasutab erinevatel lehtedel ja kontodel erinevaid kasutajanimesid ja paroole. Sama kasutajanime ja parooli kasutamine erinevatel lehtedel on levinud praktika. Autor arvab, et tuleks koolinoortele selgitada, et selline harjumus võib viia olukorrani, et kui ühe konto andmed satuvad pahatahtliku inimese kätte, siis on haavatavad ka teised kontod. Selgus, et küsitlusele vastanud õpilased oskavad ära tunda keerukamaid ning turvalisemaid paroole. Paraku selgus, et koolinoored eelistavad paroolide loomisel meeldejäävamaid ja seega ka lihtsamaid paroole - üle kolmandiku vastanutest paroole selle järgi, et neil endil oleks seda lihtne meelde jätta, mis on ka paroolide loomise kõige populaarsem põhjus. Paroole luuakse ka juhuslikel viisidel või isiklikke andmeid kasutades. Magistritöö autori arvates võiks paroolide turvalisema kasutamise soodustamiseks õpetada informaatika tundides kooliõpilasi kasutama paroolihaldureid – paroolihaldur võimaldab salvestada kõik oma paroolid ning neile on võimalik ligi pääseda vaid ühe parooliga. Kooliõpilastele tuleks sisendada, et kasulikum on luua üks ja turvaline parool, kui mitu ebaturvalist parooli. Samuti võib praktiliste harjutustena kasutada informaatika tundides PSM-i kasutamist, mis näitaks õpilastele, millisest tasemest ja lihtsusastmest alates hindab programm tema loodud parooli piisavalt tugevaks. Lisaks võiks õpilastele tutvustada kaheastmelist autentimist või Mobiil-ID või Smart-ID kasutamise võimalusi. Soovi korral võiks koolides kehtestada soovitusliku küberhügieeni test, mille tase varieerub vastavalt klassile ning mille läbimine oleks kooliõpilastele motiveeriv. Soovitusi peaks esitlema ja kasutama õpilaste enda loodud paroolide kaitsmise vajalikusena, mitte õpetama ning soodustama neile teiste õpilaste paroolide kuritarvitamist.

Lisaks lihtsatele paroolidele on küsitlusele vastanud koolinoorte seas probleemiks ka paroolide regulaarne uuendamine – paroole vahetatakse vaid vastavalt vajadusele või siis,

kui süsteem seda nõuab. Positiivsena võib välja tuua, et suurem enamus vastanutest ei kirjuta oma loodud paroole kuskile üles ning kui paroole kellelegi üldse jagatakse, siis on need lapsevanemad. Autori arvates on igati positiivne, et vanemad on laste küberkäitumisest huvitunud, selgitavad neile erinevaid ohte ning pakutakse abi paroolide kasutamisel ning loomisel. Lapsevanematel tuleks eelkõige luua lapsega usalduslik side, et laps teda nii paroolide kui muu internetitegevusega kursis hoiaks.

Tähtis on, et nii koolides kui kodudes teadvustatakse ka õpilaste endi arvates internetis levivaid ohte ja riskikäitumisi ning osatakse ka selle vastu kaitsmiseks erinevaid soovitusi anda. Samuti saavad õpilased aru ohtudest juhul, kui nende sotsiaalmeedia konto võetakse üle. Seda osatakse seostada andmete lekkega ning kooli- ja/või küberkiusamisega. Võib öelda, et koolides ja kodudes tehakse tõhusalt teavitustööd ning õpilased on ohtudest teadlikud, kuid teavitustööd internetis levivatest ohtudest tuleks jätkuvalt teha ning suunata õpilasi looma ja kasutama turvalisemaid paroole.

Positiivne on, et nii enda kui tuttavate sotsiaalmeedia kontode kaaperdamisega ei ole suurem enamus küsitlustele vastanutest kunagi kokku puutunud. Sellest võib järeldada, et hoolimata lihtsate paroolide loomisest ning nende kasutamisest, ei ole küberkiusamine küsitlustele vastanud õpilaste seas kontode kaaperdamise näol väga levinud. Suure tõenäosusega on paroole lekkinud või neid mõtlematult levitatud, kuid neid ei ole kuritarvitatud.

Kokkuvõtvalt võib tuua esile, et kooliõpilaste teoreetilised teadmised paroolide loomise ja kasutamise kohta on üsna heal tasemel, kuid praktilised tegevused vajavad veel juurutamist.

