TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Mari-Liis Üürike 153520IABM

TÄISKASVANUD TÖÖTAJA KÜBERHÜGEENI ALASED PÄDEVUSED

Magistritöö

Juhendaja: Birgy Lorenz
PhD

Tallinn 2018

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Mari-Liis Üürike

07.05.2018

Annotatsioon

Üha rohkem kasutavad inimesed töö- ja eraelus interneti ning arvutit. Lisaks võimalustele käivad internetiga kaasas ka erinevad ohud, millest kasutajad alati teadlikud ei ole. Eesti küberjulgeoleku strateegia üheks punktiks 2014-2017. aastatel on avalikkuse teadlikkuse tõstmine küberohtudest. Uus strateegia on alles koostamisel ja hakkab kehtima 2019. aastal.

Lõputöö idee sai autor Birgy Lorenz'i doktoritööst *„A digital safety model for understanding teenager internet user's concerns".* Kuna küberhügieeni ehk digitaalsete turvalisust puudutavaid oskuseid on pigem uuritud õpilaste hulgas, siis autor valis siinses magistritöös sihtgrupiks just täiskasvanud töötajad, et teada saada, kas täiskasvanud on küberhügieenis teadlikumad. Seetõttu keskendutakse siinses magistritöös täiskasvanud töötajate küberhügieeni alastele pädevuste uurimisele. Autor uurib läbiviidud internetiküsitluste kui ka intervjuude põhjal, kui pädevaks hindavad täiskasvanud töötajad oma küberhügieeni alaseid oskuseid täna ja millised on ootused küberhügieeni alaste oskuste tõstmiseks.

Antud uurimuse metoodikaks valiti e-küsitlus ja intervjuud. On oodatud, et vastajad on keskmised digikasutajad, kelle küberhügieeni tase on pigem madal, sellele ootusele annab tuge eelnevalt Eestis läbi viidud PIAAC (rahvusvaheline täiskasvanute oskuste uuring) uuring. Magistritöös uuritakse ka olukorda töökeskkonnas. Selle tulemusena saavad tööandjad sisendi, mida peaks küberhügieeni alal oma töötajatele selgitama, et tagada oma äri parim toimimine ka digivahendeid kasutades. Magistritöö lõpus antakse soovitused täiskasvanute teavitusprogrammide ja küberhügieeni alaste koolituste paremaks planeerimiseks.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 45 leheküljel, 7 peatükki, 9 joonist, 2 lisa.

Abstract

Cyber Hygiene Competencies of Mature Employee

Increasing number of people are using internet and computers in work and private life daily. With vast benefits of the internet, there is also several cybersecurity threats of which users can be unaware of. Estonian cybersecurity strategy in 2014-2017 focused on raising awareness of cyber threats. The new strategy is under development and is released in 2019.This work focuses on adult employee cyber hygiene awareness. The author investigates adult employee cyber hygiene awareness and their expectations for improvement in the future.

This thesis was inspired by supervisor Birgy Lorenz doctoral thesis „A digital safety model for understanding teenager internet user's concerns". Since cyber hygiene awareness investigations have mostly focused on school children, therefore this work focuses on the same topic, but on adult employees. The goal was to understand how aware they are and what help they might need in this matter.

From the study, the author found out that adult employees rate themselves highly skilled in communication in the digital environment and they have learned the skills by themselves using online websites. Skills to cope with different situations comes from awareness level and attitude to the challenge itself. For example, in the eyes of the respondents, the piracy is considered a mild crime, as ransomware is considered to be high risk, where respondents are lacking know-how how to deal with the issue, therefore solving the situation gets complicated. When getting the virus, people will give advises like destroy the computer, hire a hacker or call web police (who most likely cannot help anyway)? Also, cyber hygiene in the work environment was investigated, which gathered many new challenges and ideas how an employer could address cyber hygiene issues. Employees see employers responsible for raising their cyber hygiene awareness, as it is good for business security as well.

At the end of the thesis recommendations for creating adult cyber hygiene awareness programs and strategies for the program managers and employers are given.

The thesis is in estonian and contains 45 pages of text, 7 chapters, 9 figures and 2 annexes.

Lühendite sõnastik

EU	*European Union*, Euroopa Liit
IT	*Information technology*, Infotehnoloogia
RIA	Riigi Infosüsteemide Amet
HM	*Her Majesty's Government*, Inglismaa Valitsus
NHS	*National Health Service*, Riiklik Tervisehoiu Amet
P2P	*Peer-to-Peer*, Partnervõrk
NETS	*National Educational Technology Standards for Teachers*, Rahvuslik Haridustehnoloogia Standard Õpetajatele
GDPR	*General Data protection Regulation*, Üldinne Andmekaitse regulatsioon
IMD	*Institute for Management Development*, Juhtimisarengu Instituut
PIAAC	*Programme for the International Assessment of Adult Competencies*, Rahvusvaheline programm täiskasvanute pädevuse hindamiseks

Sisukord

Jooniste loetelu

1 Sissejuhatus

Tänapäeval infoühiskonnas toimimiseks pole võimalik inimestel läbi saada arvutite ja internetita – vajame seda nii isiklikus kui tööelus. Lisaks infotehnoloogia võimaluste kasutamisele peaks tavainimeste hulgas saama igapäevaseks ka tegelemine erinevate tehnoloogiliste riskide ja ohtudega, et tagada enda ja oma tööandja ettevõtte turvalisus. Paljud arvuti- ja nutikasutajad ei ole kahjuks viimastega piisavalt kursis. Eesti 2014-2017 aasta küberjulgeoleku strateegia üheks oluliseks eesmärgiks oli avalikkuse teadlikkuse tõstmine küberohtudest, mille üheks võimaluseks on teavitustöö üldsusele ja koolituste tegemine riskide märkamiseks, et ohu realiseerudes adekvaatselt hakkama saada [1].

Autor valis lõputöö teemaks täiskasvanud töötaja küberhügieeni alased pädevused. Täiskasvanud töötajad valiti sihtrühmaks seetõttu, et digitaalse ohutuse alased uuringuid on Eestis pigem tehtud noorte hulgas, kuid mitte niipalju täiskasvanute hulgas. Autoril oli isiklik huvi teada saada, kuidas ja millist nõu peaks teadlased ettevõtete juhtidele ja ka strateegiate ning teavitusprogrammide loojatele andma, et ka täiskasvanud saaks küberhügieeni alal paremaks. Lõputöö idee sai autor juhendaja Birgy Lorenz´i doktoritööst „*A digital safety model for understanding teenager internet user's concerns*“ [2].

Digioskuste ja küberhügieeni valdkonna uurimisel selgus, et nii Euroopa Liidus ja ka Eestis on õigus olla rahulolematu – liiga palju inimesi ei ole veel digipädevusi omandanud, veel vähem küberhügieeni, mis on saamas takistuseks Eesti jätkuvale eduloole digimaailmas. Eesti olukorra võrdlus teiste riikide arenguga on leitav peatükis 2. Paljude küberkuritegude õnnestumine on põhjustatud nii tavainimeste puudulikest oskustest, teadmistest ja suhtumises. Arvatakse, et digitaalne vara pole nagu „päris“ vara, mille tagajärjel näiteks ei mõtle inimene läbi piraaditud programmi või viirusega faili allalaadimisel, et sellega võidakse avada uks pahalastele oma arvutisse või nutiseadmesse (vt 3.).

Kirjanduse ja alusmaterjalide uurimise tulemusel sai selgeks, et magistritöö põhifookuseks tuleb valida nii täiskasvanud töötajate küberhügieeni alased pädevused

läbi enesehinnangu, kui ka uuringus osalejate ootused teavitustööle ja koolitustele. Selleks, et tõsta planeeritud uuringu valiidsust, kaasati väliseksperte, et mõista paremini tänast digirohket töökeskkonda, mille tarbeks küberhügieeni alaseid oskuseid parendadama peaks.

Kokkuvõtvalt on vastava magistritöö eesmärkideks teada saada:

- milliseks hindavad täiskasvanud töötajad oma küberhügieeni alaseid pädevusi
- millised on töötajate ja tööandjate ootused küberhügieeni oskuste parendamiseks

2 Küberhügieen

Antud peatükis tutvustatakse, miks digioskuste parendamine on Euroopa Liidus ja Eestis üks prioriteetsemaid teemasid. Vaadeldakse, mida tähendab küberhügieen, milline on Eesti olukord küberhügieeni valdkonnas võrreldes muu maailmaga ja kuidas võiks tavaline arvutikasutaja oma oskuseid lihtsate võtetega parendada.

2.1 Küberkaitse strateegiatest ja edukuse mõõtmisest Euroopas ning Eestis

Hetkel kehtib Euroopas EU poolt 2013. aastal välja antud küberkaitse strateegia *„Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*“. Uue strateegia väljaandmine on planeeritud 2019. aastasse. Strateegia üheks üldiseks eesmärgiks on võrgukeskkonna kaitse, mis tagaks kasutajatele võimalikult suure vabaduse ja turvalisuse. Antud strateegias esitatud Euroopa Liidu nägemus on sõnastatud viies strateegilises prioriteedis, millega on võimalik tutvuda eelnimetatud raportis [3]. Antud magistritööga kaudselt seotud eesmärk on:

- digiteadlikkuse suurendamine, näiteks 2013 aastal kutsus Euroopa Liit ühendriike organiseerima igaaastast „Küberturvalisuse kuud“ ja julgustas ettevõtteid andma kõikide tasandite töötajatele küberjulgeoleku alaseid teadmisi [3].

Hetkel kehtib Eestis Küberjulgeoleku Strateegia 2014-2017, mida pikendati 2018. aastaks ja uus valmib 2019. aastaks. Strateegia üheks üldiseks eesmärgiks oli nelja aastaga suurendada küberturvalisuse alast võimekust ja inimeste teadlikkust küberohtudest, tagamaks jätkuvat usaldust küberruumi vastu.

Olukord enne 2014. aastat näitas, et Eestis:

- 2009. aastal asutati Vabariigi Valitsuse julgeolekukomisjoni juurde küberjulgeoleku nõukogu, mille ülesanne oli strateegilisel tasandil toetada

ametkondade vahelist koostööd ja teostada järelvalvet küberjulgeoleku strateegia eesmärkide ellu viimist;

- 2010. aastal sai Riigi Infosüsteemide Amet täiendava volitused ja vahendid riigi info ja kommunikatsioonitehnoloogia infrastruktuuri kaitse korraldamiseks ja infosüsteemide turvalisuse üle järelvalve teostamiseks;
- 2011. aastal moodustati riigi- ja erasektori koostöö arendamiseks Kriitilise informatsiooni infrastruktuuri komisjon (KIIK);
- 2012. aastal koondati Politsei- ja Piirivalveameti (PPA) küberkuritegude uurimise võimekus ühte talitusse;
- 2013. aastal asutati prefektuurides küberkuritegude ja digitaaltõendite teenistused [1].

Täpsemalt on võimalik lugeda tehtud kohta „Küberjulgeoleku Strateegia 2014-2017“ ülevaatest [1].

Eesmärgid aastateks 2014-2017 (pikendatud kuni 2018) on jaotatud alameesmärkideks, mis omakorda koosnevad kindlatest tegevustest. Alameesmärkidel on oluliste teenuste infosüsteemide kaitse tagamine, riigikaitseliste võimete arendamine küberkaitse valdkonnas, küberkuritegevuse vastase võitluse tõhustamine ja võimalike küberjulgeolekuohtude maandamine kui ka valdkonnaülesed tegevused [1].

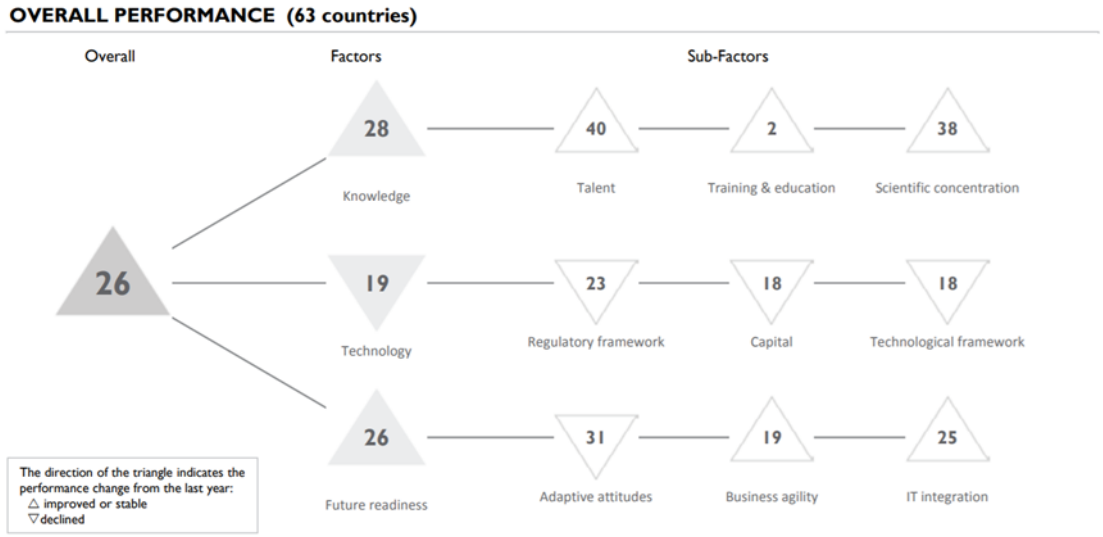
Antud magistritööd puudutavad kaudselt järgmised alameesmärgid:

- avalikkuse teadlikkuse tõstmine küberohtudest;
- riigikaitse valdkonna küberkaitse kõrge teadlikkuse tagamine;
- küberjulgeoleku lahenduste targa tellimuse arendamine;
- küberjulgeolekut toetavad õigusliku raamistiku kujundamine.

Eelnimetatud eesmärkide selgitused on toodud aruandes „Küberjulgeoleku strateegia 2014-2017“ [1].

IMD World Competitiveness Center viib igal aastal läbi maailmas uuringu, et saada teada, kui kompetentsed erinevad riigid võrreldes üksteisega on. 2017. aasta uuringus osales 63 riiki üle maailma. World Digital Competitiveness analüüsib ja hindab riikide digitaaltehnoloogiaid. Digitaaltehnoloogiad muudavad valitsuste käitumist, ärimudeleid ja ühiskonda. Antud uuringu põhjal on digitaalse konkurentsivõime kolmeks põhiliseks teguriks teadmised, tehnoloogia ja tulevane valmisolek [4]. Kuna Eesti on vastavas edetabelis 26. kohal, siis on meil pikk tee veel minna. Vaadates naaberriike, siis Läti on antud edetabelis 35. kohal ja Leedu 29. kohal. Põhjapoolsed naabrid on edetabeli tipu pool, näiteks Soome on 4. kohal, Rootsi 2. kohal ja Norra 10. kohal. Idapoolne naaber Venemaa on 42. kohal. Edetabeli topp kolm riikideks on Singapur, Rootsi ja USA [4] .

Järgmisel joonisel (Joonis 1) on näha, et Eesti on üleüldises arvestuses 26. kohal (riike kokku 63) ja millest antud hindamismaatriks koosneb [4]. 2017. aasta jooniselt on näha, et alamfaktor, milles Eesti on eesrinnas, on koolitused ja haridus.



Joonis 1 Eesti üldine tulemus digitaalse konkurentsivõime arvestuses 2017 aastal. Mõõdetakse teadmisi, tehnoloogiat ja valmisolekut tulevikuks.

Vaadates eelmiste aastate tulemusi [4], saame teada, et teadmiste faktoris on Eesti kõikides alamfaktorites läbi aastate tõusnud, kuid tehnoloogia faktoris, mida peetakse Eestis üheks perspektiivikamaks, oleme kõikides alamfaktorites läbi aastate langenud. Langenud on suhtumine ka kohanemisvõimesse. Eesti parim tulemus antud uuringusarjas jääb 2014. aastasse, tehnoloogia vallas olime aga veel madalamate „pallidega“ kui 2016. aastal [4]. Näiteks on Eesti küberjulgeoleku strateegia visiooniks, et *Eesti suudaks tagada*

riigi küberjulgeoleku ning toetada avatud, kaasava ja turvalise infoühiskonna toimimist [1], seega ootus oleks, et oleksime järgmistel aastatel kõrgemal kui 26. kohal.

2.2 Täiskasvanute üldised oskused digitaalmaailmas

Hügieenist räägitakse enamasti tööohutuse ja tervisehoiu teemade juures – käed ja hambad peaksid olema puhtad, keha pestud, töökeskkond turvaline, söödav toit ohutu jne. Viimasel ajal on hakatud hügieeni terminit „küberhügieen“ kasutama ka digimaailmas, mis on paljudele igapäevastele arvutikasutajale pigem uudis ja teeb sõnana enamasti ka palju nalja. Samas on nad enamasti nõus, et tegelikult peaks kõik inimesed tähelepanu pöörama nii oma tervise hoidmisele päriselus, kui ka „küberelus“, kus heaolu sõltub ka sellest, kui turvaliselt ja privaatselt hoitakse meid puudutavat infot. Mõlemal juhul tuleks alustada põhitõdedest ja -tegevustest, mis aitavad paremini selgitada, mis on hügieeni pidamise eesmärgiks [5].

