TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND

NARVA KOLLEDŽ
ÕPPEKAVA „ETTEVÕTLUS JA DIGILAHENDUSED''

Valeri Jakovlev

KÜBERPETTUSTE ALANE TEADLIKKUS PANGATEENUSTE VALDKONNAS IDA-VIRUMAA EAKATE NÄITEL

Lõputöö

Juhendaja: lektor Jelena Rootamm-Valter

NARVA 2022

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

Valeri Jakovlev
/*allkirjastatud digitaalselt*/
/*kuupäeva vt. digikonteineris*

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Valeri Jakovlev, (sünnikuupäev: 28.05.1992)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Küberpettuste alane teadlikkus pangateenuste valdkonnas Ida-Virumaa eakate elanike näitel'', mille juhendaja on Jelena Rootamm-Valter,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Narvas, **16.05.2022**

SUMMARY

Awareness of cyber fraud in the field of banking services in the example elderly of Ida-Virumaa

Cybersecurity, including banking fraud, has become an important issue in the area of banking services, as it concerns people's assets. Once banking services have moved towards digital channels, fraudsters have also started to operate in new ways, such as investment fraud, fraudulent calls and messages.

The importance of the problem is confirmed by the cybersecurity research campaigns conducted by the Estonian Banking Association that russian-speaking elderly are the most vulnerable to banking and investment fraud.

The goal of the thesis is identified awareness of cyber-fraud among Russian-speaking people in Ida-Virumaa and propose ways to better protect them from cyber-fraud.

In the theoretical part of the work, the author looks at the nature of cyber threats and cybersecurity and the factors influencing cybersecurity awareness among older people. Shows the main types of cyber-fraud that are most common today. Explains the psychological methods of cyber-fraud and the determinants of cybersecurity awareness among older people.

To perform an empirical part of the study, the author first characterizes the cyber-fraud environment in Ida-Virumaa. In conducting the study, the author uses a qualitative method of research and data collection through semi-structured interviews focusing on russian-speaking elderly people in Ida-Virumaa, who suffered financial losses due to cybercrime between 2020 and 2022. Interviews will take place during the period 07. - 27 March 2022 with six participants.

The study revealed that fraudsters successfully exploit social manipulation techniques through telephone calls, using the vulnerability of older people and, in most cases of fraud, cybercrime presented themselves as banking employees. Older people rely on their close people to understand cybersecurity or cyber threats and make decisions, listen to their recommendations. Based on the results of the study, the author proposed recommendations on the need to develop and provide cybersecurity training and

information programmes. Banks may be advised to change the customer service model and reduce own-initiative telephone inquiries to customers, for example by asking customers to contact the bank itself by telephone if necessary on the bank's public telephone number. This increases the workload of bank staff, but may justify itself by increasing the credibility of the banks.

The study revealed that older people have good digital skills, but fear technical failures in the use of digital devices and the level of cyber hygiene of devices are rather low, because they communicate personal and confidential data to fraudsters and provide access to their devices. Based on the results of the study, the author suggested recommendations to raise the technical awareness of older people. Banks could be encouraged to develop a technical solution for their mobile app, which could filter calls received from fraudsters by telephone number. In this way, deceptive calls do not reach subscribers.

The study reveled that older people most tend to psychological manipulation from fraudsters and most them need psychological assistance after having been in contact with fraudsters and preferred to stop using digital devices on a daily basis. Based on the results of the study, the author proposed recommendations to develop cyber-fraud victim support programmes involving trained professionals to provide assistance to people who are victims of cyber-fraud.

The author of the work finds that the recommendations suggested as a result of the study will help better protect among russian-speaking them from cyber-fraud.

SISUKORD

SISSEJUHATUS

Küberturvalisus, sealhulgas panganduspettused, on muutunud oluliseks teemaks pangandusteenuste valdkonnas, sest see puudutab inimeste vara. Kui aastaid tagasi oli üks peamisi pettuse liike raha võltsimine, siis nüüd, mil pangandus on liikunud digitaalsete kanalite suunas, on ka petturid hakanud tegutsema uutel viisidel, nagu investeerimispettused, petukõned ja- sõnumid. See on aktuaalne probleem ka Eestis, kus elanike digioskused on teadaolevalt teiste riikidega võrreldes paremad.

Viimastel aastatel on märkimisväärselt kasvanud digitaalteenuste kasutamine pangandussektoris, eriti eakate inimeste seas, kes hakkasid uute tehnoloogiate ja nende teenuste kättesaadavuse tõttu rohkem huvi kasutamise vastu tundma.

Eesti Pangaliit koordineerib pankade ühiste probleemide lahendamist ning teeb pidevalt tööd küberturvalisuse suurendamiseks. Alates 2021. aastast korraldas küberturvalisuse sotsiaalseid infokampaaniaid, et vältida küberpettusi, ning mille üheks eesmärgiks on toetada ja tõhustada inimeste informeeritust ning teadlikkust küberkuritegevuse teemadest. Küberturvalisuse infokampaaniad on suunatud eelkõige eakatele Eesti elanikele, kelle emakeeleks on vene keel. Nemad on pangandus- ja investeerimispettuste suhtes kõige haavatavamad ja vähem informeeritud pettuste ulatusest ning sellest, milline oleks õige käitumine, kui probleemid küberpettustega on ilmnenud.

Lõputöö eesmärk on teha kindlaks küberpettuste alane teadlikkus Ida-Virumaa vene keelt kõnelevate eakate seas ning teha ettepanekuid, kuidas neid paremini kaitsta küberpettuste eest.

Eesmärgi saavutamiseks püstitati järgmised uurimisülesanded:

- määratleda küberohtude mõiste ja peamised riskid,
- määratleda küberturvalisuse mõiste ja olemus,
- määratleda küberpettuste liigid,
- määratleda küberpettuste psühholoogilised meetodid ja mõjumehhanismid,
- määratleda eakate inimeste küberturvalisuse alast teadlikkust mõjutavad tegurid,
- iseloomustada Ida-Virumaa elanike küberturvalisuse keskkonda pangandusteenuste valdkonnas,
- valida meetodid Ida-Virumaa eakate küberpettuste alase teadlikkuse uurimiseks pangandusteenuste valdkonnas,
- koguda ja analüüsida andmed,

- teha järeldused ja töötada välja ettepanekud, kuidas on võimalik täiustada eakate küberpettuse valdkonna alaseid teadmisi ja paremini kaitsta neid küberpettuste eest.