Magistritöös uuriti ka, kuidas on käitumisökonoomikat kasutades võimalik suunata koolinoori looma tugevamaid paroole ning kaitsma nende turvalisust. Paroolide uuendamise vajalikkuse osas tuleks autori hinnangul teha rohkem teavitustööd või kasutada nügimist regulaarsemate paroolivahetuste poole. Ühe võimalusena võiks olla teavitamine hiljutisematest laiaulatuslikest paroolivargustest, tuues positiivsema näitena esile neid, kes regulaarselt parooli on vahetanud. Näiteks avastatakse paroolileke ning teavitatakse avalikkust sellest lekkest tunduvalt hiljem, kui leke tegelikult aset leidis – regulaarselt parooli vahetades on tunduvalt suurem tõenäosus, et võõra isiku poolt teada saadud parool vahetati vahetult peale selle lekkimist.

Samuti võiks regulaarselt avaldada või anda kõige aktuaalsem ülevaade Eestis (ja vastavate uuringute olemasolul ka Eesti koolides) kasutatavatest kõige levinumatest paroolidest, sealjuures tuua välja, et need on äraarvatavad, et mitte tekitada õpilastes „karjainstinkti“ mulje, et kuna seda kasutab suurem hulk eestlasi, on normaalsus sellisel tasemel paroole kasutada. See nügiks kooliõpilasi looma paroole erineva loogikaga (näiteks levinud parooli „123456“ puhul ei kasutataks parooli loomisel enam numbreid, kuna nende kasutamine tundub ebaturvaline) ning levinud paroolikujudest erinevaid paroole.

Magistritööd autor annab uurimistöö tulemusi analüüsides järgmised soovitused:

- Viia läbi rohkem uuringuid koolinoorte seas, mis on seotud küberhügieeni ja/või harjumustest paroolide loomisel ning kasutamisel. Tähtis on teha uuringuid kitsamatest vanusegruppides. Samuti tuleks uuringutel keskenduda erinevatele seostele. Näiteks, kas need koolinoored, kes arvavad, et koolides ning kodudes on tehtud piisavalt teavitustööd paroolide turvalisusest, loovad seetõttu ka tugevamaid salasõnu;
- Võimalusel viia informaatikatundides või -huviringides läbi praktilisi harjutusi nii PSM-ide osas kui ka kontroll- ning sekkumisgruppidega. Õpilastele kinnistuvad õiged ja valed käitumispraktikad läbi praktiliste harjutuste.
- Tutvustada kooliõpilastele kaheastmelist autentimist, paroolihaldureid jms parooli loomise programme eelkõige nutitelefonide näidetel.
- Võimalusel luua koolides iga-aastane interaktiivne küberhügieeni kursus ja test.
- Läbi negatiivsete, reaalsest elust pärit näidete, proovida nügida õpilasi kasutama keerukamaid paroole ning kinnistada harjumust neid regulaarselt vahetada.
- Erinevad era- või riigiettevõtted võiksid ära kasutada käitumisökonoomika võimalusi suunamaks koolinoori turvalisemate paroolide loomiseks ning kasutamiseks. Selleks tuleb hoolega disainida nügimistrateegia, mis arvestab kõikide eetikareeglitega.

Kui avalikud asutused on koostöös veebilehekülgede ning nutirakenduste haldajatega valmis panustama ressursse eetilise nügimisstrateegia loomiseks, võib see autori hinnangul anda aluse koolinoorte heade küberhügieeni harjumuste välja kujunemiseks. Oluline on nügimiste katsetamine uuringute käigus. Samuti on tähtis jätkata ja tõhustada

koolides teavitustööd internetis levivatest ohtudest ning turvaliste paroolide ning kasutamise harjumustest.

KOKKUVÕTE

Eesti koolinoored teevad tutvust arvutite ja internetiga aina nooremas eas, seega tuleb üha nooremas eas keskenduda lisaks interneti hüvedele ja *online*-riskide teadvustamisele ning nügida kooliõpilasi internetis turvalisemate valikute tegemise poole. Kuigi riiklikul tasandil on seatud eesmärgiks iga koolilõpetaja baasteadmiste omandamine küberohtudega toimetulekuks, on oluline küberteadlikkust tõsta juba nooremate õpilaste seas, kes puutuvad igapäevaselt kokku erinevate (sotsiaalmeedia)kontodega ning kontodega seotud paroolidega. On oluline, et koolinoored teadvustaksid parooli tugevuse tähtsust ning lisaks teadvustamisele ka looksid ning kasutaksid paroole vastavalt parimatele praktikatele. Tänu sellele suureneb koolinoorte küberhügieen ning langeb küberkiusamise ohvriks langemise risk.