Küberhügieeni mõiste osaks peetakse nii tehnilist turvalisust kui ka tehnoloogia kasutaja käitumist. Täpset mõistet veel maailmas kokku lepitud pole, kuid mitmed keskkonnad annavd vihjeid, mida selle all mõeldakse. Näiteks on oluline, et arvutikasutaja oskaks tuvastada nii pahavara ja saaks aru kui tegemist on andmekaeve (*phishing*) olukorraga [6], kui ka seda, et viimane ei jagaks enda ega ka ettevõtte kohta internetis lubamatult palju privaatset infot [7]. Head küberhügieeni alased oskused aitavad minimaliseerida ka küberkuritegude õnnestumist ja peetakse ka küberkaitse alaseks oskuste baasiks [8]

Tegelik olukord küberhügieenis pole aga kiita. Mitmetest järgnevalt vaadeldud uuringutest ning sõnavõttudest selgub, et olukord on digitehnika kasutamises keskmiselt halb, kuid veel halvem on inimeste turvakäitumine internetis. Näiteks Euroopas ei oma 44% täiskasvanutest vanuses 16-74 esmast teadmist digitaalsete seadmete kasutamisest [9]. Sama kinnitab ka Euroopa Komisjoni digitaalse majanduse ja ühiskonna volinik Mariya Gabriel, et pea pooled Euroopa täiskasvanud kodanikud ei oma algelist digitaalharidust ja kindlasti tuleb kasutusele võtta meetmeid kodanike teadmiste ning oskuste parandamiseks. Gabriel sõnul on lõhe kodanike teadmiste ja tulevastel töökohtadel vajaminevate digitaaloskuste vahel liiga suur. Ta väidab, et 90% tulevastest töökohtadest vajavad digitaalset oskust, mida neil täna ei ole piisavalt [10]. Samal teemal on võtnud sõna ka Euroopa Liidu julgeolekuliidu volinik Julian King, kes on mures Euroopa küberhügieeni taseme pärast. Selleks, et olukord paraneks on King teinud

ettepaneku haridusasutustele küberoskuste õpetamise süvendamise ja prioriseerimise osas [11]. Energia suunamine haridusasutustele annab kindlasti paremad oskused tulevastele töötajatele ja noortele.

Kuriooseks muudab asjaolu see, et täiskasvanud arvutikasutaja hea küberhügieen on oluline nii antud kasutajale kui ka ettevõttele, kus kasutaja töötab. Eespool mainitud Euroopa Liidu julgeoleku voliniku sõnul on umbes 95% küberrünnakutest olnud edukad tänu kasutajate ebapädevusele. Töötajad, kui ka nende tööandjad, peaksid olema üha enam huvitatud teadlikkuse tõstmisest küberhügieeni valdkonnas, et mitte kannatada ärilist kahju [11].

Eesti küberkaitse noor talent Teet Laeks toob välja oma arvamusartiklis, et rünnakud õnnestuvad tihti inimeste ebapädevuse tõttu, mitte, et tehnoloogia või protsessid olid „auklikud". Tema sõnul on pahalasel võimalik rünnata kolme suuremat sihtmärki, milleks on tehnoloogia, protsessid või kasutaja. Juhul kui panna need kolm kõrvuti, siis kõige nõrgemaks lüliks on saamas just kasutaja [6]. Eesti arvutikasutajate oskuste kohta saame aimu näiteks TNS Emori 2017. aastal läbiviidud kordusuuringust, kus selgus, et kolme aastaga on kasutajate teadlikus seadmete turvalisuse osas küll tõusnud, kuid teadmiste rakendamist peavad siiski vanemad vanusegrupid pigem keeruliseks, kui lihtsaks [12]. Seega üliolulineon teooriana õpitud teadmisi püüda ka praktikas rakendada [6].

Digioskuste ja küberhügieeni valdkonna uurimisel selgus, et kõige paremini iseloomustab Eesti täiskasvanud töötajaid Haridus- ja Teadusministeeriumi toodud kokkuvõte PIAAC uuringust, mis oli läbi viidud 2015. aastal. *Uuringu järgi on Eesti 16–65-aastaste elanike hulgas 43% inimesi, kelle probleemilahendusoskus tehnoloogiarikkas keskkonnas on alla 2. taseme (hinnatakse tasemel 0-3) ja kes töö tegemiseks arvutit ei kasuta. Hõivatute hulgas on selliseid inimesi 31%. Siia kuuluvad enamasti masinaoperaatorid, lihtöölised, põllumajanduses ja töötlevas tööstuses töötajad, 55+ vanuses inimesed. 9% on inimesi, kellel on head oskused, mida nad aga oma praeguses töös ei kasuta (hõivatutest 3%). Tegemist on peamiselt kuni 24-aastaste noortega. 30% inimesi väitis, et nad kasutavad töö juures arvutit, aga nende mõõdetud oskused on alla teise taseme* [13].

Samuti viis Kutsekoda läbi uuringu „Eesti tööturg täna ja homme", ning antud uuringust tuli välja, et 2025. aastaks on oodata kõige suuremat hõivatuse kasvu tarkvaraarenduses, meedia ja telekommunikatsiooni valdkondades [14]. Antud uuringu sari näitab, et juba

täna tuleb keskenduda IT-valdkonna inimeste küberhügieeni alaste oskuste parendamisele, kuid digioskuste kasutamise vajadus muutub kriitiliseks ka teistes valdkondades. Kolmandaks, Personalifirma ManpowerGroup poolt läbi viidud rahvusvaheline uuring 20 000 tööandjaga andis samamoodi hinnangu, et kõige enam töötajaid on vaja juurde IT- ja digivaldkonnas. Tööandjate ootuste kaardistamise selgus, et kõige defitsiitsem töötaja on tugevate tehnoloogiliste või digitaalsete oskustega indiviid, kellel on, samal ajal head isikuomadused (hea suhtleja, koostöövalmis ja oskuslik probleemilahendaja) [15]. Kuid Eesti ei saa jätta kõiki probleeme lahendada ainult IT-valdkonna töötajatele ja peaks kõiki oma tööealisi kodanikke tehnoloogia alal harima juba täna.

Erinevate koolitusfirmade poolt pakutakse tavalisele töötavale inimesele koolitusi, kuid sisulisel on need pigem mõeldud programmide õppimiseks. Samuti keskendutakse pigem teatud kättesaadavatele sihtrühmadele nagu õpetajad.

Järgnevalt toob autor ülevaate, milliseid digipädevuse koolitusi on leida Eestis praegu ning mida on tehtud minevikus:

- IT alased koolitused läbi veebilehe tark.ee. Antud lehelt on võimalik kõigil leida sobivaid koolitusi IT alaseks arenemiseks. Näiteks on tulemas koolitus ettevõtetele, mis hõlmab uut küberturvalisuse seadust: „Uus küberturvalisuse seadus – kuidas viia organisatsiooni tegevus seadusega kooskõlla?“. Antud lehelt leiavad ka algajad arvutikasutajad midagi, näiteks „Dokumentide koostamine MS Word baasil“ [16]. *Euroopa Sotsiaalfondi toetatava tegevuse „Täiskasvanuhariduse edendamine ja õppimisvõimaluste avardamine“ eesmärk on motiveerida täiskasvanuid õppima ning luua kvaliteetsed, paindlikud ning tööturu arenguvajadusi arvestavad õppimisvõimalused.* Seoses antud eesmärgiga pakub Haridus- ja Teadusministeerium tasuta koolitusi üle Eesti. Näiteks on pakkuda koolitused nagu „Tehnoloogia kasutamine digiajastul“ ja „Bürootöötaja digioskused“ [17];

- targaltinternetis.ee korraldab küberhügieeni tõstmiseks konverentse, kus saavad kõik huvilised osaleda, kuigi tegelikkuses on sihtrühmaks, kas lapsevanemad või õpetajad. Viimane konverents oli 06.02.2018 ning teemaks oli „Parem internet algab sinust“ [18];

- korraldatud on erinevaid kampaaniaid, et täiskasvanute digipädevus pareneks, näiteks 2009. aastal korraldati projekt „Ole kaasas“, mille eesmärgiks oli korraldada arvutialane alg- ja täiendõpe täiskasvanutele, et tuua neid internetimaailma [19];

- keskkonnad, kus leiab infot, millised on ohud internetis ja kuidas enda teadlikkust tõsta leiab näiteks RIA blogist [20];

- töökeskkonna vaatest on *tööandja kohustatud tagama töötajale tööalaste teadmiste ja oskuste arendamiseks ettevõtte huvidest lähtuva koolituse, kandma koolituskulud ja maksma koolituse ajal keskmist töötasu. Täienduskoolituse eesmärk on toetada töötaja kui spetsialisti pidevat arengut* [21];

- veel ühe näitena võib tuua projekti, mille käigus loodi digiõppe kursus „Enesejuhtmine“ puudega inimestele nende paremaks toimetulekuks. Digiõppekursus „Enesejuhtimine“ koosneb videoloengutest, slaididest, välja prinditavatest materjalidest, MP3 audioloengu võimalusest ja õppejõudude poolt individuaalsest tagasisidest [22].

Õpetajatele on loodud veebipõhine enese- ja vastastikuse hindamise vahend, milleks on DigiMina. Antud profiil aitab õpetajatel hinnata digipädevust. Tulemuslikkuse näitamine põhineb õpetajate pädevusmudelil NETS, mis on loodud rahvusvahelise Haridus- ja tehnoloogia ühingu poolt. Standardite väljatöötamiseks on mitmeid algatusi ja lähenemisviise. Näiteks Hinostroza *et al*. väidab, et info- ja sidetehnoloogiaga seotud küsimuste osas on vähemalt kaks lähenemisviisi pädevuste hindamiseks. Traditsioonilise oskuste määratlemise viis on orienteeritud riist- ja tarkvara õppimisele. Alternatiivne oskuste määratlemise viis kirjeldab laiemaid pädevusi, mida saab tarkvara arendamisel kasutada vahendina, näiteks viidates kaugsidele ning kommunikatsioonile (materjalide loomine ja jagamine, kogukonnad) [23].

Kokkuvõtvalt võib öelda, et digioskused on olulised iga valdkonna inimesele, sest isegi kui täna veel tööalaselt arvutiga kokku ei puututa, siis kaugel pole aeg, kus see saab reaalsuseks. Kindlasti on iga ettevõtte töötaja ka internetis oma ettevõtte eestkõneleja, mispärast ka vabal ajal tehtud toimingud isiklikul sotsiaalmeedia lehel võivad ühel hetkel tööandja tähelepanu pälvida.

2.3 Täiskasvanud arvutikasutaja oskuste parendamine

Euroopa Liidu kodanike oskuste kaardistamiseks on välja töötanud Euroopa komisjon teoreetilise raamistiku *The Digital Competence Framework for Citizens* (DigiComp). Antud raamistiku 1.0 versioon ilmus 2013. aastal ja uuendus 2016. aastal, mis kandis numbrit 2.0 [24]. 2017. aasta Mais täiendati juba aga ka 2.0 versiooni [25]. DigiComp raamistiku eesmärgiks on kodanike digitaalse pädevuse parendamine. Erinevad Euroopa riigid on vastava raamistiku võtnud kasutusele kas otse või osaliselt. Näiteks Eestis võttis 2016. aastal Hariduse ja infotehnoloogia sihtasutus raamistiku kasutusele kui „Õppijate digipädevuse mudel“ [26], mille alusel 2018. aastal viiakse läbi põhikooli ja gümnaasiumiõpilaste digioskuste hindamine Tallinna ja Tartu Ülikooli koostöös [27]. DigiComp annab tähenduse kasutajale, kes kasutab digitehnoloogiat enesekindlalt, vastutustundlikult ja omades ka kriitilist meelt ja seda nii tööl, õppides kui ka ühiskonnas osalemisel järgmises viies valdkonnas:

- info ja andmepädevus;
- kommunikatsioon ja koostöö;
- digitaalse sisu loomine;
- digitaalnet ohutus;
- probleemi lahendamine [28].

Kui püüda leida teooriate ja koolituste juurde ka praktilisi soovitusi, kuidas tavakasutaja saaks olla oskuslikum, siis näiteks HM Government nimetab isikuandmete kaitsmiseks mitmeid erinevaid võimalusi. Seadmete kaitsmine on viis, kuidas kasutajad saavad muuta pahalaste tegutsemise raskemaks [29]. HM Government ja Telia Eesti küberkaitse ekspert Aare Kirna on välja toodud soovitused [30], mida iga kasutaja peaks järgima. Kasutajal on:

- rangelt soovitatav kontrollida aeg-ajalt, kas kasutusel olevasse e-maili on sisse murtud. Antud infole saab ligi, kui lisada gmaili aadress näiteks veebilehele https://haveibeenpwned.com/ [30]. Eestis tekitas palju tormi sarnane veebileht Gotcha.pw, mis lubas anda ülevaate kõikide Eesti inimeste kohta [31];

- vaja luua kontodele paroolid, mis ei ole enam endaga seostatavad. Paroolid peavad olema pigem pikad kui keerukad. Sama parooli ei tohi kasutada erinevate kontodega [32]. Lisaks on Eestis mõistlik kasutada ID-kaardi või mobiili-ID logimist, mis on turvalisem lahendus, kui parool või miinimummeetmena kasutada mitmefaktorilist autentimist;

- õigus ja ka kohustus on teha oma kasutatavale seadmele tarkvarauuendusi, vajadusel paigaldada viiruse- või pahavara tõrje;

- vajadus mõelda kogu aeg kriitiliselt infole, mida sotsiaalmeedia või e-posti suhtluse vahendusel jagada, mida alla laadida ja mida avada;

- vajadus mõista, et andmete varundamine on oluline. Andmeid on võimalik varundada välisele kõvakettale või pilveteenusele;

- mõistlik kasutada arvutit piiratud juurdepääsu õigustes, mitte administraatorina. Samamoodi tuleks luua igale erinevale arvuti kasutajale erinev konto, et vähendada ristkasutust;

- võimalus saada abi. Paljud tarkvaratootjad ei lisa kahjuks oma operatsioonisüsteemide või rakendusprogrammide keelevalikusse eesti keelt. Kui ei saa aru või ei ole kindel, mida arvuti kasutaja käest tahab, siis lugeda veelkord, kui vaja tõlkida teade, küsida mõnelt tuttavalt asjatundjalt üle või kasutada interneti otsingumootorit [30].

Eelmainitud lihtsad tegevused on need, mida peaks iga arvutikasutaja teadma kui ka rakendama. Kahjuks on reaalsus see, et ka nende seitsme soovituse järgimine käib inimestel üle jõu, sest ei olda veendunud, et nende kontodesse võidakse sisse murda. Samuti on ebamugav hoida meeles erinevaid paroole. Tarkvara uuendusi ja varundamist peetakse pigem IT alaseks oskuseks, millega tegelevad pigem vastava valdkonna spetsialistid. Seega probleeme küberhügieeni alaste teadmiste ja oskustega on juba mainitud põhitõdede ja tegevuste tasemel [29].

Kokkuvõtvalt võib öelda, et juhul kui digikeskkonna kasutaja soovib toimetada turvaliselt, siis selleks vajaliku informatsiooni kättesaamine on info nappuse ja tehnilisuse tõttu raskendatud.

3 Küberkuriteod

Antud peatükis annab autor ülevaate, milliseid küberkuritegude liike on olemas ja milliseid uuringuid antud valdkonnas on eelnevalt tehtud. Samuti annab autor põgusa ülevaate küberkuritegevuse olukorrast Eestis ning maailmas.

3.1 Termin „Küberkuritegu“

Küberkuritegu on kuritegu, mis on suunatud isiku või rühma vastu. Kurjategija motiiviks on tahtlikult kahjustada ohvri mainet, põhjustada otseselt või kaudselt ohvrile füüsilist või vaimset kahju kasutades selleks arvutit ja internetti [33].

Küberkuriteod võib liigitada kolme suurde rühma ründe eesmärgi järgi. Nendeks on kuriteod:

- mis on suunatud arvuti vastu näiteks häkkimine, pahavara ja muu sarnane;
- kus arvuti on abivahendiks, mille abil kuritegu sooritatakse näiteks õngitsuskirjad, isikuandmete vargus ja krediidipettused ja muu sarnane;
- mis on arvuti sees sisuliselt toime pandud, näiteks pornograafia, vägivalla ja terrorismiga seotud ohud.

Antud liigitus võib olla ebatäpne, sest praegu puudub universaalne küberkuritegevuse liigitamise kokkulepe [34].

Levinud küberkuriteod on järgmised:

- internetis ostu/müügiga seotud pettused – ostja kõige suurematekss ohtudeks on väljastamata kaup ning mittevastav toode. Müüja poolt on ohuks, kas toote eest on tasutud ostja või varastatud krediitkaaridga;

- internetis tehtavad panga ja makse pettused – panga pettuseks nimetatakse seda, kui pettur saab ligi pangakontole ja saab sealt teha soovitud kandeid või saadakse panga detailid õngitsuskirja või mõne veebiaadressi abil, kus kasutaja peab täitma vajaminevad lahtrid;

- teised küberpettused, näiteks identiteedipettus – juhul kui pettur kasutab ära kellegi identiteeti kuriteo toime panemiseks;

- küberkiusamine – kiusamine, milleks kasutatakse elektroonilist tehnoloogiat;

- pahavara – sisaldab endas erinevaid arvutiviiruseid, Trooja hobused, nuhkvara ja lunavara;

- häkkimine või muud moodi arvutisse sisse tungimine [34].

Üle poole maailmas olevatest elanikest on juba interneti kasutajad [35]. Erinevad uuringud on näidanud, et mida suurem on internetis kasutajate arv, seda suurem on ka nende kasutajate arv, kes võivad küberkuritegevuse ohvriks langeda [34].

3.2 Küberkuritegevus maailmas ja Eestis

Maailmas läbi viidud uuringu kohaselt on küberrünnakute tõusuga kaasnenud ka edukate küberrünnakute kasv ettevõtete vastu. Võrreldes 2016. aastaga, on edukate küberrünnakute kasv ettevõtete vastu tõusnud 2017. aastaks 27% võrra. Pelgalt lunavara rünnakud kahekordistusid aastaga ehk 13% pealt 27% peale. Antud tõusus mängis suurt rolli WannaCry ja Petya, sest nendepoolsed rünnakud olid massilised. Antud uuringu järgi tõusis ettevõtetel keskmine küberjulgeoleku kulu aastas 11,7 miljoni USD, protsendiliselt kasvas antud kulu 22,7% [36].