Lõputöö teoreetilises osas määratleb autor küberohtude ja küberturvalisuse olemust ning nende omavahelist seost. Tuuakse välja peamised ja tänapäeval kõige levinumad küberpettuste liigid. Teoreetilises osas on samuti selgitatakse küberpettuste psühholoogilisi manipuleerimisründe meetodeid ja mõjutamismehhanisme ning küberturvalisuse alast teadlikkust mõjutavaid tegureid eakate hulgas. Teoreetiline käsitlus tugineb paljude autorite seisukohtadele ja uuringutele kellest peamised on Leonov, Chang, Zakira, Wang ja Washo.

Lõputöö rakenduslikus osas töö autor iseloomustab kõigepealt Ida-Virumaa küberpettuste keskkonna olulisust tuginedes Politsei ja Piirivalveameti, Justiitministeeriumi ja Kaitsepolitsei aastaraamatute 2020-2021 andmetele ja Eesti Pangaliidu küberturvalisuse infokampaania uuringutele.

Uuringu läbiviimisel kasutab autor kvalitatiivset uurimisviisi ning tegemist on juhtumiuuringuga. Andmete kogumiseks töö autor kasutab poolstruktureeritud intervjuud avatud küsimustega. Intervjuud keskenduvad küberturvalisuste ja küberpettuste kogemustele ning digitaalsete oskuste kasutamisele igapäevaelus, seahulgas käitumisele pettuse korral. Intervjuude salvestused transkribeeritakse ning salvestatakse vastused tekstina arvuti abil. Kogutud andmed grupeeritakse ning analüüsitakse kvalitatiivse sisuanalüüsi meetodiga.

Autor viib läbi ekspertintervjuu Eesti Pangaliidu esindajaga ning kasutatab kogumi moodustamisel nende küberturvalisuse infokampaania uuringu andmeid. Autor kasutab mugavusvalimi meetodid intervjuus osalejate valiku tegemisel.Valimisse kuulub kuus inimest, kes oli valitud kindlate tunnuste kohaselt. Intervjuud toimuvad ajavahemikul 07. - 27. märts 2022.

Lõputöö raames läbi viidud uuringu tulemuste, järelduste ja teoreetiliste seisukohtade põhjal töötab autor välja ettepanekud, kuidas on võimalik täiustada eakate küberpettuse valdkonna alaseid teadmisi ja paremini neid kaitsta küberpettuste eest.

Lõputöö koosneb inglisekeelsest resümeest, sissejuhatusest, kahest peatükist, kokkuvõttest, kirjanduse loetelust ning lisadest.

1. TEOREETILISED SEISUKOHAD KÜBERPETTUSTE ALASE TEADLIKKUSE ARENDAMISEKS

1.1 Küberohtude olemus ja riskid

Tänapäeva digitaaltehnoloogia kiire areng ja laialdane kasutamine on seotud küberohtude kiire kasvuga. Küberoht tähendab iga võimalikku tahtlikku rünnakut, mis on suunatud ebaseaduslike andmete kasutamisele, digitaalsete operatsioonide rikkumisele või teabe kahjustamisele.

Zakira ja Zainal (2019: 1) on seisukohal, et küberohud ja küberrünnakud muutuvad keerulisteks ja hävitavateks ning võivad mõjutada kõiki sektoreid, sealhulgas valitsust. Seetõttu on küberjulgeolek jätkuvalt esmatähtis igas suuruses organisatsioonis, kõigi tööstusharude jaoks. Piiratud ja väga üldised teadmised erinevate küberrünnakute tüüpide, ohtude ja võimalike mõjude kohta, mis võivad takistada julgeoleku kaitsmist.

Küberohtude kasvu põhjustavad mitmed tegurid, mis võivad olla seotud nende sageduse ja ulatuse suurenemisega. Üks tegur on motivatsioon küberrünnakute läbiviimiseks, ehk rahalise kasu, luureandmete ja intellektuaalse omandi saamine. Teine tegur on see, et tehnoloogia maksumus langeb, küberkuritegevuse tõkked langevad, muutes igasuguste kurjategijate jaoks lihtsamaks ja odavamaks leida uusi viise küberkuritegevuse toimepanemiseks. (Bayard 2019: 70)

Küberkuritegevuse olemus on selline, et praegu puudub tehniline suutlikkus määrata tegevusi eraisikutele, rühmadele või organisatsioonidele kõrge usalduse tasemega. Peamised küberruumi ohud on järgmised: välisriskid, siseriskid, ohud kaupade ja teenuste tarneahelas ning ohud, mis tulenevad kohalike jõudude ebapiisavast operatsioonivõimest. (Liu, Li 2021: 8177)

Sajal, Jahan jt (2019: 525) arvavad, et küberrünnakute olemus kaasaegses ühiskonnas on määratletud kui pahatahtlik katse kahjustada või häirida arvutivõrku või süsteemi. Viimasel ajal ei piirdu küberoht konkreetse sektoriga.

Peamised levinumad küberohud on (Halouzka, Burita jt 2021):

- kurivara ehk ründetarkvara (ingl. k *malware*), mis püüab krüpteerida inimese andmeid ja siis lunaraha küsida, et anda välja lukukood. Selliseid programme toimetatakse peamiselt e-posti või rämpsposti teel;

- andmepüük ehk kalastamisrünne (ingl. k. *phishing*) tähendab, et pettuslikud e-mailid saadetakse e-posti, SMS-sõnumi või sotsiaalmeediale sõnumina, milles ründaja püüab veenda ohvrit avaldama tundlikku teavet, avama linki pahatahtlikule veebilehele või avama faili, mis sisaldab pahatahtlikku koodi.