Käesoleva uurimistöö eesmärgiks on uurida koolinoorte harjumusi paroolide loomisel ning kasutamisel. Lisaks püstitati magistritöös järgmised uurimisküsimused:

1. Millised on koolinoorte harjumused paroolide loomisel ja kasutamisel?
2. Millised vahendeid on varasemalt kasutatud, et nügida inimesi turvalisemate paroolide suunas?

Uuringu läbiviimisel kasutati kvantitatiivset andmekogumismeetodit - ankeetküsimustikku.

Uuringus selgus, et küsitluses osalenud koolinoored on aktiivsed interneti ja äppide kasutajad, kus nõutakse ka kasutajanime ja parooli. Paraku ei kasuta koolinoored kasutajanimesid ning paroole piisavalt turvaliselt, kuigi koolides ning kodudes tehakse aktiivset teavitustööd. Paroole luuakse tihti juhuslikel viisidel või isiklikke andmeid kasutades, samuti ei vahetata neid piisavalt tihti. Positiivne on, et paroolide üleskirjutamine ning jagamine ei ole levinud ning õpilastel on olemas teadlikkus keerukamate ning turvalisemate paroolide olemusest ning tähtsusest. Positiivne on, et koolinoorte endi ja tuttavate sotsiaalmeediakontode kaaperdamine ei ole nende sõnul levinud.

Tööst selgub, et kõige sagedasemaks nügimisviisiks turvaliste paroolide valimiseks on parooli tugevuse mõõtja (PSM), mis on ka laialdaselt levinud.

Kindlasti on vajalik edasised uuringuid koolinoorte seas, et tuvastada ja/või kinnitada probleemid paroolide loomisel ning nende kasutamisel. Seejärel on võimalik luua eesmärgipärane ning eetiline nügimisstrateegia harjumuste parandamiseks.

Käesoleva magistritöö autori arvates said töös püstitatud uurimisküsimused ammendavad vastused.

Autor loodab, et antud töö näitab vajadust edasiste uuringute läbi viimiseks ning tõstab teadlikkust käitumisökonoomika võimaluste kasutamisest.

KASUTATUD KIRJANDUS

Alexander, K., jt. (1997). Guidelines for usability testing with children. *Interactions,* lk 9-14.

Ammi, M. jt. (2017). Using social injunctive norms to nudge usersto build green houses / El empleo de normasprescriptivas sociales para animar a los usuarios aconstruir casas ecológicas. *Psyecology Revista Bilingüe de Psicología Ambiental / Bilingual Journal of Environmental Psychology,* 8 (3), lk 297-322

Andmekaitse ja infoturbe leksikon. Kättesaadav arvutivõrgus: https://akit.cyber.ee/term/9143 (24.03.2019).

Balz, J. P, jt. (2010). Choice Architecture. Kättesaadav arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583509 (10.05.2019).

Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: Worth Publishers.

Bavel, R., jt. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123, lk 29-39.

Benartzi, S., jt. (2017). Should Governments Invest More in Nudging? *Psychological Science,* 28, lk 1041-1055.

Brocke, J., jt. (2016). Digital Nudging. *Business & Information Systems Engineering*, 58, 6, lk 433–436.

Cain, A. A. jt. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, lk 36-45.

Catalina, G., jt. (2014). Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet The risks faced by adolescents on the Internet: minors as actors and victims of the dangers of the Internet. *Revista Latina de Comunicación Social*, 69, lk 462-485.

Child, J. W. (1994). Can Libertarianism Sustain a Fraud Standard? *Ethics,* 104, 4, lk 722-738.

Choong, Y-Y., jt. (2019). Case Study – Exploring Children's Password Knowledge and Practices. *Proceedings 2019 Workshop on Usable Security (USEC)* Internet Society.

Chouseinoglou, O., jt. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, lk 83-93.

Cialdini, R. B. (2006). Influence: The Psychology of Persuasion, *Harper Business.*

Clarke, N., Furnell, S. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31, 8, lk 983-988.