Küberkuritegevus toob endaga kaasa kahju ettevõtetele, näiteks WannaCry rünnaku teadaolev kahju on 4 miljardit USD. Eestis teadaolevalt WannaCry ohvreid ei olnud [37].

RIA toob välja Küberjulgeoleku 2018. aasta raportis, et *Eesti riigiasutustes või teenusepakkujate juures ei registreeritud möödunud aastal ühtki tõsist andmelekke juhtumit. Küll kasutavad Eesti elanikud aktiivselt suurte rahvusvaheliste teenusepakkujate teenuseid, kuhu registreeritakse kontosid ka tööalast e-posti aadressi kasutades. Möödunud aasta lõpus avaldati tumeveebis 1,4 miljardi kasutaja infot ja*

parooli lihttekstina sisaldav andmebaas, kus sisaldus ka 198 000 .ee-lõpuga e-posti aadressi, mida oli kasutatud kontot luues. Ehkki andmebaasist ei selgu täpselt, millisest keskkonnast kasutajanimed ja paroolid täpselt lekkinud on, sisaldab see LinkedIni, MySpace'i, Twitteri, Tumbleri, DropBoxi, Bitcoini foorumite, Zomato, Gmaili ja Yahoo lekkinud kasutajainfot. Neist 2830 olid Eesti avaliku sektori ja ligi 2600 elutähtsa teenuse osutajate töötajate meiliaadressid [37].

Intellektuaalomandiõigustega seotud kuritegevuse arvutuslik kahju maailmas on kuni 461 miljardit dollarit aastas ning see on seotud peaaegu kõigi tooteliikide ja geograafiliste piirkondadega. Digimaailmas on eriliseks probleemiks kaitstud sisu levitamine veebis. Järelevalveasutustel tuleb tulevikus tegelda ebaseaduslike telesaadete ja digipiraatlusega. [38]. 2010. aastal oli Eestis kasutatavast tarkvarast ligi pool piraattarkvara ning tõi Eesti riigile kahju aastas 17,5 miljonit EUR [39].

Kõikidest küberkuriteo liikidest valis autor oma uuringu küsimusteks suhtumise piraatlusesse ja hakkama saamise krüptovara/lunavara juhtumi korral. Valiku aluseks sai see, et piraatlus on üks levinuimaid kuritegevuse vorme, mida mitmeski maades karistatakse leebelt või jäetakse üldse märkamata, kuna see on nii levinud nähtus. Samas piraatluse läbi luuakse kanalid, mis hoiavad kuritegelikku võrgustikku üleval, hoides paljud muidu seaduskuulekad kasutajad klientidena. Lunavara sai valitud seetõttu, et tegemist on ühe ohtlikuima pahavaraliigiga, mis takistab lõppkasutaja tööd, kuid mis võib saada saatuslikuks ka ettevõtte tehnoloogiast liigselt sõltuvale ärimudelile.

Järgmiseks tehakse magistritöös lühiülevaade nii piraatlusest kui lunavara väljakutsest.

3.3 Piraatlus

Antud peatükis toob autor ülevaate internetipiraatlusest ja peamistest piraatluse põhjustest.

3.3.1 Piraatluse ajalugu

Termin „piraatlus“ kujunemislugu intellektuaalse omandi kontekstis viib meid tagasi 17. sajandi Inglismaale, kus termin tuli kasutusele seoses raamatute kirjutamisega – kellel oli õigus teha kordustrükki ja kellel mitte. Neile, kes avaldasid raamatuid, mille õigused kuulusid kellelegi teisele, hakati viitama kui piraatidele. 18. sajandil hakati intellektuaalse omandi valdkonda riiklikul tasandil reguleerima Inglismaal, ja Prantsusmaal. Ilmusid autoriõiguse seadused ning seeläbi muutus „piraatlus“ kui autoriõigustega kaitstud teoste loata tootmine ja müümine seadusevastaseks tegevuseks [40]

Peamised objektid, mida alguses kopeeriti olid trükitud teosed. Tehnoloogia areng tõi endaga kaasa uute piraatluse vormide tekkimise, enam ei kasutatud piraatlust ainult trükitud teostel, vaid ka ülemaailmselt muusika, filmide ja tarkvara kopeerimisel. Muusikapiraatlus eksisteerib 1970. aastast [41]. Seoses uute heli- ja videokandjate ja lindistus- ja mahamängimise tehnoloogiate arenguga kasvas piraatlus massiliseks [42]. Lisaks muusika ja filmide piraatlusele kujunes piraatluse objektiks ka tarkvara. Gruppe, kes tegelesid tarkvara piraatlusega nimetati *warez* gruppideks [43].

1980. aastate alguses tekkisid esimesed organiseeritud grupid, mis tegelesid tarkvara kräkkimise ja selle levitamisega. Algselt piraatluse levitamine käis postiteenuse teel, sest tegemist oli füüsiliste teostega. Arvutivõrkude suur areng tõi endaga kaasa levitamise võrgupõhiseks. Esimene lahendused, mida kasutati oli teatetahvlisüsteem *(BBS ehk Bulletin Board System),* interneti rühmadiskussioone *(IRC ehk Internet Relay Chat)* ning USENETi uudisgruppe *(newsgroups)* [44].

Järgmiseks sammuks oli lairibaühendus *(broadband),* mis muutus populaarseks 90. aastate lõpus. Lairibaühendus võimaldas palju kiiremat interneti ja seetõttu suurte failide, näiteks filmide allalaadimine muutus populaarsemaks [44].

3.3.2 Internetipiraatlus ja põhjused

Internetipiraatlus on tegevus, mille käigus omandatakse autorõigusega teos ja/või levitatakse seda interneti teel. Teosteks võivad olla näiteks filmid, muusika, raamatud, tarkvara, mängud ja palju muud. Internetipiraatlusel on erinevaid eesmärke. Näiteks eratarbimine, tutvumine, tulu teenimine ja edasimüük. Piraatluse levinuimaks tehnikaks on P2P-võrgustikud, kus kasutajad laevad alla ja üles samu faile üheaegselt [45]. P2P failijagamine muutus ülemaailmselt populaarseks 1999. aastal, kui Shawn Fanning tõi turule rakendusega Napster. Antud rakendus võimaldas inimestel keskse vahendusserveri abil tasuta muusikafaile vahetada [44].

Intellektuaalse omandi valdkonda reguleerivad Eestis kohalikud seadused, rahvusvahelised lepingud ja Euroopa Liidu dokumendid [44]. Eestis on kehtiv autoriõiguse seadus, mis justkui peaks hõlmama ka internetipiraatlust, kui vaadata Autoriõiguse seadust §4. Teosed, millele tekib autoriõigus:

- *kirjandus-, kunsti- ja teadusteostele;*
- *teoseks käesoleva seaduse tähenduses loetakse mis tahes originaalset tulemust kirjanduse, kunsti või teaduse valdkonnas, mis on väljendatud mingisuguses objektiivses vormis ja on selle vormi kaudu tajutav ning reprodutseeritav kas vahetult või mingi tehnilise vahendi abil. Teos on originaalne, kui see on autori enda intellektuaalse loomingu tulemus.*

Teosed, millele tekib autoriõigus, on järgmised: arvutiprogrammid, mida kaitstakse nagu kirjandusteoseid. Kaitse laieneb arvutiprogrammi mis tahes väljendusvormile; muusikateostele tekstiga ja ilma tekstita; audiovisuaalsetele teostele [46].

Piraatluse leviku Eestis teeb raskesti jälgitavaks §26**,** mis ütleb, et *audiovisuaalse teose ja teose helisalvestise kasutamine isiklikeks vajadusteks autori nõusolekuta on lubatud reprodutseerida ehk koopia tegemine audiovisuaalset teost või teose helisalvestist kasutaja enda isiklikeks vajadusteks (teaduslikuks uurimistööks, õppetööks). Teose autoril, aga samuti teose esitajal ja fonogrammitootjal on õigus saada õiglast tasu teose või fonogrammi sellise kasutamise eest* [46].

Seadusest hoolimata kasutatakse Eestis piraatlust aktiivselt ja tagajärgi kartmata, sest peamiselt kasutatakse seda siiski enda tarbeks. Alljärgnevalt on välja toodud kümme peamist põhjust, miks piraatlus on populaarne. Kasutaja:

- ei soovi teenuse eest tasuda – antud põhjuse taga ei ole mitte midagi muud, kui kasutaja on teadlik, et antud film/mäng on võimalik saada tasuta, siis seda võimalust ka kasutatakse;

- ei oma vahendeid, et soovitud teenust endale lubada ja seetõttu kasutab piraatlust – näitena võib tuua Adobe Photoshop programmi. Kasutajal ei ole vahendeid, et seda programmi endale lubada ja seetõttu otsitakse tasuta võimalusi programmi saamiseks;

- soovitud teenus (filmid, telesarjad või muud sarnased) ei ole saadaval soovitud regioonis;

- soovitud teenus (filmid, telesarjad või muud sarnast) jõuab soovitud regiooni hilinemisega;

- soovitud teenuse eest tasumine on keerukas ja paljudel juhtudel on vaja selleks krediitkaarti;

- soovib teenust kasutada ainult ühe korra ning seetõttu ei soovi selle eest tasuda;

- arvab, et teenusepakkujal on juba piisavalt kasumit, ning seetõttu usuvad, et teenusepakkuja ei paneks pahaks, kui üks kasutaja kasutab soovitud teenust tasuta;

- kasutab piraatlust, sest ka teised kasutavad – see on normaalsus. Paljudel on kahjuks mentaliteet, et juhul kui teised teevad, siis justkui on see hea põhjendus sellele;

- ei tea, et tegemist on piraatlusega. Antud põhjus võib tunduda imelik, kuid võib juhtuda, et kasutajal ei ole tehnoloogia vallas piisavalt teadmisi, et aru saada, et kõik internetis tasuta olevad võimalused ei pruugi olla legaalsed [47].

Paraku võib öelda, et ka paljudele Eesti elanikele tundub, et on tavapärane varastada digitaalset eset. Inimesed ei suhtu digitaalsesse ja füüsilisse esemesse samaväärselt [47]. See võib olla üheks põhjuseks, miks inimesed ei saa aru ka muudest küberkuriteo liikidest, sest „digitaalne asi“ ei tundu samaväärsena „päris asjaga“, seega ka digitaalne kuritegu pole paljude meelest „päris kuritegu“. Samas on piraatlus üks viise, kuidas saab sokutada lisaks piraaditud programmile kasutaja seadmesse pahavara, millega viia ellu teisi kuritegusid. Kuna paljud kasutavad teadmatusest piraatprogramme ka tööarvutis, siis seeläbi on võimalik tekitada kahju ka ettevõttele.

Käesolevas magistritöös võetakse piraatlusesse suhtumine üheks uuringuküsimuseks, et teada saada trende inimeste arusaamas suhtumises piraatlusesse.

3.4 Lunavara

Antud peatükis selgitab autor, mis on lunavara ja kuidas lunavara intsidenti ennetada. Lisaks toob autor ülevaate lunavaraga seotud olukorrast maailmas ja Eestis.

Viimastel aastatel on üks ohtlikum pahavara olnud lunavara. Lunavara on pahavara, mis takistab kasutajal arvutis olevate programmide või failidele ligi pääseda. Piltlikult võib lunavara kasutaja arvuti pantvangi võtta ning nõuda vabastamise eest lunaraha. Lunavara võib liigitada kaheks:

- ekraaniluku-lunavara. Ekraaniluku- lunavara näeb välja üldjuhul selline, et kasutaja ekraanile ilmub aken, mis ütleb, et arvutit ei saa enam kasutada enne, kui on tasutud lunaraha (tavaliselt krüptovaluutas). Kasutaja hirmutamiseks kuvatakse ekraanile siivutute lehekülgede ekraanitõmmiseid. Sellisel kujul hirmutamine on aga mõeldud rohkem lastele ja noorukitele, kuid mõjub efektselt ka teistele kasutajatele. Üldjuhul ekraaniluku-lunavara faile ei krüpteeri ja sellest saab vabaneda kui kasutada viirusetõrjeprogrammi.

- krüpteeriv lunavara. Krüpteeriv lunavara jätab enamasti arvutis olevad programmid puutumata, kuid võtab enda valdusesse kasutaja dokumendid. Tavaliselt on dokumendid kasutajatele just kõige väärtuslikumad. Failide krüpteerimiseks kasutatakse avaliku võtme krüptograafiat. Antud meetodiga kasutatakse avaliku ja salajast võtit. Esimese võtmega andmed lukustatakse ja teise võtmega tehakse need lahti. Kurjategijad valmistavad ette serveris

võtmepaari ja saadavad avaliku võtme kasutaja nakatunud arvutisse, kus lunavara programm saab asuda tööd tegema. Peale seda, kui lunavaral on õnnestunud failid enda valdusesse võtta, siis pakub kurjategija arvuti kasutajale salajase võtme ostmise võimalust. Lunavara satub arvutisse tavaliselt läbi programmide turvaaukude, nakatatud veebilehtede, väliste andmekandjate (näiteks mälupulk) või e-kirjade kaudu [48].

Esimene dokumenteeritud lunavara juhtum on leitav aastast 1989, mille nimi on AIDS Trojan tuntud ka nimega PS Cybrog1. Joseph L. Popp saatis 20 000 nakatunud diski rahvusvahelisele AIDSi konverentsile. Arvutid nakatusid lunavaraga, kui diski enda arvutisse panid. Paljud küberkurjategijad mõistsid 2006. aastal, et interneti abil saab lunavaraga raha teenida üle maailma. 2011. aastal algas lunavara suur levik hinnatakse, et maailmas oli 60 000 erinevat lunavara. Usutakse, et 2012. aastal antud number kolmekordistus. Tuntuimad lunavara nimed olid: CryptoLocker (September 2013); Locker (Detsember 2013); SynoLocker (August 2014); CryptoWall 2.0 (Jaanuar 2015) ja Chimera (November 2015) ning palju muid [49].

Uuringud näitavad, et lunavara on kasvav trend nii eraisiku kui ettevõtte rünnakute vaatest. Arvatakse, et ettevõttetele tehakse lunavara rünnakuid maailmas iga 40 sekundi tagant. Lunavara hind on viimastel aastatel tõusnud. Näiteks – 2016. aastal oli lunavara keskmiseks hinnaks juba 1077 dollarit. 2017. aasta esimeses kvartalis oli kümnest pahavara juhtumist kuuel korral tegu lunavaraga. Lunavara tekitas globaalselt 2017. aastal kahju kokku viis miljonit USD [50].

Näiteks:

- 2017. aasta maikuus sattus üle maailma erinevad ettevõtted lunavara WannaCry küüsi. Ohvriks langes maailmas üle 150 riigi ettevõtted. Ettevõtetest langes ohvriks Suurbritannia NHS haigla ja Hispaania suurim telekommunikatsiooni ettevõte Telefonica. Mõne tunni jooksul nakatus hinnanguliselt 36 000 süsteemi 11 erinevas riigis, sealhulgas Venemaa, Türgi, Saksamaa, Jaapan ja Filipiinid [51].

- 2014. aastal oli kokku Eestis mõni üksik lunavara juhtum. 2015. aastaks teatati RIA´le juba 150 lunavara juhtumiga. 2015. aastal said näiteks lunavaraga pihta Tallinna Sadam ja Tallinna Kiirabi [52]. 2016. aasta veebruaris tegeles CERT.EE

781 küberkuriteo juhtumiga, millest 128 kohta teavitas riigisektor ja 653 kohta erasektor. Kõige kõrgema prioriteediga olid erinevat tüüpi lunavarajuhtumid. 2016. aasta veebruaris tegeleti nii TeslaCrypt lunavaraga kui ka Locky- nimelise lunavaraga [53].

- 2017. aasta juuni hommikul tabas maailma lunavaralaine, mis jõudis ööpäevaga 64 erinevasse riiki ja sealhulgas Eestisse. Riigi Infosüsteemi Ameti andmetel Eestis nakatus pahavaraga kaks Saint-Gobaini kontserni kuuluvat ettevõtet: Ehituse ABC ja väiksem tehas [54].

Lunavara ei ole küll kõige levinum pahavara tüüp, kuid kindlasti üks suurematest, millel on võimekus väga suurt kahju teha. Spetsialistide uuring 2017. aastal näitas, et lunavara eelne ennetustöö on kõige pakilisem küberjulgeoleku probleem [55]. Samuti juhul kui lunavara intsident on juba juhtunud, siis ühtset lahendust, kas tasuda lunaraha või mitte, autor ei leidnud. Pigem sai aimu, et kas küsitud lunaraha tasuda, sõltub andmete väärtusest ja kasutajapoolsest otsusest [56]. Näiteks Gunther Ollmanni, Vectra Networki turvaülema, sõnul on vahel lausa mõistlikum tasuda lunaraha, kui üritada enda jõududega pantvangi võetud failid tagasi saada. Lunaraha maksmine tundub küll riskantne, kuid Ollmanni sõnul on siiski tegemist kõige kiirema viisiga, kuidas soovitud andmed tagasi saada. Nimelt ei oska Ollman mainida ühtegi lunavara intsidenti, kus kasutajale ei oleks antud andmeid tagasi [56].

Riigi Infosüsteemide Ameti (RIA) sõnul üks kohtadest, kus Eesti kasutaja kindlasti lunavara osas abi saab on RIA kodulehelt. Põhilised vastumeetmeid, mida RIA soovitab on järgmised:

- arvutis peaks olema filter, et lunavara üldse ei jõuakski arvutisse, üldjuhul on tegemist viirusetõrje ning netis sirvimise keskkonna häälestamine;

- tuleks takistada lunavara käivitamist. Esimeseks filtriks on kasutajad – nemad peavad olema piisavalt teadlikud, et nad igale poole ei klikiks. Teiseks on operatsioonisüsteemide keerulisem seadistamine nii, et vales kataloogis fail lihtsalt ei käivituks;

- teha pidevalt varukoopiaid;

- luua kasutajatele piirangud juba enne kui juhtub lunavara intsident. Oluline on ära hoida olukord, kus pahalane pääseks ligi varukoopiatele ja asutuse failiserverile [57].