Autori arvates kasvab ja moderniseeritakse jätkuvalt küberrünnakute ja -ohtude tüüpide arvu, võttes arvesse tänapäeva ühiskonna tehnoloogilist kasvu ja digiteerimist. Küberkuritegijad keskenduvad jätkuvalt rünnakutele finantsettevõtete vastu, samuti organisatsioonidele, mis on väga sõltuvad nende digiteenuste kättesaadavusest.

Bobrici arvates (2020:19) võib küberruumi peamisi ohuagente kirjeldada üksustena, kes teevad oma kasuks vaenulikke tegusid, et saada isiklikkult füüsilist või psühholoogilist kasu, nagu küberkurjategijad, insiderid, riigid, korporatsioonid, haktivistid ja terroristid. Wainwright ja Kettan arvavad (2019: 176), et ründevektorid on tee või vahendid, millega ohuagent saab juurdepääsu arvutile või võrgule pahatahtlikuks tegevuseks. Ründevektoritel on suur taksonoomia. Lühike nimekiri sisaldab inimelemente, veebi- ja brauserirünnakuid, internetiohtu, mobiilirakenduste e-poode ja USB mälupulki.

Organiseeritud ja informatiivne kuritegevus on tihedalt seotud, koosneb küberrünnakutest inimeste või finantssektori vastu, infopettustest, nagu ebaseaduslikud oksjonid või kasutaja pangakontode kahjustamine elektroonilise kaubanduse veebisaitidel, ning krediitkaarte kasutavatest pettustest, kahjustades pangaautomaate ja varastades andmeid pangakaartidelt. (Bobric 2020: 20)

Tehnoloogia areneb ja infrastruktuuri hajutaneb, uued valdkonnad, rakendused, tehnoloogia ja infrastruktuur kasvavad, pakutavate teenuste kvaliteet paraneb, elu muutub lihtsamaks ja eelkõige kiireneb töö ja tehingud. Kiired muutused ja transformatsioonid on tihedalt seotud uute küberohtude, häirete ja haavatavuse vormide tekkega. (Arslan, Sağıroğlu 2019: 240)

Esitatud seisukohad näitavad, et küberoht on tänapäeval suur oht mitte ainult avalikule ja erasektorile, vaid ka tavakodanikele, sest see areneb pidevalt tehnoloogiliselt progressiivses ühiskonnas. Järgmises alapeatükis käsitletakse küberturvalisuse mõistet ja olemust, mis on seotud küberohude valdkonna kiire arenguga.

1.2 Küberturvalisuse mõiste ja olemus

Küberturvalisuse suurendamine on viimasel ajal üks kõige aktuaalsemaid teemasid, sest uute tehnoloogiate kasutuselevõtt ja kiiresti muutuv digitaalsektor on aidanud kaasa

küberkuritegevuse arengule. Küberkuritegevuse valdkonna analüütikud ja teoreetikud arvavad, et Interneti populaarsuse suurenemise tõttu on sellest saanud üksikisikute, organisatsioonide ja riikide probleem, sest teatised häkkimiste, andmevarguste, süsteemikulude, pettuste ja vihkamiskõnede kohta tekitavad hirmu ja muret uute tehnoloogiate pärast, mida praegu nimetatakse küberkuritegudeks (Chang, Coppel 2020).

Mõistel „küberturvalisus“ puudub täpne ja üldiselt kokkulepitud definitsioon. Mihaela arvates (2020: 352) on küberturvalisus üldine termin ennetavate ja reageerivate meetmete jaoks, mis keskenduvad teabe konfidentsiaalsusele, terviklikkusele ja kättesaadavusele, vastupidiselt võimalikele nõrkustele. Küberruum on küberinfrastruktuuri tekitatud virtuaalne ruum, mis hõlmab kogutud, töödeldud või edastatud teabe ulatust. Selles kontekstis on küberkuritegu ilmnenud asjaolu tõttu, et kurjategija kujutab endast või realiseerub teataval finants- ja majanduslikul motivatsioonil teatavat haavatavust või pidevat ohtu kolmandale isikule.

Küberturvalisus võib määratleda ka globaalse nähtusena, mis kujutab endast valitsuste jaoks keerulist sotsiaal-tehnilist väljakutset, kuid nõuab üksikisikute kaasamist. See puudutab ka tähtsamaid probleeme, millega valitsused täna silmitsi seisavad, sest küberturvalisuse nähtavus ja üldsuse teadlikkus on endiselt piiratud. (Janssen, Bruijn 2017)

Eesti digitaalne ökosüsteem on riiklikes määrustes määratletud kriitilise elutähtsa teenusena, mis allub tugevamatele küberturvalisuse riskijuhtimismeetmetele ja oluline valitsemistava toimimise tagamisel (Pernik 2019: 11). Hädaolukorra seaduse § 41 lõike 2 kohaselt on määratletud: „elutähtsa teenuse osutaja peab elutähtsa teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid’’(HOS 2017). Vastavalt Küberturvalisuse seadusele peatükki § 6 lõikele 4 on välja selgitatud koostööpõhimõte: „küberturvalisuse tagamisel ja küberintsidentide lahendamisel teevad osalised koostööd ja võtavad vajaduse korral arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust" (KüTS 2018).

Põhilised elutähtsad teenused - eelkõige kriitilised teenused, nagu finantssüsteem, ettevõtted, transport, energeetika, telekommunikatsioon ja tervishoid - muutuvad riigi ja valitsusväliste osalejate peamisteks küberohtlikeks eesmärkideks (Pernik 2019: 81). Sebai, Harjan jt (2020: 124) jaotavad, et tehnoloogia arengut ja kõiki valdkondi, eriti finantsvaldkondi silmas pidades, kus finantstehnoloogial peaks lähitulevikus olema oluline roll finantsteenuste juhtimises. Kuna finantstehnoloogiad muutuvad tähtsamaks, on vaja tugevamaid

küberturvalisuse mehhanisme. Selle tulemusena ei kaotata finantstehnoloogia eeliseid. See nõuab teatud ettevalmistustaset paljudes valdkondades, sealhulgas küberjuhtimises, nagu Interneti-tehnoloogiate parem mõistmine ja analüüs ning turvafaktid, julgeolekualased partnerlused.