Decker S., Sieverding M., Zimmermann F. (2010). Information about low participation in cancer screening demotivates other people. *Psychol Sci*, 21(7), lk 941-943

Denham, N., jt. (2016). Secure modular password authentication for the web using channel bindings. *International Journal of Information Security*, 15, 6, lk 597-620.

Duffy, S. W., Myles, J. P., Maroni, R. (2016). Rapid review of evaluation of interventions to improve participation in cancer screening services. *Journal of Medical Screening*, 24, 3, lk 127-145

Duggan, G. B., jt. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, 70, 6, lk 415-431.

Egelman, S., jt. (2013). Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, lk 2379-2388

Euroopa Komisjon. (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.

Euroopa Parlament. (2016). Cyberbullying among Young People. Kättesaadav arvutivõrgus: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf (28.10.2018).

Florencio, D., Herley, C. (2007). A Large-Scale Study of Web Password Habits. *The 16th international conference on World Wide Web*, lk 657-666.

Furnell, S. (2001). Cybercrime: vandalizing the information society. *Web Engineering International Conference*, lk 8-16.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security*, 26, (7-8), lk 445-451.

Garaigordobil, M., Martínez-Valderrey, V. (2014). Effect of Cyberprogram 2.0 on Reducing Victimization and Improving Social Competence in Adolescence. *Revista de Psicodidáctica,* 19, 2, lk 289-305.

Glaeser, E. L. (2006). Paternalism and Psychology. The University of Chicago Law Review 73, 1, lk 133-156.

Glassmann, M, Vandenwauver, M. (2009). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 3, lk 233-244.

Goodin, D. (2012). Why passwords have never been weaker—and crackers have never been stronger. Ars Technica. Kättesaadav arvutivõrgus: https://arstechnica.com/information-technology/2012/08/passwords-under-assault/ (13.03.2019).

Government Office for Science. (2014). Using behavioural insights to improve the public' s use of cyber security best practices. Kättesaadav arvutivõrgus: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (29.10.2018).

Griffin, R. J., jt. (2000). Protection Motivation and Risk Communication. *Risk Analysis*, 20, 5, lk 721-734.

Hainsalu, O. (2017). Kuidas valida hea parool, mis ei unune? *Digi*, 150, 7. Kättesaadav arvutivõrgus: https://dea.digar.ee/cgi-bin/dea?a=d&d=AKdigi201710.2.29.4 (13.03.2019).

Han, W., jt. (2018). Shadow Attacks based on Password Reuses: A Quantitative Empirical View. IEEE Transactions on Dependable and Secure Computing, 15, lk 309 – 320

Helsper, E. J., Kalmus, V., jt. (2013). Country classification: opportunities, risks, harm and parental mediation. Kättesaadav arvutivõrgus: http://eprints.lse.ac.uk/52023/1/Helsper_Country_classification_opportunities_2013.pdf (28.10.2018).

Hinduja, S., Patchin, J. W. (2014). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* Thousand Oaks, CA: Corwin.

Höysniemi, J., jt. (2003). Half-Day Tutorial: Evaluating Interactive Products for and with Children. *Human-Computer Interaction*, lk 1027-1028.

Infosüsteemide turvameetmete süsteem ISKE. M 2.11 Paroolide kasutamise reeglid. Kättesaadav arvutivõrgus: https://iske.ria.ee/8_03/ISKE_kataloogid/7_Kataloog_M/M2/M_2.11 (13.03.2019).

Justiitsministeerium. (2018). Kriminaalpoliitika põhialused aastani 2030. Eelnõu. Seletuskiri.

Kahneman, D., Tversky, A. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, 211 (4481), lk 453-458.

Kaljulaid, K. (2017). Keynote speech at the European Defence Agency Annual Conference "Security in the digital age: the added value of European cooperation". Kättesaadav arvutivõrgus: https://www.president.ee/en/official-duties/speeches/13766-keynote-speech-at-the-european-defence-agency-annual-conference-qsecurity-in-the-digital-age-the-added-value-of-european-cooperationq-/index.html (13.03.2019).

Khern-am-nuai, W., jt. (2017). Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment. *Proceedings of the 50th Hawaii International Conference on System Sciences*, lk 587-596.

Kuustemäe, M. (2015). 6. ja 9. klassi õpilaste hinnangud enda digipädevustele. Magistritöö, Tartu Ülikool.

Küberturvalisuse seadus. -RT I, 22.05.2018, 1.