Käesolevas magistritöö empiirilises osas uuriti samamoodi, kuidas käituksid Eestis täiskasvanud vastajad ning kui tundlikud on ettevõtjad, kui selline olukord peaks juhtuma, et ettevõtte arvutid on lunavaraga nakatunud.

4 Metoodika

Antud magistritöö eesmärkideks oli välja selgitada, milliseks hindavad täiskasvanud töötajad oma küberhügieeni alaseid pädevusi ja millised on töötajate ja tööandjate ootused küberhügieeni oskuste parandamiseks. Tegemist on seega inimkäitumise ja suhtlemise uuringuga, mis on oma olemuselt pigem sotsiaalteaduste valdkonda kuuluv, kuid vajalik läbi viia just infotehnoloogi vaatest, kuna viimane saab sellele lisada konteksti puudutava lisaväärtuse. Sotsiaalteadusetes kasutatakse tihti kahte põhilist metoodikat empiiriliste andmete kogumiseks, mis on küsitlus ja intervjuu. Ka antud lõputöös kasutas autor andmete kogumist kahest allikast: interneti küsitlusest ja intervjuusdest. Lisaks sellele kasutati tulemuste valideerimiseks spetsialistide abi, et vähendada autori mõju uuringu tulemuste interpreteerimisel.

Küsitlus ehk ankeetimine on kirjalik kaugküsitlus, küsitlejal ei ole otsest kontakti küsitletavatega. Küsitletavad täidavad küsitluse interneti teel läbi e-ankeedi. E-ankeetimise eelised on järgmised: e-ankeeti saab vastaja täita endale sobival ajal, andmeid saab koguda samaaegselt mitmetelt inimestelt ja osalejate arv on seetõttu suurem kui paberankeetimisel, odav, saadud andmeid mugavam, kui ka veakindlam analüüsida, sest jääb ära paberilt arvutisse saadud andmete sisestamine. E-ankeetimise puudused on järgmised: ei saa olla kindel, kes tegelikult ankeedi täitis, peab usaldama vastajat, keda ei saa kontrollida, vead ankeedi täitmisel, kui juhend ebapiisav ja täidetud ankeetide laekuvus minimaalne [58].

Autor osales töögrupis, mille eesmärgiks oli koostada ja läbi viia Kaitseministeeriumi poolt tellitud uuringutest Küberpähkel. Küberpähkli uuring-testimist viiakse läbi 1-2 korda aastas, milles selgitatakse välja erinevate sihtrühmade küberteadlikkus. Tegemist on seirega, mida viiakse Eestis läbi alates 2015. aastast kõigepealt Haridus ja Infotehnoloogia sihtasutuse poolt, milles Küberpähkel toimis võistlusena 200-600 õpilasele üritusel Robotex ja teiste õpilasürituste raames. Alates 2017. aastast korraldab Küberpähkli uuringut Tallinna Tehnikaülikooli Küberkriminalistika ja Küberjulgeoleku

keskus, Birgy Lorenz-i (antud magistritöö juhendaja) juhtimisel. 2017. aasta sügisel viidi läbi uuring 4.-9. klasside õpilastele ja 2018. aasta talvel viidi läbi uuring kogu elanikkonnale alates 10. aastast alates. Käesolevas töös on kasutatud andmeid 2018. aasta talvel läbiviidud uuringust, mille üldiseks eesmärgiks oli saada aru õpilaste ja elanikkonna küberhügieeni alastest teadmistest ja oskustest erinevates olukordades.

2018. aasta uuring Küberpähkel viidi läbi interneti teel ja selleks kasutati e-testimiskeskkonna Limesurvey võimalusi. Osaleda said kõik eesti keelt mõistvad inimesed ajavahemikus 15.01.2018 kuni 11.02.2018, kui nad olid vähemalt 10 aastat vanad. Uuringu Küberpähkel valimiks kujunes mugavusvalim, kuna uuringut täitsid huvilised vabatahtlikkuse korras. Uuringus osalemise info saadeti laiali koolidele läbi koolide üldise e-maili aadressi, jagati edasi läbi sotsiaalmeedia, jagati läbi erinevate e-posti listide ja reklaamiti ka kahes online meedia artiklis. Magistritöö autor aitas kaasa madala ankeetimise protsendi kasvatamisel jagades ankeeti täiskasvanud vastajatele oma tutvusringkonnas (köökaaslastele ja tuttavatele ning nende ettevõtetele).

Uuringus osales kokku 2078 inimest, kellest 555 olid märkinud ennast vanemaks kui 21 ja tegevuselt töötama (vastajatest oli 315 meessoost ja 240 naissoost). Sellest moodustuski magistritöös kasutatud valim. Kuna vastajate arv on kõrge, siis puudub alus karta, et analüüsist saadud tulemused oleks ebausaldusväärsed. Uuringus osalejad said märkida ankeedile ka oma tegevusvaldkonna, mis näitas, et vastajad on pigem keskmiselt või kõrgelt haritud ja oskavad tehnoloogiat kasutada pigem hästi. Uuringu tulemuste tõlgendamisel saab järeldusi teha ainult antud vastajate kohta. Võib teha järeldusi ka ühiskonnas ühe või teise teema trendide osas, kuid selle usaldusväärsus on pigem keskmine, sest uuringus osalejate arv ei ole piisav andmaks üldist hinnangut täiskasvanud töötajate kohta Eestis üldiselt.

Uuringus oli 41 küsimust: 9 taustküsimust ning 32 uuringu-testi küsimust. Uuritavad teemad olid: privaatsus ja turvalisus, tehniline taiplikkus, kriitiline mõtlemine ja sotsiaalmeedia manipulatsioon (inimkäitumist mõjutavad küberkuriteod ja kelmused) ja hoiakud küberhügieeni tõstmise osas. Antud uuringusse lisas autor omapoolt neli küsimust ning kaks näidisjuhtumit, mida antud lõputöö raames sooviti analüüsida (vt Lisa 1). Sarnased küsimused olid kasutusel ka 2017. aasta Küberpähkli uuringus õpilastega ja autor pidas neid oma töö kontekstis oluliseks. Küsimuste juures olid antud valikvastused, mida sai Likert skaalas hinnata. Küsimused vaadati üle ka väliste ekspertide poolt, et

lisada usaldusväärsust. Küsimused, mida antud lõputöö autor küsitlusse lisas olid järgmised:

- milliseks hindate oma digitaalseid ja küberhügieeni alaseid oskuseid täna?
- millistest kohtadest olete saanud digitaalse ohutuse/küberhügieeni alaste oskuste parandamiseks teavet, koolitust?
- millisest kohast sooviksite saada abi oma digitaalse ohutuse/küberhügieeni alaste oskuste tõstmiseks?
- Eestile on vaja küberhügieeni alaste oskuste kasvatamiseks ühiskonnas..

Näidisjuhtumid, mida autor Küberpähkli uuringusse lisas on järgmised:

- Prantsusmaal blokeeritakse kasutaja internetti ligipääs, kui avastatakse, et ta laadib alla piraatfilme (peale kolmandat vahele jäämist). Mida Te arvate sellest?
- sõbra arvuti on nakatunud lunavaraga. Varukoopiat arvutis olevatest failidest pole. On vaja kätte saada vajalikud failid. Failide avamise eest küsitakse 100 eurot, 7 päeva pärast tõuseb hind 200 euro peale. Mida soovitate sõbral teha?

Küsitlusest saadud andmed esitati autorile andmetabelina, milles oli kaasas ka taustaküsimused. Andmed olid kodeeritud: kasutusel olid nii nimitunnused, järjestustunnused, arvtunnused ja binaarnsed tunnused. Andmete analüüsimiseks kasutati programmi MS Excel ja andmeid vaadeldi esialgu läbi sagedustabeli, kuid antud töös tulemuste esitamiseks kasutab autor lintdiagrammi. Lintdiagramm on üks populaarsemaid diagramme ja sarnaneb tulpdiagrammile. Juhul kui tulpdiagrammis on tulemused toodud vertikaalsete tulpadena üksteise kõrval, siis lintdiagramm on sisuliselt horisontaalsete tulpadega. Lintdiagrammi eeliseks on lihtne haaratavus üldistele tulemuste esitamiseks. Saadud tulemused on pigem kvantitatiivsed ja kirjeldavad ja vastajate arvamusi võrreldi eraldi ka soopõhiselt kui ka vanuse järgi gruppides (21-40 ja 41-60), et mõista kas on ka erinevusi.

Saadud tulemuste alusel koostas autor järgmised sammud, et saadud andmeid valideerida mõne teise meetodiga. Uuringu teiseks valideerivaks meetodiks valiti intervjuu (vt Lisa 2). Intervjuu on meetod, mille puhul intervjueerija vestleb vahetult intervjueeritavatega.

Autor kasutas struktureeritud intervjuu liiki, mis tähendab, et intervjueerijal on ees küsimustega ankeet [59]. Silmast silma intervjuu läbiviimise eelised on: mahukus; lisaküsimuste küsimise võimalus; kõrge vastuste kvaliteedi määr; keskmiselt odav. Puudusteks on küsitleja võimalik mõju ankeedi tõlgendamisse; ajakulukas, sest iga uuritavaga tuleb koos protsess läbi teha [58]. Intervjuud viidi läbi selleks, et valideerida uuringu Küberpähkel tulemusi. Lisandväärtusena uuris autor intervjuu käigus töötajatelt ka töökeskkonna kohta, ning sai nii töötajate, kui ka tööandja tagasiside nende ootustele.

Intervjuud viidi läbi 10.04.2018 kuni 13.04.2018 ja intervjuu kestuseks oli 45 minutit. Uuringus on kasutatud andmed on esitatud anonüümselt. Intervjuud lindistati ja tehti märkmeid paberile, et tagata vastajate mõtete ühene edastamine ja vähendada autori omavoli andmete ülesmärkimisel. Samuti andis lindistamine võimaluse intervjuud taasesitada, kui oli vaja teha täpsustusi. Intervjuude küsimustele lisaks said uuritavad oma vastuseid selgitada ja vajadusel täiendada, kui autor oli millestki teisiti aru saanud. Intervjuud viidi läbi kuue valitud asutuse täiskasvanud töötajaga. Valitud ettevõte ei ole oma põhitegevuselt IT-teenust pakkuv ettevõte, kuid seal kasutatakse igapäevaselt tehnoloogiat. Tehnoloogia igapäevane kasutamine on ärimudeli üks alus, et töö saaks tehtud efektiivselt ja turvaliselt. Intervjuu viidi läbi erineva taustaga töötajatega – tavatöötajad (2), spetsialistid või IT valdkonna esindajad (3) ja juht (1). Osales kolm meest ja kolm naist. Kuna intervjuudest saadud andmed on kvantitatiivsed ja küsitletud on piiratud arv inimesi, siis üldistusi Eesti kohta teha nende põhjalt ei saa.

5 Tulemused ja analüüs

Tulemused esitatakse vastavalt seatud eesmärkidele. Esiteks esitatakse tulemused täiskasvanud töötajate enesehinnangu, kui ka läbi viidud situatsioonide lahendamise kohta ja teiseks antakse ülevaade töötajate ja tööandja ootustest küberhügieeni oskuste parendamisele.

5.1 Täiskasvanud töötajate oskused

Antud peatükis toob autor välja, millised on uuringus osalenud täiskasvanud töötajate küberhügieeni alased oskused vastajate enesehinnangu järgi. Kui vastajate enesehinnang on madal, siis seda enam eksitakse lihtsamate reeglite vastu, kui ka tehakse otsuseid ja tegusid, mis viitavad vähesele oskusele ja teadlikkusele. Kui enesehinnang on põhjendamatult kõrge, siis võib see viidata spetsialisti oskustele, kuid ka sellele, et ollakse harjunud tegema vastavates olukordades kiireid otsuseid, mis vahel võivad lõppeda halvasti. Kui kasutajal on põhjendamatult kõrge enesehinnang, siis vahel võib olla nii, et üldine küberhügieeni tase on küll teoreetiliselt kõrge, aga reaalses ohuolukorras oskused alati ei avaldu. Näiteks võiks tuua olukorra, kus enamasti üsna hästi oma andmeid hoidev inimene satub kaubanduskeskuses vaimustusse loosipakkumisest ja sisestab oma e-maili pakkuja andmebaasi, mis loob olukorra, kus lisaks loositulemustele hakkavad saabuma ka muud soovimatud e-mailid, millest vabanemine võib osutuda pigem keeruliseks. Sarnane olukord võib juhtuda ka IT juhiga, kes kasutab lohakalt lihtsaid paroole.

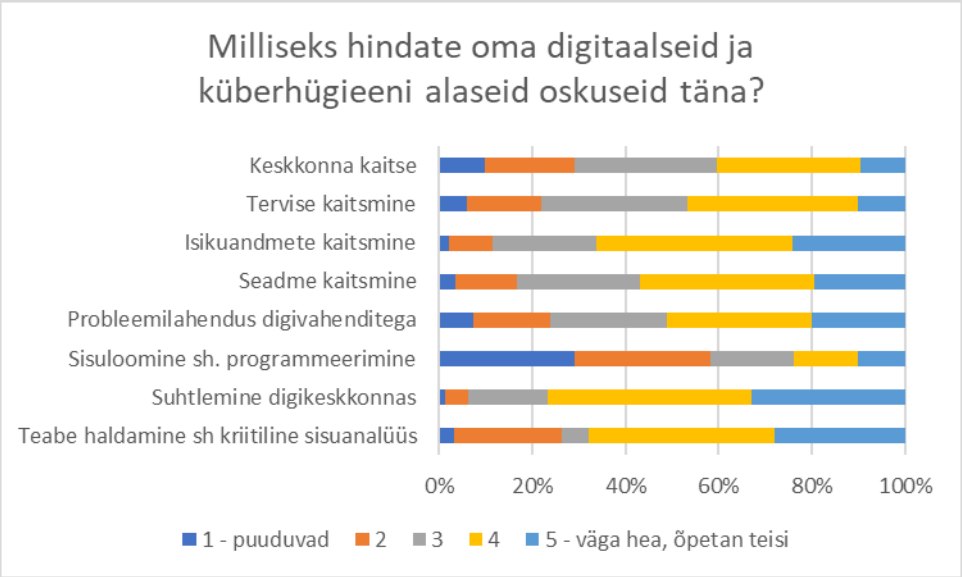
Oskuste kontrollimist e-testimise juures on keeruline läbi viia, seega parim viis oli panna vastajatele ette teoreetiline situatsioon, mida tuli antud raamistikus lahendada. Situatsioonideks valiti suhtumine piraatlusesse ja käitumine lunavara juhtumi korral.

5.1.1 Täiskasvanud töötajate enesehinnang ja selle iseseisev arendamine

44% Euroopa elanikkonnast vanuses 16-74 aastased ei oma esmast teadmist digitaalsete seadmete kasutamisel (vt 2.2.). Autori poolt koostatud uuring toob välja, kuidas valimis

olnud täiskasvanud kasutajad hindavad oma pädevust küberhügieeni valdkonnas vastavalt DigiComp mudelile [24].

Uuringus osalenud vastajad olid kõik keskmised või head arvutikasutajad, sest antud uuring on läbi viidud interneti vahendusel ja seda sai täita ainult arvutis olles. Vastajad hindasid kõrgelt enda digitaalseid ja küberhügieeni alaseid oskuseid teabe haldamises, digikeskkonnas suhtlemises ja isikuandmete haldamises (privaatsus ja veebipettus). Madalamaks hinnati oma oskuseid sisuloomises ja keskkonna kaitses (teadvustamises digitehnoloogia mõju keskkonnale). Täpsema ülevaate tulemusest on näha joonisel (Joonis 2).



Joonis 2. Täiskasvanud töötajate digitaalsete oskuste hindamise küsimuse tulemused

Antud tulemuste (Joonis 2) järgi võib öelda, et 76,6% vastajatest peab end heaks või väga heaks digikeskkonnas suhtlejateks. 67,7% vastanutest peab end heaks või väga heaks teabe haldamisel ja 66,1% vastanutest peab end heaks või väga heaks isikuandmete kaitsmises. Kõige madalamalt hindavad vastajad end sisuloomises/programmeerimises – 58,2% vastajaid väidab, et selline oskus puudub või pigem puudub. Kui hinnata digitaalset pädevust, siis sinna alla läheb probleemide lahendamine digivahenditegaja digikeskkondades (51,2% vastanutest peab end pädevaks, ehk heaks või väga heaks) ning seadme kaitsmine - rakendate ohutuse ja turvameetmeid (56,9% vastanutest peab end pädevaks).

Kui vaadata, kuidas hindavad end erinevast soost vastajad, siis erinevust ei ilmne.76,7% naissoost vastanutest ja 76,5% meessoost vastanutest tunneb end pädevalt digivaldkonnas suhtlemises. Vaadates probleemilahendamise tulemusi, siis naiste ja meeste vahe on erinev. 29,6% vastanud naistest peab end probleemilahenduses pädevaks ja 69,4% vastanud meestest peab end probleemilahenduses pädevaks. Sarnane tulemus on ka seadme kaitsmises – 32,2% vastanud naistest peab end antud valdkonnas pädevaks ja 67,8% vastanud meestest peab end antud valdkonnas pädevaks. Antud tulemust võis kallutada see, et vastajate hulgas olid paljud mehed IT erialaga, kuid naised mitte.