Jansseni ja Bruijni arvates (2017: 1) muutub ühiskond küberfüüsiliseks ühiskonnaks, millel on sõltuvus info- ja kommunikatsioonitehnoloogiast kõigis igapäevaelu aspektides, mis muudab küberjulgeoleku vajaduse väga suureks. Küberturvalisuse immateriaalne iseloom, sotsiaal-tehnilised sõltuvused, mitmetähenduslik mõju ja küberturvalisuse vastase võitluse vaidlustatud iseloom seab selle poliitikakujundajatele väljakutseks. Kübeberturvalisus on võimalik lavastada erineval viisil, millel on inimestele erinev mõju.

Autori arvates on küberturvalisus tänapäeval, kiire tehnoloogilise kasvu tõttu, väga oluline valdkond, mida tuleb arendada, ning samuti tuleb välja töötada meetodid selle parandamiseks riigi sees, suheldes avaliku ja erasektori kui ühise ökosüsteemiga.

Küberturvalisus on suur aspekt, mis muutub üha olulisemaks, sest maailm on muutunud väga seotuks ja võrk on kasutusel isegi põhisidevahendite jaoks. Tänapäeval toob võrgu ulatuslik kasutamine kaasa teatavad riskid ja vahendid, mida küberkurjategijad saavad kasutada oma rünnakutes valitsuste, organisatsioonide või inimeste vastu. (Narmatha 2020) Homburgeri arvates (2019: 225) ei ole riigid mitte ainult oma ideede suhtes, mis käsitlevad käitumise reguleerimist küberruumis, vaid ka nende info- ja kommunikatsioonitehnoloogia arendamise seisundit. Võttes arvesse küberruumi arhitektuuri, vastastikuse seotuse ja sõltuvuse soodustavaid tegevusi, peab igal riigil olema ka võimsust oma võrkude ja süsteemide turvamiseks.

Küberturvalisus ja küberohtud on omavahel seotud, ilma üheta ei saa olla teist - küberturvalisuse teadlikkust ei ole võimalik tõsta ilma küberturvalisuse ohtudest aru saamata. Teadlikkus aitab kaasa küberkultuuri kujunemisele kaasa kaasaegses ühiskonnas. Järgmises alapeatükis käsitletakse küberpettuse peamisi liike, mis mõjutavad teadlikkust kübermaailmast.

1.3 Küberpettuste liigid

Tehnoloogia laialdane kasutamine ei ole ühiskonnale mitte ainult kasu toonud, vaid ka ahvatlenud pettureid ja kurjategijaid kasutama seda rahalise kasu saamiseks. (Ali et al. 2019: 408) Küberpettused arenevad kiiresti ja peamiseks suundumuseks on

sotsiaalmanipuleerimisrünnakud, mis kujutavad tõsist ohtu erinevatele riiklikele infrastruktuuridele, kasutajate andmetele ja küberruumides toimuvale tegevusele.

Mõistet „sotsiaalne manipuleerimisrünne" (ingl. k. *social engineering)* võib arvuti ja küberturvalisuse kontekstis kirjeldada kui küberpettuse liike, kus ründaja kasutab inimlikku haavatavust selliste vahendite abil nagu mõjutamine, veenmine, pettus, manipuleerimine, et saada salajast teavet, häkkida arvutisse või võrku ning saada volitamata juurdepääs kasutajaandmetele. (Wang et al. 2021: 2)

Leonov, Vorobyev jt (2019: 2) arvavad, et sotsiaalne manipuleerimisrünne põhineb isiku, ettevõtte või objekti kohta teabe kogumisel isikliku vestluse teel või e-posti, mobiiltelefoni või muude sidevahendite abil, kus üks osapool annab enda teadmata teavet. Manipuleeritakse inimloomusega, kasutades ära selliseid omadusi nagu ahnus, hirm, kiirustamine ja kergemeelsus, et saada ohvrilt vajalikku teavet või tekitada teatud kahju. (Leonov, Vorobyev et al. 2019: 2)

Tabel 1. Küberpettuste sotsiaalse manepuleerimisründe liigi struktuur

Füüsiline	**Sotsiaalne**	**Tehniline**	**Sotsiotehniline**
Prügis tuhnimine (ingl. k. *dumpsted diving*) Üle õla piilumine (ingl. k. *shoulder surfing*) Sappa võtmine (ingl. k. *tailgating*)	Andmepüük (ingl. k. *phishing*) Andmete kogumine SMS-ide kaudu (ingl. k. *smishing*) Helistamispettus (ingl. k. *vishing*)	Ohmuotsing (ingl. k. *google hacking*) Veebilehtede võltsimine (ingl. k. *pharming*) Pahatahtlik teisik (ingl. k. *evil twin*)	Harpuunimine (ingl. k. *spearphishing*) Vaalapüük (ingl. k. *whaling*) Hirmvara (ingl. k. *scareware*) Ettekääne (ingl. k. *pretexting*)

Allikas: Hijji ja Alam 2021. Autori koostatud.

Tabelil 1 on kujutatud, kuidas autor näeb küberpettuste liigi struktuuri. Küberkurjategijad kasutavad erinevaid pettusemeetodeid, mis sõltuvad sotsiaalse manipuleerimise valitud liigist.