Lorenz, B., Kikkas, K. (2019). Digitaalne kirjaoskus infoühiskonnas. Kättesaadav arvutivõrgus: https://entk.ee/wp-content/uploads/2019/02/1-2-birgy-ja-kaido.pdf (01.04.2019).

Luik, P., Naruskov, K. (2015). Küberkiusamise fenomeni tajumine Eesti õpilaste seas: sooline võrdlus kiusamise kriteeriumite ja liikide alusel. *Eesti Haridusteaduste Ajakiri*, 3, (2), lk 186–215.

Maddux, J. E., Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19, 5, lk 469-479.

Majandus- ja Kommunikatsiooniministeerium. (2018). Küberturvalisuse strateegia 2019-2022.

Marcano-Olivier, M. jt. (2019). A low-cost Behavioural Nudge and choice architecture intervention targeting school lunches increases children's consumption of fruit: a cluster randomised trial. International Journal of Behavioral Nutrition and Physical Activity, 16, lk 20.

Miller, C. jt. (2012). Measuring the Food Environment: A Systematic Technique for Characterizing Food Stores Using Display Counts. *Journal of Environmental and Public Health*, 2012, lk 1-6.

Mullainathan, S., Thaler, R. (2015). Behavioral Economics. International Encyclopedia of the Social & Behavioral Sciences (Second Edition), lk 437-442.

Oravec, J. A. (2017). Emerging "cyber hygiene" practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. 2017 IEEE International Professional Communication Conference (ProComm).

Peled, Y. (2019). Cyberbullying and its influence on academic, social, and emotional development of undergraduate students. Heliyon, 5, 3.

Punch, S. (2002). Research with Children: The Same or Different from Research with Adults? *Childhood*, 9, 3, lk 321-341.

Rauber, J., jt. (2017). Behavioral Insights All Over the World? Public Attitudes Toward Nudging in a Multi-Country Study. Kättesaadav arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921217 (10.05.2019).

Reisch, L. A., Sunstein, C. R. (2016). Do Europeans like nudges? *Judgment and Decision Making*, 11, 4, lk 310–325.

Renaud, K., Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies, 120, lk 22-35.

Shen, C. jt. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, 61, lk 130-141.

Strauss-Raats, P. (2013). Kuidas töötajaid soodsas suunas mõjutada? Tööinspektsiooni infokiri. Kättesaadav arvutivõrgus: https://www.ti.ee/fileadmin/user_upload/failid/dokumendid/Meedia_ja_statistika/Teavitustegevus/Infokirjad/2013/infokiri_nr_28/detsember2013_tookeskkond1.pdf (29.10.2018).

Sunstein, C. R. (2017). Nudges that fail. *Behavioural Public Policy*, 1, 1, lk 4-25.

Sunstein, C. R. (2015). The Ethics of Nudging. Yale Journal on Regulation, 32, 2, lk 413-450.

Sunstein, C. R., Thaler R. H. (2018). Nügimine. viis toetada valikuid, mis viivad tervise, jõukuse ja õnneni. Tallinn: Tänapäev.

Tartu Ülikooli Johan Skytte poliitikauuringute instituudi kirjalike tööde koostamise ja vormistamise juhend. Kättesaadav arvutivõrgus: https://skytte.ut.ee/et/oppimine/oppematerjalid-juhendid-1 (03.01.2019).

The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius. Kättesaadav arvutivõrgus: https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705 (13.03.2019).

Turow, J. (2011). *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven: Yale University Press.

Täht, K. (2015). Õpilaste eluga rahulolu ning sellega seotud tegurid PISA 2015 uuringu näitel, Tartu Ülikool. Kättesaadav arvutivõrgus: https://www.innove.ee/wp-content/uploads/2017/11/%C3%95pilaste-rahulolu-PISA-2015.pdf (09.02.2019).

Weir, M., jt. (2010). Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. *Proceedings of the 17th ACM conference on Computer and communications security*, lk 162-175

West, R. (2008). The Psychology of Security. *Communications of the ACM*, 51, 4, lk 34–41.