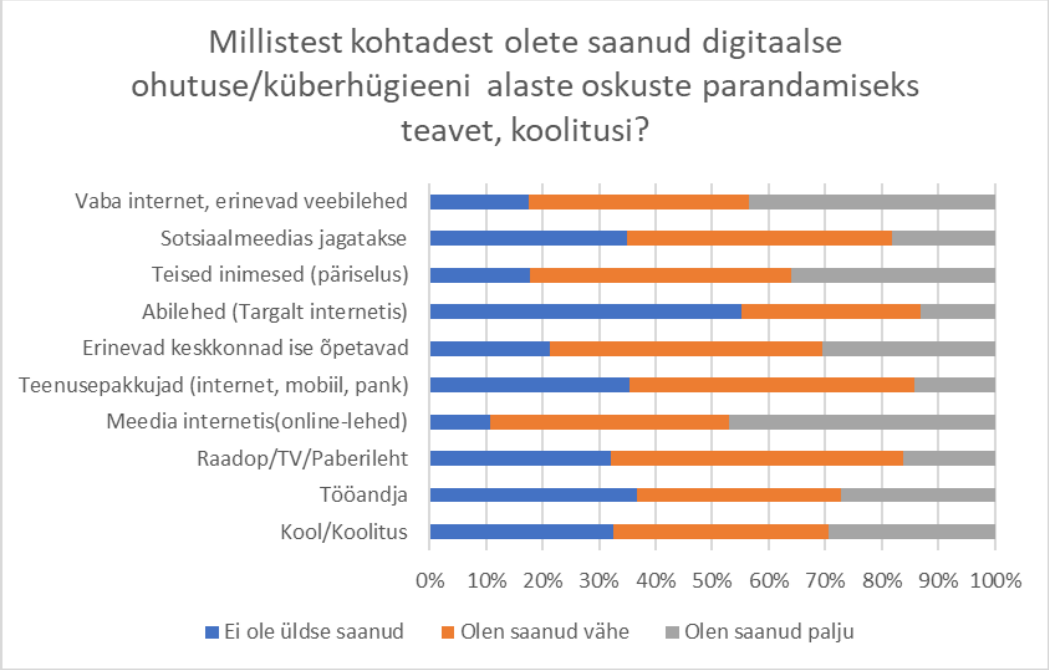
Samuti vaatas autor, kas digipädevuse olukord erineb vanuseliselt. 59,4% vastanutest, kes hindavad end pädevaks probleemilahendamises digikeskkonnas on 21 kuni 40 aastased. 40,6% vastanutest, kes hindavad end pädevaks probleemilahendamises on 41 kuni 60 aastased. 48,8% vastanutest, kes hindavad end pädevaks seadme kaitses on 21 kuni 40 aastased ning 51,2% vastanutest, kes hindavad end pädevaks seadme kaitsmises (rakendate ohutuse ja turvameetmeid) on 41 kuni 60 aastased. Antud tulemuse kohta võib öelda, et nooremad vanuses 21-40 aastased tunnevad end probleemilahenduses mugavamalt, sest võib arvata, et nooremad on antud oskusi saanud koolist või ülikoolist Võrdsed tulemused on vastajatel seadme kaitsmise osas, mis võib olla tingitud sellest, et üha rohkem räägitakse ühiskonnas arvuti/nutitseadme lukustamisest (vt 2.3.).

Intervjuu tulemustest tuli samuti välja, et töötajad veedavad arvutis/nutiseadmes väga palju aega. Digiseadmeid kasutatakse 8 tundi tööjuures ja koju jõudes jätkatakse tegevusi meelelahutuse valdkonnas. Intervjueeritavad pidasid end samuti üsna oskuslikuks ja hindasid ennast viie palli süsteemis kolme palli väärilisek. Kõik intervjueeritavad andsid mõista, et on teadlikud küberhügieenist või nõuetest, et kasutada tehnikat turvaliselt. Vastajate meelest on oluline omada teadmisi internetis info jagamise, veebilehtede külastamise ning failide alla laadimise ohutuse kohta.

Kokkuvõtteks võib öelda, et naised ja mehed peavad end võrdselt pädevaks tavatoimingute tegemisel. Digitaalse pädevuse valdkonnas tunnevad meessoost vastajad ennast naissoost vastajatest kindlamalt. 21 kuni 40 aastased vastajad hindavad end pädevamaks kui 41 kuni 60 aastased vastajad. Antud põhjuseks võib olla see, et need vastajad, kes on alla 40 aasta on saanud arvutikasutuse kohta infot koolist/ülikoolist ja alustasid tehnika kasutamist nooremas eas.

.

Teine suurem küsimus keskendus enese aitamisele läbi info leidmise ja koolituste. Kui teoreetilises ülevaates selgus (vt 1.1.), et täiskasvanud töötajate oskused on Euroopas keskmiselt pigem halvad ja kui Küberpähkli uuringust selgub, et inimeste enesehinnangud ei ole nii madalad, siis oluline on teada saada, millistest kohtadest inimesed abi oskuste parendamiseks hangivad. Uuringu teoreetilise osa kirjutamiseks otsis autor võimalusi, mida täna täiskasvanutele pakutakse. Selgus, et koolitusi, mis puudutaks otseselt küberhügieeni, oli pigem vähe.,. Pigem pakuti koolitusi lapsevanematele, töövahendite kasutuskoolitusi läbi IT koolitusfirmade ning ettevõtetele. Järgmisel joonisel (Joonis 3) on välja toodud, kust saavad täiskasvanud peamiselt informatsiooni küberhügieeni kohta.



Joonis 3. Kohad, kus täiskasvanud saavad infot küberhügieeni kohta

Selgus, et kõige populaarsem koht, kus vastajad said küberhügieeni alaseid teadmisi on meedia (online-ajalehed). 47% vastajatest saab peamise informatsiooni küberhügieeni kohta meediast. Populaarsuselt teisel kohal on erinevad veebilehed, näiteks sobilik erileht oleks arvatavasti Arvutikaitse.ee. 43,4% vastajatest saab küberhügieeni alast infot internetis erinevatelt veebilehtedelt. Kõige vähem kasutavad vastajad abilehtesid nagu Targalt Internetis. Selle põhjenduseks võiks olla see, et antud veebileht on suunanud oma fookuse õpilastele, vanematele ja õpetajatele. 55,1% täiskasvanuid ütleb, et abilehtedest

ei ole nemad üldse infot saanud. Abilehed on siis näiteks keskkonna infovärav turvalisuse tagamiseks, mis on avatud erinevate sotsiaalmeedia portaalide juurde.

Ka läbi viidud intervjuu kinnitas saadud mõtteid, et peamine allikas, kus intervjueeritavad saavad informatsiooni on meedia. Samuti mainitakse, et põgusalt saadakse informatsiooni ka tööandjalt, kuid see seisneb pigem esmakordselt tööle asumise ajal sovitustest tehnika kasutamiseks, näiteks arvuti lukustamine töökohalt lahkudes. Intervjuudest tuleb välja, et täiskasvanutel on huvi abilehtede vastu. Lastele, õpetajatele ja lastevanematele suunatud leht on juba olemas, nagu „Targalt internetis." Täiskasvanutele sarnast lihtsat veebilehte intervjueeritavate meelest veel olemas ei ole, kuid intervjueeritavad usuvad, et sellest oleks abi.

Kokkuvõtteks saab öelda et peamiselt saavad vastajad informatsiooni meediast. Nii Euroopa kui ka Eesti küberjulgeoleku strateegias oli küberteadlikkuse kasvatamine üks prioriteete. Üks võimalus selleks, on meedias seda kajastada.Teine võimalus oleks luua sobilik abiveeb ka täiskasvanutele, mis oleks „inim-keeles", mitte „IT-keeles".

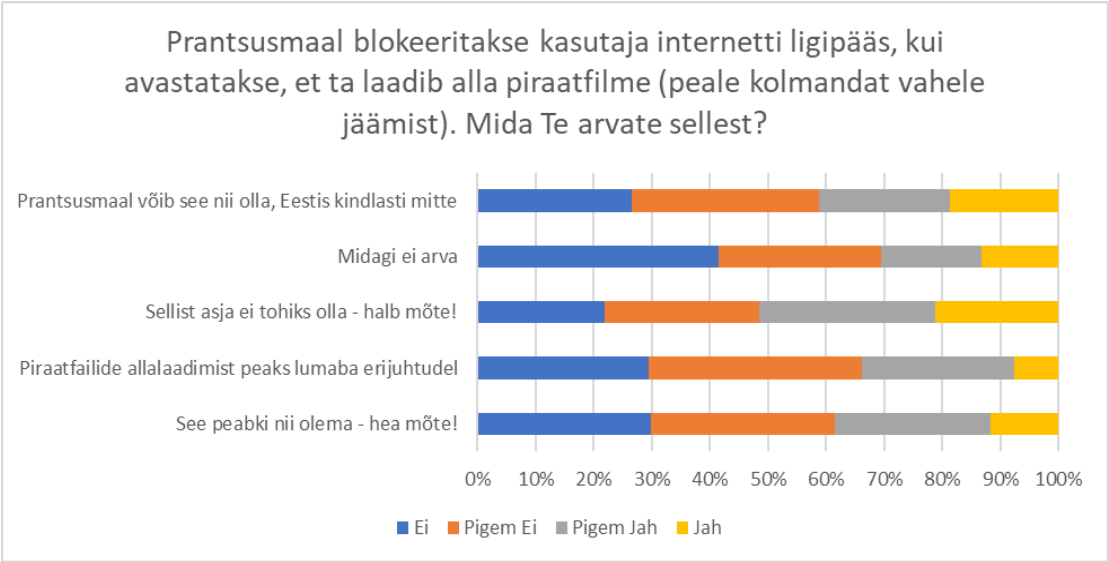
5.1.2 Käitumine näidisolukorras

Üheks uuringu osaks olid näidisolukorrad. Näidisolukorrad loodi kahe aktuaalse teema kohta, milleks valiti piraatlus ja lunavara. Antud näidisolukordades pidid vastajad hindama enda käitumist Likert skaalat kasutades erinevate valikute osas. Näidisülesanne annab aimu, milline on vastaja esimesed mõtted ja sammud, kui ta peaks hakkama vastavat olukorda lahendama.

5.1.2.1 Piraatlus

Internetipiraatlus käigus omandatakse ja levitatakse interneti kaudu ebaseaduslikult autoriõigusega kaitstud teoseid. Antud näidisolukord, aitab autoril aru saada, milline on täiskasvanud töötajate suhtumine piraatlusesse.

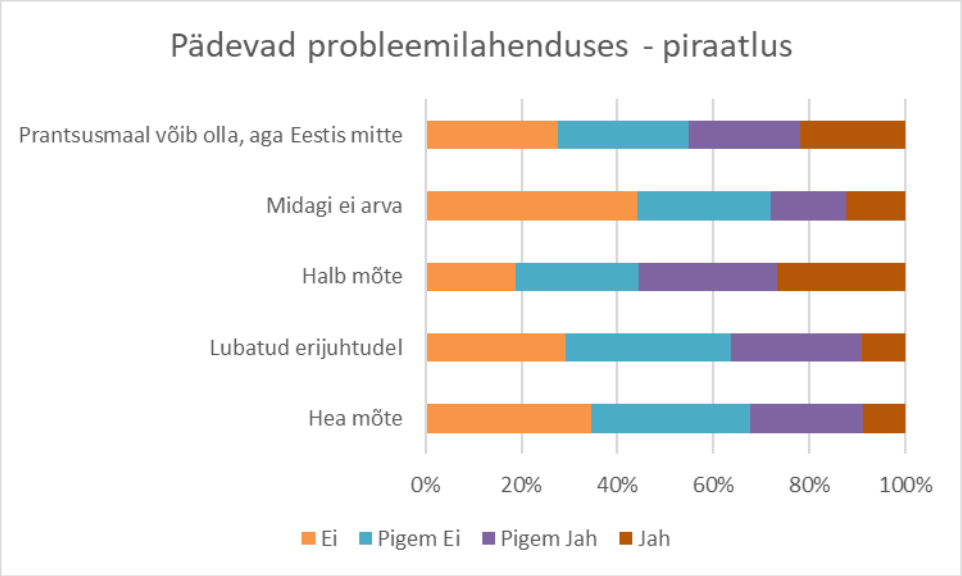
Joonisel (Joonis 4) on välja toodud, mida arvaksid vastajad, kui näiteks Prantsusmaal kehtestataks antud reegel: Internet blokeeritakse, kui jäetakse kolm korda piraatlusega vahele. Joonisel (Joonis 4) on toodud vastajate arvamused.



Joonis 4. Näidisolukord – piraatlus

Vastavalt joonisele (Joonis 4) arvab 51,6% vastanutest, et tegemist on halva mõttega ja sellist reeglit ei tohiks olla. Samuti on näha, et vastajad arvavad, et antud reegel on ka Prantsusmaa poolt ebamõistlik. Siinkohal on paslik viidata 2017. aasta Küberpähkli õpilaste tulemustele, millest selgus, et ka nemad peavad vastavat reeglit väga ebapraktiliseks ja Eestis oleks selline samm katastroof [60]. See näitab trendi, et Eesti ühiskonnas ei ole mitte kõik liikmed valmis tarkvara ja digitaalse sisu eest maksma.

Autor vaatas ka eraldi üle vastajate, kes peavad end pädevaks probleemilahenduses, kas nemad suhtuvad piraatlusesse samamoodi, nagu üleüldine tulemus või esineb erinevusi. Tulemused on toodud joonisel (Joonis 5).



Joonis 5. Pädevad täiskasvanud probleemilahenduses -piraatlus

Vaadates joonist (Joonis 5), siis ka end tehnoloogiaalaselt pädevaks pidavad vastajad ei ole nõus sellega, et piraatluse eest karistataks nii karmilt. 67,6% vastanutest arvab, et piraatluse eest karistamine nii karmilt ei ole hea mõte. Samas on näha, et üle 60% vastanutest arvab, et piraatlust ei tohiks siiski lubada ka erijuhtudel, seega võib väita, et Eesti ühiskonnas on arvamus piraatluse osas pigem lõhestunud.

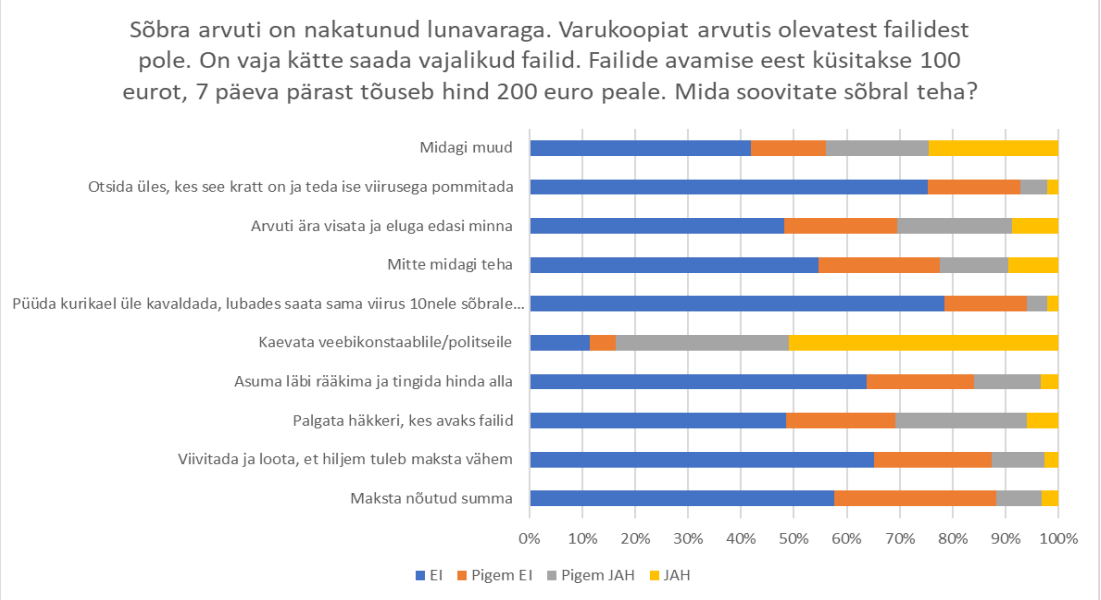
Intervjuus osalejate arvamuse kohaselt, aga ei ole piraatlus tänasel päeval enam nii aktuaalne teema, kui näiteks 10 aastat tagasi. Kõik intervjueeritavad kasutavad nii tööl kui ka kodus legaalseid programme ja ei näe otseselt vajadust piraatluse harrastamiseks. Intervjuu tulemustel pole piraatlus enam nii populaarne, kui vanasti, kuid tuleb välja tõsiasi, et vastajad ei saa ka päris täpselt aru, millal on tegemist piraatfailiga ja millal mitte ja kas see on üldse karistatav kuritegu. Vastajad arvavad, et kunagi oli piraatlus populaarsem, sest Eestis puudusid paljud võimalused muusikat, filme, programme legaalselt soetada või oli soetamine väga kallis. Tuuakse välja, et piraatlus peaks olema kuidagi reguleeritud, kuid Prantsusmaa kohta tehtud näidislahendus oleks liiga karm. Samas ei osanud ükski intervjueeritav ise paremat lahendust probleemile pakkuda.

Kokkuvõttena võib öelda, et vastajad justkui saavad aru, et piraatlus ei ole õigustatud tegevus ja sellega kaasneb ohtusid, kuid siiski ei suudeta aktsepteerida karme reegleid ja seda kasutatakse endiselt, kui vajadus tekib. Samas seos piraatluse ja kuritegevuse vahel jääb vastajate hulgas pigem arusaamatuks.