Hijji ja Alam (2021: 6) jaotavad sotsiaalse manipuleerimisründe järgnevatesse liikidesse:

- füüsiline – ründajad teevad mõningaid toiminguid, et koguda teavet ohvri kohta füüsilistest materjalidest;
- sotsiaalne – ründajad kasutavad psühholoogilisi meetodeid, et veenda sihtkasutajat e-posti, tekstisõnumite ja telefonikõnede kaudu;

- tehniline – ründajad kasutavad seda tüüpi üldtuntud sidevõrkudes ja otsingumootorites, et koguda vajalikku teavet ohvrite kohta ning katsetada nii arvamis- kui ka pragunemisparoole, et saada kasutaja kohta lisateavet;
- sotsiotehniline – ründajad võtavad arvesse teatavaid tegureid, nagu ohvri sotsiaalne kultuur, inimkäitumine, kasutatav tehnoloogia ja infrastruktuuri ehitus, samuti eesmärke ja väärtusi, et suurendada eduka küberrünnaku võimalusi.

Autori arvates sunnib digiteerimise kiirus ründajaid kasutama uusi pettusemeetodeid ja võib omistada füüsilisi rünnakuid. Mattera ja Chowdhury (2021: 5) jagavad füüsiliseks rünnakuks need ohud, mis ei kasuta tehnoloogiat ja võivad hõlmata füüsilisi toiminguid, nagu ettevõttesse sisenemine. Järgmises alajaos on esitatud manipuleerimisrünnaku füüsilise liigi määratlus.

Prügis tuhnimine (ingl. k. *dumpster diving*) – üksikisikute või ettevõtete prügi sõelumine, et leida kasutusest kõrvaldatud esemeid, mis sisaldavad tundlikku teavet. (Li et al. 2022: 6) Osa teabest, mida on võimalik esitada, sisaldab paberitükke, millele on märgitud telefoninumbrid või salasõnad, töötajate kodused aadressid, klientide nimekirjad, finantsandmed ja vanad ärikataloogid, ning see teave võib olla mõeldud rünnakuks. (Wokabi 2019)

Sappa võtmine (ingl. k. *tailgating*) – on vahend piiratud alale sisenemiseks, järgides selleks volitatud isikut. (Li et al. 2022: 6) See on tegu, kus ründaja jälitab kedagi, kellel on seaduslik juurdepääs sellele alale ja kes võib paluda ohvril ust hoida või lihtsalt siseneda turvaloaga isiku taga. (Matera, Chowdhury 2021)

Üle õla piilumine (ingl. k. *shoulder surfing*) – on lihtne, kuid tõhus lähenemine, kus sotsiaalmanipuleerimise ründaja jälgib lähedalasuvate ohvrite füüsilist tegevust ning jälgib või kuulab salaja, kuidas konfidentsiaalset teavet räägitakse või trükitakse. (Li et al. 2022: 6)

Autori arvates erinevad sotsiaalsed manipuleerimisrünnakud infoturbe kontekstis selle rakendamise viisist. Peamised manipuleerimisrünnakute liigid on andmepüük (ingl. k. *phishing*), telefonikõnede pettus (ingl. k. *vishing*) ja andmete kogumine SMS-ide kaudu (ingl. k. *SmiShing, SMS phishing*), mis hõlmab erinevaid liike. Järgmises alajaos on esitatud manipuleerimisrünnaku sotsiaalse liigi määratlus.

Andmepüük (ingl. k. *phishing*) on internetipettuse liik, mille puhul ründaja soovib ohvrilt saada näiteks sotsiaalvõrgustike, mobiiltelefonipanga, veebipoodide jms sisselogimisandmeid. (Leonov et al. 2019: 2) See on kõige levinum ja ohtlikum sotsiaalse

manipuleerimisründe liik. Andmepüüdja saadab petusõnumeid, mis tunduvad pärinevat mainekatelt ja usaldusväärsetelt osapooltelt. Ründaja eesmärk on püüda saada ohvritelt isiklikku ja tundlikku teavet. (Asani et al. 2021: 1707)

Huseynovi ja Kösei (2021: 174) toovad välja peamised andmepüügi liigid:

- domeenide võltsimine (ingl. k. *domain spoofing)* – ründajad loovad kasutajate petmiseks pahatahtliku veebisaidi, suhtlevad kasutajatega ja koguvad väärtuslikku teavet selle veebisaidi kaudu;
- e-posti kaudu andmete kogumine (ingl. k. *email phishing*) – küberkurjategijad saadavad meilisõnumeid, mis väidavad end olevat seaduskuulekalt üksuselt, ning püüavad veenda rünnaku all olevaid sihtmärke andma konfidentsiaalset teavet;
- otsingumootori kaudu andmete kogumine (ingl. k. *search engine phishing*) – kuigi veebipõhine otsingumootori platvorm on seaduslik, saavad kasutajad otsida ja külastada küberkurjategijate loodud ebaseaduslikku veebisaiti, mille eesmärk on varastada tundlikku teavet;
- sotsiaalmeedia kaudu andmete kogumine (ingl. k. *social media phishing*) – sotsiaalmeedia platvormide nagu Facebook, Twitter, Pinterest või Instagram abil püüavad küberkurjategijad veenda sotsiaalmeedia kasutajaid külastama pahatahtlikke lehti või postitusi, võltslehti jne.

Andmete kogumine SMS-ide kaudu (ingl. k. *SMS phishing, SmiShing*) on andmepüügi liik, kus ründajad kavatsevad varastada ohvrite isikuandmeid, kasutades neile saadetud SMS-sõnumeid. (Balim, Gunal 2019) Petturid kutsuvad tavaliselt kasutajat üles klõpsama lingil, helistama telefoninumbrile või võtma ühendust ründaja poolt SMS-i teel antud e-posti aadressiga. Sõnumid sarnanevad sageli sõnumitele mobiilipangast, veebipoest või sotsiaalvõrgustikust; küberkurjategijad kasutavad sarnast lausestruktuuri, sõnu ja fraase. (Boukari et al. 2021)

Helistamispettus (ingl. k. *vishing*) – selle andmepüügi liigi sisuks on telefonivestlus, kus ründajad võtavad endale eri rollid ja tutvustavad end pangatöötajatena, potentsiaalsete klientidena või advokaatidena. Nad üritavad saada isiklikku teavet ja infot ohvri krediitkaardi ja pangakontode kohta ning muid isiklikke andmeid. Kättesaadav teave võimaldab ründajal pääseda ligi ohvri isiklikule pangakontole ning varastada rahalisi vahendeid või toime panna pettusi isikuandmetega. (Leonov et al. 2019)

Autori arvates enamik tehnilisi rünnakuid, mida on nähtud tegelikes stsenaariumites, põhinevad esialgsel inimkontaktil. Tehniliselt kasutatakse nippe isikliku ja tundliku teabe, näiteks krediitkaardi PIN-koodide ja registreerimisandmete hankimiseks. Järgmises alajaos on esitatud manipuleerimisrünnaku tehnilise liigi määratlus.