LISAD

Lisa 1. Ankeetküsitlus

Üldandmed

Vanus

Sugu

Küsimused

1. Kas kasutad aktiivselt veebilehti/äppe, kus on vajalik kasutajanimi ja parool?

    - Jah
    - Ei

2. Kas kasutad erinevatel lehtedel sama kasutajanime ja parooli?

    - Jah
    - Ei
    - Vahel

3. Mille järgi valid parooli?

    - Et oleks lihtne meelde jätta
    - Et oleks võimalikult lühike
    - Et kellelgi teisel oleks raske ära arvata
    - Muu variant

4. Kui vastasid eelmisele küsimusele "Muu variant", siis palun täpsusta enda vastust.

5. Kuidas lood endale salasõna?

    - Kasutan salasõna loomise äppe
    - Kasutan enda nime, sünniaega ja/või muid isiklikke andmeid
    - Kasutan suvalisi kombinatsioone
    - Kasutan meeldejäävaid sõnu
    - Kuidas kunagi
    - Muu meetod

6. Kui vastasid eelmisele küsimusele "Muu meetod", siis palun täpsusta enda vastust.

7. Kas kirjutad oma parooli tavaliselt kuhugi üles?

    - Jah
    - Ei

8. Kas oled kunagi jaganud oma parooli kellelegi teisele?

    - Jah
    - Ei
    - Ainult oma emale/isale
    - Ei ole kindel/ ei mäleta

9. Kui tihti vahetad parooli?

    - Mitte kunagi
    - Ainult siis, kui peab.
    - 1-2 korda aastas
    - 3-4 korda aastas
    - 5+ korda aastas

10. Milline pakutud paroolidest on Sinu arvates kõige turvalisem?

    - parool
    - Sven97
    - elevant
    - Eestlane_olen_ja_eestlaseks_j22n!
    - Ykj94@mH.7
    - 12345678
    - Qwerty

11. Kas logid end peale sotsiaalmeedia konto kasutamist välja (isiklikust nutiseadmest)?

    - Jah
    - Ei
    - Vahel
    - Oleneb veebilehest/äpist

12. Kas oled endale teada olevalt sattunud olukorda, kus keegi teine on Sinu sotsiaalmeedia konto üle võtnud?

    - Jah
    - Ei

13. Kas tead kedagi, kelle sotsiaalmeedia konto on üle võetud?

    - Jah
    - Ei

14. Kas koolis on piisavalt räägitud internetis levivatest ohtudest?

    - Jah
    - Pigem jah
    - Ei
    - Pigem ei

15. Kas koolis on piisavalt räägitud sellest, kuidas end nende ohtude eest kaitsta?

    - Jah
    - Pigem jah
    - Ei
    - Pigem ei

16. Kas kodus on piisavalt räägitud internetis levivatest ohtudest?

    - Jah
    - Pigem jah
    - Ei
    - Pigem ei

17. Kas kodus on piisavalt räägitud sellest, kuidas end nende ohtude eest kaitsta?

    - Jah
    - Pigem jah
    - Ei
    - Pigem ei

18. Mida pead suurimaks ohuks, kui keegi on Sinu konto üle võtaks?

Lisa vajadusel muid mõtteid või probleeme salasõnade loomise või kasutamise kohta.

STUDENTS' PASSWORD CREATION AND MANAGEMENT HABITS AND POSSIBILITIES OF NUDGING TOWARDS SAFER CHOICES

Krista Valli

Summary

In today's information society, children are starting to use the computer and the internet at a younger age, which offers opportunities to develop their horizons and spend their leisure time. However, in addition to the positive aspects, children are also vulnerable to cyber threats. To protect themselves from these threats, children must be aware of them and be able to navigate the Internet as safely as possible.

One of the easiest ways to reduce the risk of being a victim of a cyber-attack (for example cyber-bullying) is creating a strong password and keeping it safe. This Master's thesis examines the habits of students in creating and using passwords. To do this, the author has conducted a survey among students aged 9 to 16 in different schools in Estonia.

The survey conducted by the author revealed that most students are aware of the dangers of using a weak password. They are also familiar with the recommendations for a secure password. However, they often choose a weak password and do not update it regularly.

As a solution, the author suggests using the knowledge of behavioral economics to nudge children towards making safer choices.

Little research has been done to find out how children create and manage passwords, and so far no research has been published in Estonia. Thus, one of the motives of this Master's thesis is to fill this gap and offer an input into further research. It is also proposed to use the knowledge of behavioral economics and its possibilities for raising the awareness of strong password management, and trying to create good habits at an early age and making them stick.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Krista Valli,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Koolinoorte harjumused paroolide loomisel ja kasutamisel ning võimalused nende nügimiseks turvalisemate valikute suunas“, mille juhendajad on Leonore Riitsalu ja Madis Raaper, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Krista Valli

20.05.2019