5.1.2.2 Lunavara

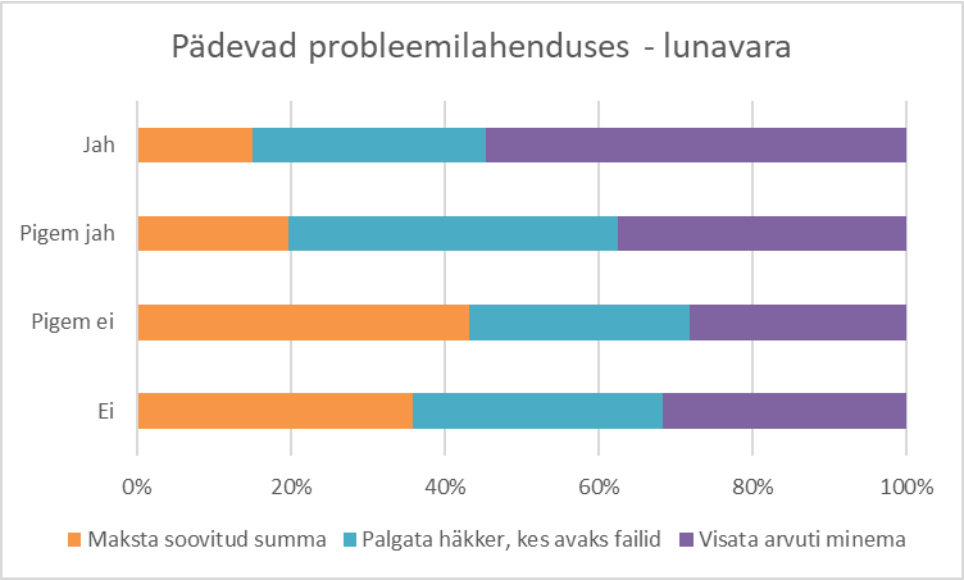
Lunavara on pahavara, mis takistab kasutajal arvutis olevate programmidele või failidele ligi pääseda. Piltlikult võtab lunavara kasutaja arvuti pantvangi ning nõuab vabastamise eest lunaraha. Antud näidisolukord, aitab autoril aru saada, milline on täiskasvanud töötajate teadmised ja suhtumine lunavarasse.

Vaadates antud joonist (Joonis 6), siis on näha, et 83,6% vastajatest soovitaks kaevata veebikonstaablile või politseile. Kõige vähem tõenäoliseks osutus vastusevariant – otsida viiruse jagaja üles ning asuda samalaadsele vastutegevusele.



Joonis 6. Näidisolukord - lunavara

Palju huvitavamad on vastusevariandid, milleks on palgata häkker, nakatunud seade ära visata ja tasuda soovitud summa Autoril tekkis huvi, et mida teeks antud olukorras kasutajad, kes hindavad end pädevamalt probleemilahenduses. Järgmisel joonisel (Joonis 7) selgub, et vastajad ei ole nõus tasuma lunaraha, nagu ka kõik teised vastajad, aga soovitavad, kas arvuti ära visata või pöörduda häkkerite poole.



Joonis 7. Pädevad probleemilahenduses – lunavara

Kuna vastused on seinast seina, siis see näitab, et esiteks pole inimestel arusaama, mis on lunavara viirus ning esimene õlekõrs on haarata tugevama abi järgi, milleks antud olukorras oli veebikonstaabel, kes internetis tasuta nõu annab. Edasised valikud näitasid, et tegelikkuses olukorrale head lahendust polegi, sest häkkeri palkamine tooks kaasa ikkagi lisakulud ja tulemus oleks sisuliselt teadmata. Arvuti äraviskamine näitab, et inimesed on juba ette lootuse kaotanud või annavad nõu, mis pole adekvaatne. Kui teha tagasipõige teooriasse (vt 2.4.), siis sealsed eksperdid andsid nõu maksta ja oma failid tagasi saada või olla „teinekord“ targem, ning teha varukoopiad, siis antud uuringus vastajad seda meelt ei olnud, et failide kättesaamiseks peaks kurjategijaid nende tegevuses toetama.

Intervjueeritavate meelest on lunavara nende jaoks uus tundmatu termin, ning seda riski peaks ühiskonnas enam selgitama. Kaks intervjueeritavat olid seda meelt, et failide tagasi saamiseks tuleks tasuda nõutud summa ja loota, et failid saab tagasi. Üks intervjueeritav tõdeb, et tuleks pöörduda spetsialisti poole, kes saaks ehk olukorra päästa ning samuti tõdeb, et vahel võib juhtuda, et ei olegi enam midagi päästa. Kaks vastajat (lihttöötajatest vastajad) on nõutud ja ilmselt otsiks infot internetist, ning pöörduks siis tööl IT poole või mõne IT valdkonna sõbra poole. Üks intervjueeritavast ütleb, et tuleb osta uus andmete varundamise ketas ja võimalusel nii palju andmeid ümber salvestada kui võimalik. Üllatav oli see, et peaaegu pooled vastajate tutvusringkonnast olid juba lunavara probleemiga kokku puutunud. Peale lunavara mainiti küberkuritegudena muid pahavara

ja viiruseid, näiteks Facebooki konto ja ka arvuti kaaperdamist. Muredele üldiselt oldi saadud läbi IT osakonna lahenduse, kuid ise vastavat olukorda ikkagi lahendada ei osataks, kui see ette kerkiks. Abi vajaksid ka IT teadlikumad vastajad.

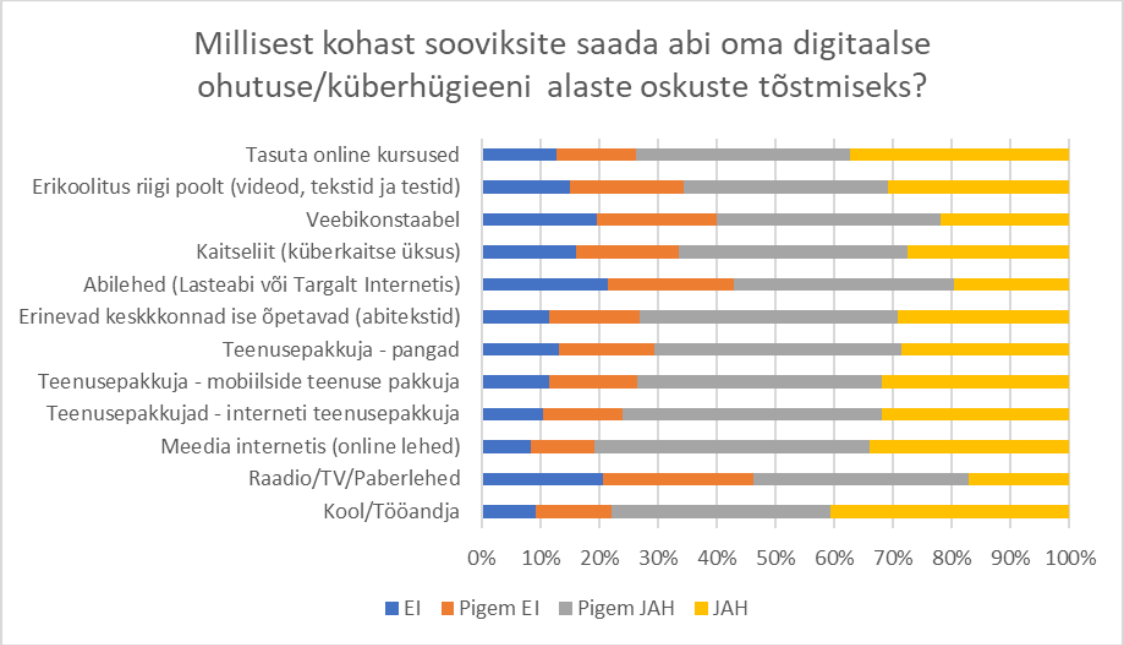
Kokkuvõtvalt võib öelda, et lunavara teema ühiskonnas on pigem läbi rääkimata ja lahendused pole siiani inimeste teadmistesse jõudnud. RIA kui ka teised eksperdid (vt 2.4.) soovitavad regulaarseid varukoopiate tegemist juba aastaid, aga ometigi on see asi, milles inimesed pidevalt eksivad.

5.2 Küberhügieeni alaste oskuste arendamine

Euroopa Liit, kui ka Eesti on kindlad, et küberhügieen on teema, millest peab ühiskonnas rääkima (vt 1.1.). Antud peatükis uurib autor vastajate käest, et kust nad sooviksid saada antud valdkonna kohta infot ja mida nad arvavad üleüldiselt antud teema lahendamisest Eestis.

5.2.1 Töötajate ootused küberhügieeni alaste oskuste parendamiseks

Küberhügieeni teadlikkuse tõstmine on oluline valdkond ja enne teavitustöö alustamist tuleks uurida, mil moel sooviksid täiskasvanud kasutajad informatsiooni. Järgmisel joonisel (Joonis 8) on välja toodud täpsem ülevaade, kus vastajad sooviksid saada informatsiooni küberhügieeni alaste teadmiste kohta.

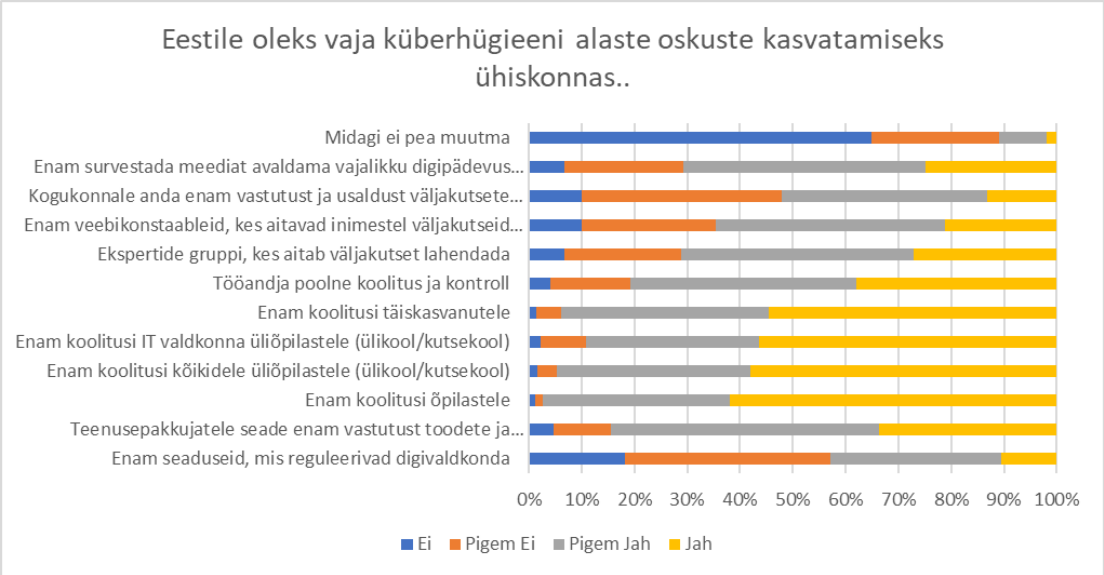


Joonis 8. Kohad, kus täiskasvanud soovivad saada infot küberhügieeni kohta

Vastavalt ülaltoodud joonisele (Joonis 8) on tulemustes näha, et üle 80% vastanutestsoovivad saada informatsiooni küberhügieeni alaste teadmiste tõstmiseks meediast internetis (online lehed),. 77,8% vastajatest soovib saada küberhügieeni alaseid teadmisi koolist või tööandjalt. populaarne vastus on ka tasuta online kursused, kus 37.3% vastajatest valis vastuseks „Jah“ ning 36,4% vastanutest „Pigem Jah“. Kui vaadata antud joonist (Joonis 8) üleüldiselt, siis üle poolte vastanutest üteleb „Jah“ ja „Pigem Jah“ kõikidele pakutud lahendustele. Seega üle 50% vastanutest soovib saada infot küberhügieeni alaste teadmiste kohta kõikidest võimalikest kohtadest.

Intervjuust tuleb välja, et peamiselt soovivad vastajad saada infot küberhügieeni alaste teadmiste kohta tööandjalt. Samas toob eraldi välja tööandjast vastaja, et tema soovib samuti saada eelnevalt infot, mida ja kuidas töötajatele tuleks edastada. Näitena toob ta välja praegu aktuaalse GDPR (*General Data protection Regulation*) regulatsiooni. *„Kõik tööandjad teavad, et tuleb teha erinevaid muudatusi, kuid tööandjatel puudub täpne õpetus.“*

Järgmisena uuriti milliseid meetmeid tuleks Eesti ühiskonnas rakendada selleks, et küberhügieeni alane olukord pareneks. Tulemused on toodud välja järgmisel joonisel (Joonis 9).



Joonis 9. Küberhügieeni alaste oskuste kasvatamine Eesti ühiskonnas

Antud jooniselt (Joonis 9) näeb, et vastajad on väga huvitatud küberhügieeni alaste teadmiste tõstmisest. Vastanud arvavad, et tuleb teha rohkem koolitusi õpilastele, üliõpilastele, IT valdkonna üliõpilastele ja täiskasvanutele. Antud vastusest saab järeldada, et kõikidele vanusegruppidele tuleb siiski antud valdkonnas keskenduda. Üle 80% vastanutest soovib tööandja poolset koolitust ja kontrolli. Lisaks arvatakse, et Eestis peaks olema ekspertide grupp, kes aitaksid väljakutset lahendada. Vastanud usuvad, et rohkem peaks olema veebikonstaableid ja ka teenusepakkuja peaks jagama küberhügieeni alast infot seadme soetamisel. Oodatakse, et tuleks survestada meediat, et info jõuaks enamate inimesteni. Peaaegu 90% vastajatest on nõus, et midagi peab muutma ja vanaviisi enam ei saa. Samas on näha, et vastanud ei usu, et reguleerivate seaduste loomine oleks antud olukorra parendamisel lahenduseks.

Intervjuust tuli välja, et digitaalsest ohutusest tuleks hakata rääkima juba lasteaias. Intervjueeritavad olid seda meelt, et lastele, noortele ja tudengitele on võimalus läbi haridussüsteemi õpetada turvalist käitumist digimaailmas. Praegu on ka tööturul täiskasvanud inimesed, kes koolis omal ajal arvutite kohta infot ei saanud, küberhügieenist rääkimata. Vastajad usuvad, et digioskustega kimpus olevatele töötajatele peaks antud infot edastama tööandja. Sellest väljendus ka arvamus, et need kes juba on „digipädevad“ vajaksid vähem õpetust. Viidates tagasi teooriasse (vt 1.1), siis ka Euroopa Liidu eksperdid toovad välja, et vastus paremateksteadmisteks ja oskusteks peitub koolis, kuid kui keskendutakse ainult kooliskäijatele, siis jäetakse unarusse need inimesed, kes enam koolis ei käi ja kellel pole ka lapsi, kuid kes võibolla viibivad tööturul veel mitmed aastakümned. Kindlasti ei piisa ühekordsest rääkimisest, väid tegemist on järjepideva protsessiga, kus vanu teadmisi meelde tuletatakse ning uusi juurde lisatakse, mis vahepeal on tehnoloogia arengus toimunud (näiteks targad kodumasinad). Sellised lahendused meenutavad töötajatele kohustuslikena kehtivaid tuleohutuse ja sarnaseid koolitusi, mida tööandja peab pakkuma.

Küberjulgeoleku strateegia 2014-2017 (vt 1.1) üheks eesmärgiks oli ühiskonnas digipädevuse kasvatamine. Juhul, kui vaadata saadud tulemusi, siis on näha, et täiskasvanutele ei ole teavitustööst piisanud, ning nad sooviksid saada informatsiooni kõikvõimalikest kohtadest. Samuti usuvad vastajad, et ühiskonnas peab midagi ette võtma, et olukord paraneks ja üheks selleks võimaluseks saaks olla koolituste pakkumine ja ka tööandjatele vastutuse jagamine.

5.2.2 Töökeskkonna arendamine

Lisandväärtusena uuris autor intervjuu ajal intervjueeritavatelt töökeskkonna kohta, et aru saada, kas tööandja poolt on juba näiteks rakendatud regulatsioone erinevate küberhügieeni alaste toimingute osas. Küberhügieen on oluline tööandja vaatest (vt 1.1.), sest küberkuritegude korral on töötajast arvutikasutaja nõrgim lüli ja selle kaudu on võimalik ettevõttele ka ärilist kahju tekitada.

Kõik intervjueeritavad tõdevad, et ettevõtetel on erinevaid regulatsioone, kuid kui neid regulatsioone oleks liiga palju, siis töötaja ei suuda neid kõiki ühtemoodi hästi täita. Regulatsioonid digitaalse ohutuse vallas peaksid olema pigem intuitiivsed ja toetama seeläbi turvalist käitumist, kuid mitte tekitama olukorda, kus toimuks ka karistamine. Autor toob siin ära erinevad teemad, mille üle intervjuudes töökeskkonda arendamise kohta kõik vastajad midagi arvasid:

- esimesena tuuakse välja e-mailidega saadetud failide avamine. Kindlasti tuleb töötajal veenduda, et tegemist on korrektse failiga. Igaüks eeldab, et kõik teavad, milline on korrektne ja ebakorrektne kirja manus, aga tegelikkuses on sellest vahel raske aru saada.Enamasti on nii, et kui saabub ettevõttesse e-kiri, siis töötajal on kohustus veenduda e-kirja korrektsuses enne selle avamist. Antud ettevõtte töötajad ei olnud teadlikud, mida teha olukorras, kus on avastatud näiteks õngitsuskiri. Enamasti käitutakse „sisetunde alusel“, mis igal inimesel on teatavasti erinev – osad otsustavad kirja ignoreerida või kustutada, teised saadaks IT teenindusse, kui selliste kirjade hulk hakkab sagenema, kolmandad oleks lihtsalt nõutud, et kuidas saab kirja manust, seda avamata, pidada ohtlikuks, kui kiri ise tundub ohutu;

- teisena tuuakse välja tehnika ja teenuste ristkasutuse turvalisus. Intervjueeritavad annavad teada, et peamiselt kasutavad töötajad töö poolt antud sülearvutit, mida võib koju kaasa võtta, ikkagi töö tegemiseks, sest kodukontori võimalus on tänasel päeval tööandja vastutulek töötaja soovidele. On juhuseid, kus tööks on kasutusel ka osaliselt isiklik arvuti. Selleks, et töö kirjadele kiirelt ligi pääseda saavad töötajad kasutada isiklikku või töö poolt antud nutitelefoni. Sellisel juhul usuvad intervjueeritavad, et seadmel peab olema kindlasti parooliga ekraanilukk. Intervjueeritavad usuvad, et peamine reegel, mis tööseadmega kaasneb ongi selle korrektne lukustamine (parool, ekraanilukk töökohalt või arvuti juurest lahkudes).