Ohmuotsing (ingl. k. *google hacking*) on teabe kogumise tehnika, mida kasutab ründaja, kes kasutab täiustatud Google'i otsingumeetodeid. Google'i häkkimine võimaldab tuvastada veebirakenduste turvariske, koguda teavet ettevõtte või üksikute sihtmärkide kohta, avastada tõrketeateid, avaldada tundlikku teavet, avastada mandaate sisaldavaid faile ja muid tundlikke andmeid. (Wokabi 2019: 13)

Veebilehtede võltsimine (ingl. k. *pharming*) on vähem levinud andmepüügi liik, kuid rohkem täiustatud ja kaasaegne. Ololade jt (2020: 2014) toovad selle andmepüügi tüübi näiteks ohvri netiliikluse salajase ümbersuunamise teisele IP-aadressile, mille eesmärk on suunata teatud saidi külastajaid samailmelisele võltssaidile, kus nad võivad paljastada oma tundlikku teavet (sisselogimise andmed, paroolid), alla laadida kahjulikku tarkvara või osaleda tahtmatult pettuses.

Pahatahtlik teisik (ingl. k. *evil twin*) on andmete kogumise tehniline tüüp, kus ründaja seab üles WI-FI võrgu sama nimega nagu seal asuv asutus, kes pakub WI-FI-t. Ründaja teeb vajalikud seadistused, et kasutaja ei läheks seaduslikku WI-FI võrku, asendades selle küberkurjategija võrguga, kus ta saab jälgida, mida kasutaja teeb ja kogub paroole, krediitkaardi numbreid ja installeerib viiruseid ka teistesse arvutitesse. (Ahad Ahadi et al. 2021)

Autori arvates sotsiotehnilised võtted on sotsiaalse manipuleerimisründe ühed võimsamad, ühendades nii sotsiaalse kui tehnilise tüübi. See kombinatsioon suurendab eduka küberrünnaku võimalusi ja kõige levinum rünnakuvorm on andmepüük. Järgmises alajaos on esitatud manipuleerimisrünnaku sotsitehnilise liigi määratlus.

Harpuunimine (ingl. k. *spearphishing*) – andmepüügi liik, mis on suunatud konkreetsele inimesele või inimeste rühmale. Selleks teevad ründajad tavaliselt ulatuslikku luuretegevust, uurivad sotsiaalmeediat ja muid allikaid, mis sisaldavad teavet nende kavandatud sihtmärgi kohta, mis suurendab märkimisväärselt edu tõenäosust. Peamine eesmärk on sama: sundida ohvrit minema võltsitud veebilehele ja hankima mandaati või avada konkreetset dokumenti, klõpsates lingil, mis automaatselt installeerib rünnakutarkvara ja selle pahavaraga saavad ründajad manipuleerida kaugelt nakatunud arvutiga. (Leonov et al. 2021: 6)

Vaalapüük (ingl. k. *whaling*) – organisatsioonidele suunatud andmepüügi liik. Ettevõte võib saada näiliselt ohutu e-kirja koos tagasikutsumise või kaebusega töökoha kohta, üleskutse õiguskaitsele või lihtsalt mistahes teabe täpsustamisega, kus linkide või lisandite avamine

võimaldab juurdepääsu mandaadile ja muule isiklikule teabele või käivitab rünnakuvara. (Park, Rayz 2019)

Hirmvara (ingl. k. *scareware*) – on andmepüügi liik, mis paneb ohvrit arvama, et nende arvuti on nakatunud pahavara või viirusega, ning pakub seejärel selle probleemi lahendamiseks tarkvara paigaldamist, mida ründaja saab kasutada täieliku juurdepääsu saamiseks ohvri arvutile ja edasiseks manipuleerimiseks. (Gupta et al. 2021: 1)

Ettekääne (ingl. k. *pretexting*) – on andmepüügi liik, kus ründaja kasutab eelkujundatud stsenaariumi, et legaliseerida oma suhtlus potentsiaalsete ohvritega, vähendada nende kahtlusi ja eksitada neid lõpuks ohtlikule veebilehele sellele klõpsates või alla laadides. Tavaliselt kasutatakse selles stsenaariumis andmete kogumise veenmise põhimõtteid andmete kogumisel ohvri jaoks olulises kontekstis, näiteks kliendiküsitluse e-kirjade koostamisel, milles kasutatakse vastastikkuse põhimõtet. (Sharevski, Jachim 2021: 207)

Autori arvates kaasaegses maailmas on küberpettuse ohvriks võib sattuda igaüks olenemata soost, vanusest ja haridustasemest. Küberpettuste psühholoogilised meetodid on käsitletud töö järgmises alapeatükkis.