Kõigil töötajatel on isiklik tööarvuti ja kasutajanimi, mida nad saavad töö tegemiseks. Juhul kui on vaja mingil põhjusel laenata kolleegi tööarvutit, siis kõik vastajad on ühel nõul, et tuleb kasutada enda kasutajanime ja sellisel juhul probleemi nad ei näe. Intervjueeritavate sõnul ei ole antud teema väga aktuaalne, sest kõigil on enda seadmed, mis käivad ka kodus kaasas. Samas oht, et seda kasutavad pereliikmed on väike, sest tänasel päeval on antud vastajate pereliikmetel enda seadmed. Samas mainitakse, et selge see, kui kasutab mõni pereliige, siis töötaja on vastutav antud tegevuse eest. Mis puutub aga e-kirjade ristkasutusse, siis pigem on tavapärane, et tuleb saata tööasju isikliku e-maili pealt ja vastupidi. Intervjueeritavad mainivad, et isikliku e-maili kasutatakse vahel testimiseks, nt veenduda, et ettevõtte süsteemi kiri jõuab. Üks intervjueeritavatest ütleb, et vahel leiab töövälisel ajal mõne artikli, mida tuleks tööjuures täpsemalt uurida ja saadab selle enda isiklikult e-maililt töö e-mailile. Kuna vahel on ettevõtted sõlminud lepingu, et tööandja võib töötaja emaile kontrollida, siis isiklike kirju tööandja avada ei tohiks, seega enamasti on lepingus punkt, et töötaja ei tohi tööpostkastist isiklikke kirju saata. Lõpuks tuuakse lahendusena välja, et juhul kui on tööarvuti kasutamisel kindlad regulatsioonid, siis peaks neid ka aeg-ajalt töötajatele meelde tuletama. Peamised rikkumised tulevad vastajate meelest siiski sellest, et töötaja ei olnud teadlik või oli kiire;

- kolmandaks puutuvad töötajad kokku erinevate andmetega, kuid peamised kriitilised andmed, millega töötajad kokku puutuvad on isikuandmed, ärisaladused ja klientide andmed. Näiteks mälupulga kasutamisel tekkis intervjueeritavate seas erimeelsus. Üks intervjueeritavatest oli arvamusel, et mälupulga kasutamine peaks olema ettevõtetes keelatud. Ülejäänud arvavad, et mälupulga kasutamine ei peaks olema ettevõtetes keelatud, kuid loomulikult ei ole tööfailide laadimine mälupulgale lubatud. Tööandja sõnul tuleb töötajaid usaldada ja ei tasu kõike võimalusi ära keelata. Samas ei teadnud ükski intervjuus osalejatest vastata, millist viirusetõrjet tööandja nende tööarvutis kasutatakse ja kas sellega mälupulga kasutamise korral ka viiruseid kontrollitakse;

- neljandaks teemaks kerkis tööarvutis olevad programmid ja nende legaalsuse tagamine. Lahendusena nähti ette, et kõik programmid arvutis peaksid olema seadistatud läbi IT-administraatori, kes vastutab ka tarkvara heakorra eest (et see

on legaalne, uuendatud ja viirusevaba ja nii edasi). Samas usuvad töötajad, et juhul kui töötajal on vaja tööarvutisse X programmi isiklikuks tarbeks, siis peaks tööandja sellele vastu tulema. Kõige enam peaks tööandja pöörama tähelepanu, et kõik kasutusel olevad programmid töötaja arvutis oleksid legaalsed;

- viiendaks teemaks võeti ette traadita interneti ehk WIFI võrgu kasutamine ettevõtetes, mida nähti kui mugavusteenust, mis on enamasti tänapäeval ettevõtetes normaalsus kui erisus. Vastajad tõid välja, et oluline on pakkuda erinevaid WIFI alamvõrke töötajatele ja külalistele, ning mõlemad peaksid olema kaitstud parooliga. Teoorias justkui kõik teavad, et töötaja isiklik seade võiks olla pigem külaliste võrgus ja tööks vajalik seade töö võrgus, kuid reaalsuses nenditakse, et kui üks võrk on kiirem, siis selle taha ühendatakse ka seade. Eelistatuna ühendatakse ka isiklike seadmetega töö sisevõrku, mis peaks olema ette nähtud ainult töökoha seadmetele. Põhjenduseks tuuakse, et töövõrk tundub turvalisem;

- kuuenda teemana arutleti isikliku sotsiaalmeedia kasutamist tööajal ja tööseadmega. Teatakse, et osades ettevõtetes ei või külastada sotsiaalmeediat, uudiste portaale tööajal ja tööseadmega. Vastukaaluks tuuakse välja, et liigsed või töötajale arusaamatud reeglid võivad pigem tööd segada ja loomingut pärssida, kui turvalisust tagada, sest kui töötaja tahab töö ajal internetti pääseda, siis küll ta selleks võimaluse leiab ja siis see arvatavasti ei oleks nii turvaline. Teiselt poolt nendivad intervjueeritavad, et on oluline, et tööandjal oleks ülevaade töötajal kasutusel olevatest programmidest, töövõrgus käivatest seadmetest, sest kui on sattunud töötaja programmide hulka midagi kahtlast, siis on võimalik, sellega koheselt tegeleda ning selle võrra võib kahju olla väiksem;

- seitsmendaks tuuakse välja pilveteenuste kasutamise probleemid. Probleemiks on pigem see, et reegleid pole- kõik intervjueeritavad usuvad, et isikliku pilve kasutamine tööasjade hoidmiseks ei ole mõistlik lahendus, kuid antud tegevust on ettevõttel väga keeruline kontrollida. Tööandjast vastaja lisab, et tänasel päeval puudub antud ettevõttes töötajal isikliku pilveteenuse kasutamiseks konkreetne vajadus, sest töötaja saab soovitud infole ligi tööarvuti ja VPN ühendust kasutades. Sama ettevõtte töötajad seda samas välja tuua ei osanud.

Antud intervjuust sai autor teada, et trend on avatuse poole ja liigsed regulatsioonid ei ole töötajatele meeltmööda. Pigem soovivad töötajad saada rohkem informatsiooni võimalike ohtude kohta, et töötajana käituda arvutis targemalt. Ka intervjuus osalenud tööandja usub samuti, et suund on avatuse poole, kuid ta nendib ka seda, et piir eraelu ning tööelu vahel on õhkõrn. Juhul kui tööandja soovib, et töötajad oleksid loomingulised ja tooks ettevõttele väärtust, siis ei saa pidevalt seada erinevaid piiranguid, sest erinevad regulatsioonid pigem takistavad töö tegemist, kui sellest kasu saadakse. Seega turvalisus ei ole otseselt asi, mida ei võiks mugavuse vastu välja vahetada, aga reaalsuses seda tihti siiski kiputakse tegema, mõtlemata ohtudele, sest need ohud tunduvad olevat nii ettevõtte töötajatele kui ka tööandja esindajale pigem abstraktsed, kui reaalsed.

6 Soovitused

Antud magistritöö keskendus täiskasvanud töötajate küberhügieeni alastele oskustele ja ootustele selle parendamisel. Soovitused seega saab anda kolmele sihtrühmale: teadlikkuse tõstmise programmid/strateegiate loojad, tööandjad ja töötajad.

Teadlikkuse tõstmise eest vastutajad saavad:

- luua täiskasvanutele õppijatele toetav veebileht. Töötajad on leidlikud õppijad, kes leiavad vajaliku õppevara internetist – online meediast, abiveebidest – loo sobilikke keskkondasid, milles inimesed saaks oma oskuseid reaalselt proovile panna. Kui lastele ja lapsevanematele ja õpetajatele on programm „Targalt internetis“, siis täiskasvanutele, kes sinna sihtrühma ei kuulu pole oma keskset veebipesa kuskohast otseselt „inimkeelselt“ abi saada, uudiseid lugedes, teste teha ja oma küberhügieeni alastes oskustes veenduda;

- luua koolitusprogramm või e-kursus, mida saab huviline kasutada eneseharimiseks või tööandja kasutada oma töötajate koolitamiseks. Kõige lihtsam on teha ennetustööd inimestega, kes on veel haridussüsteemis – koolis, ülikoolis, kutsekoolis või osalevad koolitustel. On vaja tekitada formaalseid ja ka mitteformaalseid õppimisvõimalusi täiskasvanutele, kes haridussüsteemis enam ei ole;

- märgata erinevaid sihtrühmasid ja vajadusi ühiskonnas (vanemad inimesed, vähese digioskusega inimesed jt.). Kõik ei pea olema küberhügieenis samal tasemel, aga kõikidel peaks olema baastase. Kuna täna puudub arusaam, mis on baastase ja mis on sellele järgnevad astmed praktilisel tasemel, siis tuleks kõigepealt luua maatriks, ning selle alusel saab hakata juba looma teste ja materjale.

Tööandjad saavad:

- harida kõiki oma töötajaid küberhügieeni alal järjepidevalt, kas kord aastas või vähemalt korra kahe aasta jooksul. Vajadusel tuleks läbi viia hindamine;

- võtta erilise hoole alla töötajad, kes pole kunagi arvuti ja tehnoloogiakasutust koolis, koolitustel või iseseisvalt omandanud. Arvatavasti on teadmistes augud, mida tuleks täita. Selle üle rõõmustavad nii töötajad ise kui ka tööandja, kui oskamatusest tehakse vähem vigu, näiteks klikitakse lahti vähem viiruseid või andmekaeve kirju;

- motiveerida ja tunnustada turvalist käitumist teiste vahenditega. Näiteks luua tunnustussüsteem, avatud õhkkond, et inimesed oma muredest ja töökeskkonda puudutavatest väljakutsetest räägiks. Aita inimestel luua tugisüsteem, kus ka kolleeg saab kolleegilt nõu küsida. Kaks pead on kaks pead! Reeglite küllus ei ole lahendus, sest see demotiveerib töötajaid;

- omada ülevaadet, kuidas toimetavad töökeskkonnas teie töötajad – palju tuleb ette tehnika, teenuste ristkasutust, palju laetakse siseinfot pilveteenustesse, kas asutuse WiFi on eesmärgipäraselt kasutuses või muud sarnast. Selle kohta saab luua ülevaate ja anda soovitusi, kuidas oleks turvalisem;

- omada tegutsemisjuhiseid ja strateegiat, mida teha olukorras „X“. Tänases töös vaadeldi kahte olukorda nagu piraatlus ja lunavara, kuid neid juhtumeid on veelgi, mille vastu ettevõtja peaks ennast valmistama. Parimal juhul jaga neid tegutsemismalle ennetavalt ka oma töötajatega ja võta kasutusele riske maandavad lahendused.

Töötajad saavad:

- pöörduda mure korral IT abiteenuse poole või pidada kolleegiga aru;

- harida ennast erinevate võimaluste abiga – uurige kirjeldust, lugege veebilehti, leidke konverentse ja koolitusi, jagage mõtteid kolleegidega. Oskused paremini hakkama saada aitavad teid ennast ja on rõõmuks ka tööandjale, kelle äri ja mainet te seeläbi vähem ohtu seate.

7 Kokkuvõte

Antud magistritöö teema on Eesti kui ka Euroopa ühiskonnas aktuaalne, sest mõlema üheks küberjulgeoleku strateegia eesmärgiks on avalikkuse teadlikkuse tõstmine küberohutuses. Uurimuses keskendus autor täiskasvanud töötajate küberhügieeni alastele pädevustele ja nende uurimisvõimalustele. Sooviti teada saada kui pädevaks hindavad täiskasvanud töötajad oma küberhügieeni alaseid oskuseid täna enesehindamise korras ja millised on ootused küberhügieeni alaste oskuste tõstmiseks, nii läbi viidud uuringu kui ka intervjuude põhjal.

Andmete kogumiseks osales autor töögrupis, mille eesmärgiks oli koostada ja läbi viia Kaitseministeeriumi poolt tellitud uuring-test Küberpähkel. Antud uuringusse lisas autor omapoolt neli küsimust ning kaks näidisjuhtumit, mida antud magistritöös analüüsiti. Uuringu teiseks valideerivaks meetodiks valiti intervjuu, mis viidi läbi kuue täiskasvanud töötajaga. Saadud vastuste analüüsimisel selgus, et vastajad hindavad end kõige pädevamaks digitaalkeskkonnas suhtlemises ja oskused on enamus omandanud ja hoidnud pigem iseõppimise teel läbi erinevate online veebilehtede. Oskused hakkama saada erinevates olukordades sõltuvad nii teadlikkusest kui ka suhtumisest probleemi, näiteks, kui piraatlust peetakse leebeks kuriteoks, millega ei peaks Eestis tegeletama, siis lunavara juhtumi korral puudub arusaam täiesti, mida peale veebipolitseile kurtmise reaalselt ette võtta – kas visata arvuti ära või palgata häkker.

Uuriti ka olukorda töökeskkonnas, mis joonistas välja mitmeid uusi väljakutseid, mida just tööandja peaks oma töötajatele selgitama, et tagada oma äri parim toimimine ka digivahendeid kasutades. Töötajad ise aga näevad tööandjat kui ühte nurgakivi oma küberhügieeni alaste oskuste parendamisel. Magistritööga seotud eesmärgid seega täideti.

Antud magistritöö tulemusi saab kasutada järgmise Küberkaitse julgeoleku strateegia loomise toetuseks, et motiveerida Eestis astuma samme tegelemaks töötajate küberhügieeniga. Samuti saab magistritöö abil tõuke tööandja, kelle abi töötajad vajavad, et olla turvalisem. Magistritöö tegemine näitas, et oleks vaja uurida, millist e-keskkonda ja materjale, kui ka koolitusi vajaksid töötajad küberhügieeni vallas.

Kasutatud kirjandus

[1] Majandus- ja Kommunikatsiooniministeerium, „Küberjulgeoleku strateegia 2014-2017,“ 2014.

[2] B. Lorenz, „A digital safety model for understanding teenager internet user's concerns,“ Tallinn, 2017.

[3] European Commission, „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,“ Brussels, 2013.

[4] „IMD WORLD DIGITAL COMPETITIVENESS RANKING 2017,“ IMD WORLD COMPETITIVENESS CENTER, 2017.

[5] R. Dunham, „Linford & Company, LLP,“ 2017. [Võrgumaterjal]. Available: https://linfordco.com/blog/how-is-your-cyber-hygiene/.

[6] T. Laeks, „Forte,“ 19 November 2016. [Võrgumaterjal]. Available: http://forte.delfi.ee/news/militaaria/kuberhugieen-uue-aja-moiste-millest-algab-pihta-riigi-sojaline-julgeolek?id=76260859.

[7] „Start IT,“ Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, 2018. [Võrgumaterjal]. Available: https://startit.ee/mida-tahendab-kuberhugieen/.

[8] J. Gridin, „ByteLife,“ 2016. [Võrgumaterjal]. Available: http://www.bytelife.com/blog/turvalisus-kuber-kuberturvalisus/.

[9] E. Commission, 19 October 2017. [Võrgumaterjal]. Available: https://ec.europa.eu/epale/en/resource-centre/content/digital-skills-gap-europe.

[10] „Irish Tech News,“ 21 January 2018. [Võrgumaterjal]. Available: https://irishtechnews.ie/near-half-of-european-adults-lack-basic-digital-skills-says-eu-commission/.

[11] „Government Computing:,“ 15 September 2017. [Võrgumaterjal]. Available: http://central-government.governmentcomputing.com/news/eu-security-chief-europe-faces-a-cyber-security-skills-gap-5927303.

[12] K. Emor, „Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring,“ 2017.

[13] Haridus- ja Teadusministeerium, „Täiskasvanute oskused, nende kasutamine ja kasulikkus Eestis. PIAAC uuringu temaatiliste aruannete kokkuvõtted,“ Haridus- ja Teadusministeerium, Tartu, 2015.

[14] Tööjõuvajaduse seire- ja prognoosisüsteem OSKA, „Eesti tööturg täna ja homme. Ülevaade Eesti tööturu olukorrast, tööjõuvajadusest ning sellest tulenevast koolitusvajadusest,“ Tallinn, 2017.

[15] „Manpower OÜ,“ 2018. [Võrgumaterjal]. Available: http://humanage.manpower.ee/uuring-suhtlemisoskusega-spetsialist-tooturul-defitsiit/.

[16] „tark.ee,“ 2018. [Võrgumaterjal]. Available: https://www.tark.ee/category/koolitused/arvutiope-it-koolitus?post_type=training.

[17] „Haridus- ja Teadusministeerium,“ 2018. [Võrgumaterjal]. Available: https://www.hm.ee/et/tegevused/taiskasvanuharidus/tasuta-kursused.

[18] „Targalt internetis,“ 2018. [Võrgumaterjal]. Available: http://www.targaltinternetis.ee/.

[19] „Vaata maailma SA,“ 2018. [Võrgumaterjal]. Available: http://www.vaatamaailma.ee/projektid/ole-kaasas.

[20] „Riigi Infosüsteemide Amet,“ 2018. [Võrgumaterjal]. Available: https://blog.ria.ee/.

[21] „Tööelu,“ 2017. [Võrgumaterjal]. Available: https://www.tooelu.ee/et/tootajale/Toosuhted/tooleping/lepingueelsed-labiraakimised/Tootaja-koolitusvoimalused.

[22] „etis.ee,“ 2009. [Võrgumaterjal]. Available: https://www.etis.ee/Portal/Projects/Display/63979485-4b2b-408b-b8da-b566549abc53?tabId=tab_GeneralData.

[23] T. V. M. L. K. T. Hans Põldaru, „Web-based self- and peer-assessment of teacher's digital competencies,“ 2012.

[24] V. Riina, P. Yves, C. G. Stephanie ja V. D. B. Godelieve, „DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model.,“ Publications Office of the European Union, 2016.

[25] C. G. Stephanie, V. Riina ja P. Yves, „DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use,“ Publications Office of the European Union, 2017.

[26] Hariduse Infotehnoloogia Sihtasutus, „Õppijate digipädevuse mudel,“ 2016.

[27] „Haridus- ja teadusministeerium,“ 2018. [Võrgumaterjal]. Available: https://www.hm.ee/et/uudised/tana-algav-tasemetoo-annab-voimaluse-esmakordselt-moota-opilaste-digioskusi.

[28] „European Commission,“ 10 May 2017. [Võrgumaterjal]. Available: https://ec.europa.eu/jrc/en/digcomp.

[29] O. Pickup, 7 December 2017. [Võrgumaterjal]. Available: https://www.telegraph.co.uk/money/criminal-activities/how-to-maintain-good-cyber-hygiene/.

[30] „Arvutikaitse,“ 2018. [Võrgumaterjal]. Available: http://www.arvutikaitse.ee/arvutikaitse-algtoed/.

[31] H. Lõugas, „geenius.ee,“ 2018. [Võrgumaterjal]. Available: https://geenius.ee/uudis/215-000-eesti-kasutaja-parooliga-andmebaas-on-nuud-netis-avaldatud-ja-otsitav/.

[32] A. K. K. K. Birgy Lorenz, „“The Four Most-Used Passwords Are Love, Sex, Secret, and God”: Password Security and Training in Different User Groups,“ 2013.

[33] T. S. Y. A. Shukoa yadav, „Cyber crime and security,“ International Journal of Scientific & Engineering Research, 2013.

[34] C. M. &. J. M. Reep-van den Bergh, „Victims of cybercrime in Europe: a review of victim surveys,“ 2017.

[35] 2017. [Võrgumaterjal]. Available: https://www.internetworldstats.com/stats.htm.

[36] Ponemon Institute LLC, Accenture, „Cost of Cyber Crime Study,“ 2017.

[37] Riigi Infosüsteemide Amet, „Küberturvalisus 2018,“ 2018.

[38] EUIPO, EUROPOL, „2017 aasta olukorraaruanne - võltsimine ja piraatlus Euroopa Liidus,“ 2017.

[39] 2012. [Võrgumaterjal]. Available: https://www.aripaev.ee/uudised/2012/04/26/piraattarkvara-tekitab-aastas-eestile-18-miljonit-eurot-kahju.

[40] A. Johns, „The Intellectual Property Wars from Gutenberg to Gates," Chicago University Press, Chicago, 2019.

[41] R. B.-F. Shoshana Altschuller, „Is Music Downloading The New Prohibition? What students reveal through an ethical dilemma," Ethics and Information Technology, 2009.

[42] J. Kennedy, „THE RECORDING INDUSTRY 2006 PIRACY REPORT," IFPI, 2006.

[43] „TechoPedia," 2018. [Võrgumaterjal]. Available: https://www.techopedia.com/definition/4386/warez.

[44] A. Teder, „Eesti noorte hoiakud internetipiraatluse suhtes," Tartu, 2009.

[45] R. M. Siegfried, „Student Attitudes on Software Piracy and Related Issues of Computer Ethics," 2005.

[46] Riigikogu, „Riigiteataja," 2017. [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/116062017008?leiaKehtiv.

[47] „fossbytes," 29 May 2017. [Võrgumaterjal]. Available: https://fossbytes.com/10-reasons-why-people-do-piracy-and-download-movies-shows-albums-software/.

[48] „Forte," 14 April 2016. [Võrgumaterjal]. Available: http://forte.delfi.ee/news/tarkvara/mis-on-lunavara-ja-kuidas-valtida-arvuti-pantvangi-sattumist?id=74235995.

[49] „Varonis," 2016. [Võrgumaterjal]. Available: https://blog.varonis.com/a-brief-history-of-ransomware/.

[50] „Barkly," June 2017. [Võrgumaterjal]. Available: https://blog.barkly.com/ransomware-statistics-2017.

[51] The Proofpoint, „Quarterly treat report Q1 2017," The Proofpoint, 2017.

[52] Riigi Infosüsteemide Amet, „RIIGI INFOSÜSTEEMI AMETI KÜBERTURVALISUSE TEENISTUSE 2015. AASTA KOKKUVÕTE," Riigi Infosüsteemide Amet, 2016.

[53] Riigi Infosüsteemide Amet, „RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE VEEBRUAR 2016," Riigi Infosüsteemide Amet, 2016.

[54] „Riigi Infosüsteemide Amet," 2017. [Võrgumaterjal]. Available: https://blog.ria.ee/tag/lunavara/.

[55] „Statista," 2017. [Võrgumaterjal]. Available: https://www.statista.com/topics/4136/ransomware/..

[56] C. Everett, „Ransomware: to pay or not to pay?," Computer Fraud & Security, 2016.

[57] „Riigi Infosüsteemide Amet," 2016. [Võrgumaterjal]. Available: https://blog.ria.ee/lunavarajuhtumi-ennetamine/.

[58] M. Uus, „Kvantitatiivsed ja kvalitatiivsed meetodid probleemi kirjeldamiseks ning põhjuste tuvastamiseks," 2007.

[59] 2016. [Võrgumaterjal]. Available: https://www.tlu.ee/~sirvir/Intervjuu_vaatlus_ja_sisuanals/intervjuu_liigid.html.

[60] „Küberpähkel,“ 2018. [Võrgumaterjal]. Available: https://kyberpahkel.c-lab.ee/?page_id=154.

Lisa 1 – Küberpähkel uuring-test

Taustaküsimused

Teie sugu

Valige üks järgnevatest vastustest

Palun valige ainult üks järgnevatest:

mees

naine

Millisesse vanusegruppi kuulute?

Valige üks järgnevatest vastustest

10-15 aastased

16-20

21-25

26-30

31-35

36-40

41-45

46-50

51-55

56-60

61-65

66-70

70 ja vanemad

Hõivatus

Märkige palun kõik, mis sobivad

Ei õpi/ei tööta
Töötate
Õpilane põhikoolis
Õpilane gümnaasiumis
Õpilane/üliõpilane kutsekoolis
Üliõpilane rakenduskõrghariduses
Üliõpilane bakalaureuse astmel
Üliõpilane magistrantuuri astmel
Üliõpilane doktorantuuris
Üliõpilane või õpilane IT-ga seotud erialal
Üliõpilane Küberkaitsega seotud erialal

Milline on Teie tänaseks omandatud kõrgeim haridustase?
Vastake sellele ainult siis, kui järgmised tingimused on täidetud:
Vastus oli 'Üliõpilane või õpilane IT-ga seotud erialal' või 'Üliõpilane Küberkaitsega seotud erialal' või 'Üliõpilane doktorantuuris' või'Üliõpilane magistrantuuri astmel' või 'Üliõpilane bakalaureuse astmel' või 'Üliõpilanerakenduskõrghariduses' või 'Õpilane/üliõpilane kutsekoolis' või 'Töötate' või 'Ei õpi/ei tööta' küsimuse juures '5 [B5]' (Hõivatus)
Palun valige ainult üks järgnevatest:

Alghariduseta
Algharidus (1.-6. klassi)
Põhiharidus (8/9. klassi)
Kutsekeskharidus põhihariduse baasil
Keskharidus (10/12. klassi)
Kõrgharidus
Keskeri-, tehnikumiharidus
Bakalaureus või sellega võrdsustatud
Magister või sellega võrdsustatud
Doktor või sellega võrdsustatud

Täpsustus: millises valdkonnas töötate?

Vastake sellele ainult siis, kui järgmised tingimused on täidetud: Vastus oli küsimuse juures '5 [B5]' (Hõivatus)

Palun valige ainult üks järgnevatest:

Administratiivtöö
IT
Koolitus/Personalitöö
Meedia
Teenindus
Turundus/Reklaam
Õigusteenused
Finants/Raamatupidamine
Juhtimine
Riik- ja avalik haldus
Haridus/Teadus
Muu valdkond

Neli autori lisatud küsimust

Milliseks hindate oma digitaalseid ja küberhügieeni alaseid oskuseid täna?

Palun valige kõige sobivaim vastus: 1 - puuduvad 2 3 4 5 - väga head/õpetate teisi

Teabe haldamine sh. kriitiline sisuanalüüs
Suhtlemine digikeskkonnas sh. otsesuhtlus
Sisuloome sh. programmeerimine
Probleemilahendus digivahenditega ja – keskkondades
Seadme kaitsmine (rakendate ohutuse ja turvameetmeid)
Isikuandmete kaitsmine (privaatsus, veebipettused)
Tervise kaitsmine (väldite tehnoloogia kasutusest tulenevaid terviseriske)
Keskkonna kaitse (teadvustate digitehnoloogia mõju keskkonnale)

Millistest kohtadest olete saanud digitaalse ohutuse/küberhügieeni alaste oskuste parandamiseks teavet, koolitust?

Palun valige kõige sobivaim vastus: ei ole saanud üldse; olen saanud vähe;olen saanud palju

Kool/Koolitus
Tööandja
Raadio/ TV/ paberleht
Meedia internetis (onlain-lehed)
Teenusepakkujad (internet, mobiil, pank vms) õpetavad
Erinevad keskkonnad ise õpetavad (abitekstid)
Abilehed (Lasteabi, Targalt Internetis, Veebikonstaabel)
Teised inimesed (päriselus)
Sotsiaalmeedias jagatakse
Vaba Internet, erinevad veebilehed

Millisest kohast sooviksite saada abi oma digitaalse ohutuse/küberhügieeni alaste oskuste tõstmiseks?
Vastusevarjandid: Ei, Pigem Ei, Pigem Jah, Jah

Kool/Tööandja
Raadio/TV/paberleht
Meedia internetis (online lehed)
Teenusepakkujad - interneti teenusepakkuja
Teenusepakkujad - mobiilside teenuse pakkuja
Teenusepakkujad – pangad
Erinevad keskkonnad ise õpetavad (abitekstid)
Abilehed (Lasteabi või Targalt Internetis)
Kaitseliit (küberkaitse üksus)
Veebikonstaabel
Erikoolitus riigi poolt (videod, tekstid ja testid)
Tasuta online kursused

Eestile oleks vaja küberhügieeni alaste oskuste kasvatamiseks ühiskonnas...

Vastusevarjandid: Ei, Pigem Ei, Pigem Jah, Jah

Enam seaduseid, mis reguleerivad digivaldkonda
Teenusepakkujatele seada enam vastutust toodete ja teenuste turvalisuse osas
Enam koolitusi õpilastele
Enam koolitusi kõikidele üliõpilastele (ülikool/kutsekool)
Enam koolitusi IT valdkonna üliõpilastele (ülikool/kutsekool)
Enam koolitusi täiskasvanutele
Tööandja poolne koolitus ja kontroll
Ekspertide gruppi, kes aitab otsustada, kuidas väljakutsed lahendada
Enam veebikonstaableid, kes aitavad inimestel väljakutseid lahendada
Kogukonnale anda enam vastutust ja usaldust väljakutsete lahendamises

Näidisolukorrad

Sõbra arvuti on nakatunud lunavaraga. Varukoopiat arvutis olevatest failidest pole. On vaja kätte saada vajalikud failid. Failide avamise eest küsitakse 100 eurot, 7 päeva pärast tõuseb hind 200 euro peale. Mida soovitate sõbrale?
Vastusevarjandid: Ei, Pigem Ei, Pigem Jah, Jah

Maksta nõutud summa
Viivitada ja loota, et hiljem tuleb maksta vähem
Palgata häkkeri, kes avaks failid
Asuda läbi rääkima ja tingida hinda alla
Kaevata veebikonstaablile/politsei
Püüda kurikaelad üle kavaldada, lubades saata sama viiruse 10nele sõbrale edasi, kui failid avatakse
Mitte midagi teha
Arvuti ära visata ja eluga edasi minna
Otsida üles, kes see kratt on ja teda ise hakata muude viirustega pommitama
Midagi muud

Prantsusmaal blokeeritakse kasutaja internetti ligipääs, kui avastatakse, et ta laadib alla piraatfilme (peale kolmandat vahelejäämist). Mida Te arvate sellest?
Vastusevarjandid: Ei, Pigem Ei, Pigem Jah, Jah

See peabki nii olema - hea mõte!
Piraatfailide allalaadimist peaks lubama erijuhtudel
Sellist asja ei tohiks olla - halb mõte!
Midagi ei arva
Prantsusmaal võib see nii olla, aga Eestis mitte

Lisa 2 – Intervjuu küsimused

Küberhügieen

1. Kirjeldage enda kogemust tehnikaga?
2. Kirjeldage, mida tähendab Teie jaoks küberhügieen?
3. Kui pädevaks peate end küberhügieeni valdkonnas viie palli süsteemis, kus 1 on üldse mitte ja 5 on väga pädevaks?
4. Kuidas tunnete end arvuti kasutamisel?
5. Kellelt küsite enamasti abi juhul, kui peaks olema vaja lahendada mõni tehnilisem küsimus?
6. Millist infot ja kus kohast küberhügieeni kohta üldiselt saate?
7. Nimeta TOP kolm teemat, mille kohta viimasel ajal kõige sagedamini infot on küberhügieenialaselt jagatud?
8. Kus soovite saada antud infot?

Küberkuriteod

1. Nimeta, milliseid küberkuritegusid tead?
2. Milline on tõenäosus, et Teie mõnega kokku puutute, kas siis enda töö- või koduarvutis?
3. Piraatlus – mis arvate, kas Teie ettevõtte programmid on legaalsed? Kuidas on olukord kodus?
4. Mis on Teie arvates piraatluse kõige suuremad probleemid?
5. Lunavara – kas lunavarast on Eesti ühiskonnas piisavalt räägitud?
6. Juhul kui keegi ütleb sõna lunavara, siis mis see on? Kirjelda oma sõnadega.

7. Kas Teie või Teie tuttavatest keegi on kokku puutunud lunavaraga? Juhul kui jah, mida ette võeti?

8. Kujutage ette olukorda, et Teie sõber (töökaaslane) kurdab, et tema arvutis on lunavara ja ta ei saa enam failidele ligi. Mida soovitate?

9. Juhul kui Teie ettevõttes peaks juhtuma lunavara intsident, siis kuidas peaksite tegutsema? A: Kas ettevõte on kõiki töötajaid informeerinud, et juhul kui selline asi juhtub, siis tuleks käituda järgmiselt? B: Juhul kui ei ole, kuidas käitute? C: Mida sooviksite, et Teie ettevõte vastava teema kohta räägiks oma töötajatele?

Töökeskkond

1. Kas ja milliseid reegleid on teada Teie valdkonna ettevõtete raames?

2. Palun loetlege, millised on kriitilised andmed, millega Teie valdkonna töötajad kokku puutuvad?

Tööarvuti/nutiseadme kasutamine Teie valdkonna ettevõtte töötajatel.

SEADMED/INSTALL/VÕRK

3. Mis arvate, milliseid regulatsioone on Teie valdkonna ettevõttel tarvis töötajatele selgitada?

4. Mis arvate, kas Teie valdkonna ettevõttel on lubatud mälupulga kasutamine?

5. Mis arvate, milline on Teie valdkonna ettevõtte töötajal arvutis või nutiseadmes olev viirusetõrje programm?

6. Kuidas Teie valdkonna ettevõtte töötaja saab enda arvutisse tööks vajaliku programmi?

7. Juhul kui tööarvutisse on vaja X programmi. Kas ja kuidas Teie valdkonna töötaja selle endale, saaks kui saaks?

8. Kirjelda palun olukorda töökoha WIFIga. Kas Teie valdkonna ettevõte peamiselt kasutab parooliga WIFIt ja kuidas on reguleeritud isiklike seadmete ühendamine WIFIga?

TEGEVUSED

9. Mis arvate, kui levinud on Teie valdkonna ettevõttes tööarvutile seatud regulatsioonid, mis keelas tööarvutis teha isiklikku elu või meelelahutust puudutavaid operatsioone?

10. Juhul kui oleks, siis mis sa arvad, kuidas sellest regulatsioonist kinni peetakse? Nt kui lehekülgesid ei ole IT poole poolt suletud.

E-MAIL

11. Kas Teie valdkonna ettevõtte töötajale saadetud kiri on kohustuslik avada, sh manus?

12. Kuidas käitute, kui tegemist on kahtlase kirjaga ja on alust arvata, et tegemist on andmekaevega?

13. Mis arvate, kas Teie valdkonna töötajatel on kunagi juhtunud, et kasutavad isiklikku e-maili/sotsiaalmeediat tööasjade saatmiseks?

14. Juhul kui inimene alustab tööd finantsvaldkonnas, siis kas ja kuidas üldiselt on töölepingus kirjas, et töötaja kirjavahetust võidakse jälgida?

PILV

15. Mida arvate, kas Teie valdkonna ettevõtted kasutavad pilveteenuseid ja millised peaksid olema reeglid juhul kui jah?

16. Mis arvate, kas on lubatud Teie valdkonna töötajatel tööasjade lisamine isiklikku pilve?

ÜHISKASUTUS

17. Kas töötajate tööarvutit võivad kasutada ka teised kolleegid?

18. Juhul kui tööarvuti on lubatud koju kaasa võtta, kas Teie valdkonna töötajatel võib juhtuda, et tööarvutit kasutavad pereliikmed (laps, elukaaslane)?

19. Milliseid koolitusi Teie valdkonna ettevõtte teeb/on teinud? (millest rääkinud, kas infotunnid, e-kirja teel pigem jms)

20. Kas soovite veel midagi lisada antud teemade kohta?