1.4 Küberpettuste psühholoogilised meetodid

Küberrünnakud, milles kasutatakse sotsiaalse manipuleerimise liike, on psühholoogilised rünnakud, mis kasutavad ära inimese kognitiivsete funktsioonide nõrkusi. (Montanez at all. 2020: 1) Washo (2021: 1) määratleb sotsiaalse manipuleerimise rünnakut kui pettust, nii et psühholoogilise lähenemise kontseptsiooni mõistmiseks on vaja mõista nii ründaja kui ka ohvri mõtteid ja käitumisviise. (Washo 2021)

Sotsiaalse manipuleerimise meetodid põhinevad inimese otsustusprotsessi teatud atribuutidel, mida nimetatakse kognitiivseteks eelarvamusteks. Need eelarvamused, mida mõnikord nimetatakse „inimeste riistvara vigadeks“, on kõrvalsaadused sellest, kuidas aju kasutab lühikesi lõike andmete kiireks töötlemiseks. (Shermanet et al. 2020)

Norris ja Brookes (2021) defineerivad kognitiivse psühholoogia mudeliks, kus eksitavate sõnumitega silmitsi seistes on inimestel psühholoogilised omadused, nagu kalduvus teha kiireid ja tihti ka valesid otsuseid. Ohvrid ei suuda sageli ära tunda petlikke sõnumeid, mis tuleneb inimese psühholoogilistest teguritest, nagu isiksus, madal enesekontroll,

impulsiivsus ja tunnetusvajadus. See võib kajastada kognitiivseid jõupingutusi, mida nad teevad iga sõnumi töötlemisel. (Norris, Brookes 2021)

Alkis ja Temizel (2015) toovad välja kuus mõjuprintsiipi, millel sotsiaalne manipuleerimisrünne põhineb:

- vastastikkus (ingl. k. *reciprocity*) – inimesed kalduvad vastama üldlevinud tõigale, et nad peaksid aitama neid, kes on neidki varem aidanud;
- pühendumus ja järjepidevus (ingl. k. *commitment and consistency*) – kui inimesed on pühendunud mingile ideele või eesmärgile, siis on tõenäoline, et nad teevad kõik endast oleneva, et olla oma sõnades ja tegudes järjekindlad, sest see vastab nüüd nende kujutlusvõimele;
- sotsiaalne tõestus (ingl. k. *social proof*) – see tähendab kalduvust järgida teiste eeskuju, öelda "jah" inimestele, kes neile meeldivad ja järgida veenvat sõnumit, kui ka teised inimesed on seda järginud;
- võim (ingl. k. *authority*) – inimesed kalduvad alluma seaduslikku autoriteeti esindavate inimeste palvetele, kartes võimalikke karistusi või vastutust;
- meeldivus (ingl. k. *liking*) – see tähendab inimeste kalduvust olla mõjutatud nende poolt, kes neile meeldib;
- puudumise tunne (ingl. k. *scarcity*) – inimesed tunnevad, et nad on kohustatud tegema midagi piiratud aja jooksul ja see tekitab neis ärevust, hirmu ja pettumust.

Li jt (2020) toovad välja sotsiaalse manipuleerimisründe meetodid ja inimeste haavatavust järgmisena:

- kergeusk (ingl. k. *gullibility*) – kõige ärakasutatuim haavatavus, sest enamik inimesi kaldub loomulikult uskuma seda, mida teised ütlevad, selle asemel, et esitada täpsustavaid küsimusi;
- uudishimu (ingl. k. *curiosity*) – omadus, mis julgustab inimesi avaldama salastatud infot;
- viisakus (ingl. k. *courtesy*) – kirjeldab asjaolu, et paljud inimesed tahavad vaikimisi olla abiks ja kasulikumad;
- ahnus (ingl. k. *greed*) – muudab ohvri haavatavaks auhindade andmise meetoditele (nt altkäemaks);
- hirm tundmatu ees (ingl. k. *fear an unknown*) – meetod nii inimeste hirmutamiseks kui ka stimuleerimiseks;
- kergemeelsus (ingl. k. *thougtlessness*) – tavaline nähtus, sest ei saa oodata, et kõik inimesed mõtleksid kogu aeg asju läbi;
- apaatia (ingl. k. *apathy*) – omadus, mis paneb inimesi ignoreerima asju, mida nad ei pea tegema;
- vastutuse hajutamine (ingl. k. *diffusion of responsibility*) – kirjeldab, kuidas inimesed ei taha midagi teha, isegi kui nad on vastutavad, sest nad arvavad, et teised vastutustundlikud inimesed teevad selle ära.

Veenmise kunst on sotsiaalse manipuleerimise rünnakus eriti kvaliteetne ning see keskendub ründaja ja ohvri omavahelisele seosele. (Washo 2021) Veenmise omadused, mis on

küberturvalisuse kognitiivse psühholoogia põhikontseptsioon, on inimtunnete ja käitumise mõistmiseks traditsioonilises raamistikus olulise tähtsusega. (Montanez jt. 2020)

Wang jt (2021: 11900) toovad välja veenmiseks kasutatavad järgmised psühholoogilised mõjutamismehhanismid:

- sarnasus (ingl. k. *similarity*) – see tekitab sümpaatiat, ebakõla viib ebameeldivuseni ja mida rohkem kellegi vaated sarnanevad meie omadega, seda rohkem see inimene meeldib meile;
- tähelepanuvõime häirimine (ingl. k. *distraction in persuasion*) – inimestel on üldiselt piiratud tähelepanu nägemisele, kuulmisele ja mõtlemisele ning see aitab veenda peamiselt vastuargumentide protsessi katkestamise ja suhtlemisvõime suurendamise teel;
- allika usaldusväärsus (ingl. k. *source credability*) – inimesed kalduvad automaatselt alluma autoriteedi näitajatele ja järgnevad autoriteedile ja familiaarsusele, sest need omadused tähendavad usaldusväärsust ja madalat riski.

Autori arvates kasutavad küberkurjategijad psühholoogilise mõju liike sõltuvalt küberrünnakust. Kognitiivsed psühholoogilised võtted sobivad hästi iga võimaliku sotsiaalse manipulerimisründe tehnikaga, kuid on olemas ka diskursiivsed psühholoogilised võtted, mida kasutatakse eriti petukõnedes.

Mõistel „diskursiivne psühholoogia“ puudub täpne ja kokkulepitud definitsioon. Kilby ja Lennoni (2021: 5) arvates käsitleb diskursiivne psühholoogia psühholoogilisi nähtusi nagu mälu või identiteet, kuid peamine mõte seisneb diskussiooni ülesehituses, näiteks metafooride ja repertuaaride kaudu, ning teatud asjade ülesehituses, asendades ühe „versiooni” sündmustest teisega.

Chen (2020: 1077) paljastas diskursiivset psühholoogiat kasutavate petturite järgmised vestlusoskused:

- kordumine (ingl. k. *repetition*) – petukõnede tehnika, mis hõlmab hirmutavate sõnade või lausete kordamist, et viia ohver paanikasse;
- katkestamine (ingl. k. *interruption*) – petturid võivad kasutada vestluse katkestamist, et kontrollida ohvrite psühholoogilist survet;
- suprasegmentaalsed oskused (ingl. k. *suprasegmental skills*) – vestluse käigus kasutatakse üht asjakohast akustilist parameetrit, mis hõlmab kõneelemente nagu hääle kõrgus, intensiivsus, pikenenud helid, kõne kiirus jne.

Sotsiaalse manipuleerimise küberrünnakud kanaliseerivad oma psühholoogilisi rünnakumeetodeid, et veenda ohvrit tegutsema vastavalt rünnaku kavatsusele. Rünnakud kasutavad ära inimeste suhtlemisnõrkusi ja käitumisstruktuure, et leida õige lähenemine

igale inimesele. Küberturvalisuse alast teadlikkust mõjutavad tegurid eakate hulgas on käsitletud töö järgmises alapeatükkis.

1.5 Eakate küberturvalisuse alast teadlikkust mõjutavad tegurid

Küberkuritegevuse ohvrite sotsiaaldemograafilist profiili on vanuse ja hariduse osas väga vähe uuritud. Suurem osa teadusuuringutest on keskendunud vanematele inimestele, sest ründajatel on nendega lihtne manipuleerida ja arvatakse, et nad on küberturvalisuse valdkonnas suuremas ohus (Whitty 2019).

Blackwood-Brown jt (2019) arvavad, et eakad on üks kõige haavatavamaid internetikasutajate rühmi küberrünnakute puhul, mis on suuresti tingitud nende piiratud teadmistest ja oskustest küberjulgeoleku valdkonnas. Seega on küberturvalisuse alane teadlikkus vanemate täiskasvanute jaoks hädavajalik, et võidelda küberrünnakutega, millega nad silmitsi seisavad. (Blackwood-Brown et al. 2019)

Cross (2020) leiab, et petturite sihipärane huvi eakamate vastu on otseselt seotud nende küberturvalisuse järgmiste haavatavate teguritega:

- füüsiline (ingl. k. *physical*) – hõlmab eakate inimeste kognitiivsete protsesside vähenemist, nagu vananemisega kaasnev vaimsete võimete halvenemine;
- rahaline (ingl. k. *financial*) – jaotab eakate inimeste atraktiivsuse selliste finantspositsioonide tõttu nagu säästud, pensionifondid ja krediidivõimalused;
- sotsiaalne (ingl. k. *social*) – viitab eakate inimeste haavatavusele, sealhulgas üksinduse, sotsiaalse isolatsiooni või negatiivsete sündmuste põhjustele, nagu hiljutine lähedase surm.

Juarez jt (2018) märgivad, et vanem elanikkond demonstreerib aktiivset soovi õppida tundma uusi internetitehnoloogiaid ning paljud kasutavad neid selleks, et seista vastu üksindusele ja isolatsioonile, jääda sotsiaalselt aktiivseks, suhelda perega ja nautida pensioniiga. Need võimalused on otseselt seotud suurenenud riskiga saada pettuse ohvriks, mis tuleneb piiratud teadmistest küberjulgeoleku valdkonnas. (Juarez at al. 2018)

Morisson ja Benjamin (2020) rõhutavad oma uuringus järgmisi tegureid, mis aitavad kaasa küberturvalisuse haavatavusele eakate inimeste hulgas:

- sotsiaalses suhtluses tehtavad uuendused (ingl. k. *renewing social interaction*) – kaasaegsete tehnoloogiate kaudu toimuv sotsiaalne suhtlemine, kasutades sotsiaalvõrgustikke, mis suurendavad ohtu isiklikule küberturvalisusele ebakindluse või ebapädevuse tõttu;
- rahaliste vahendite muutumine (ingl. k. *changes in finance*) – toob kaasa sissetuleku vähenemise pärast pensionile jäämist, mis tekitab ebamugavust ja kehtestab uued

eeskirjad finantshoiakute kohta, kuid ka suurendab huvi internetipanganduse teenuste vastu, et kontrollida oma kulusid;

- muutused igapäevaharjumustes (ingl. k. *a loss of day-to-day routine*) – rohke vaba aja olemasolu julgustab rohkem uurima internetivõimalusi, rakendusi telefonis, võrgumänge ja muid asju, mis ohustavad küberjulgeolekut, kuna puuduvad oskused ja kogemused;
- muutused tajutavas pädevuses (ingl. k. *loss of perceived competency*) – madal enesekindlus ja tehnoloogilise teadlikkuse ja arvutioskuse alahindamine;
- tugistruktuuride kaotus (ingl. k. *loss of technical support structures*) – varem omandatud küberturvalisuse alased teadmised muutuvad vananenuks ning uute teadmiste omandamine ja kohanemine muutustega toob vanematele inimestele kaasa riskantseid otsuseid, kuna tugineb vananenud arusaamadele.

Norris, Brookes jt (2019) väidavad, et teadusuuringud on rohkem keskendunud vanusele kui riskitegurile, mida vanemad täiskasvanud peavad küberkuritegevuse suhtes tundlikuks. Tegelikult võib vanust pidada hoopis kaitseteguriks, sest vanemad inimesed on küberturvalisuse mõistmisel vastutustundlikumad, kuna on tehnoloogilise progressi suhtes jätkuvalt usaldamatud. (Norris, Brookes et al. 2019)

Autori arvates võib küberturvalisuse haavatavust mõjutavaid tegureid, mida peetakse eakate inimeste näitel, osaliselt arvesse võtta ka teistes vanuserühmades. Küberturvalisuse alane teadlikkus mängib tähtsat rolli iga inimese igapäevases tegevuses, et püsida kaitstud kiirelt muutuvas digitaalses ühiskonnas.

Järgmises peatükis esitab autor tema poolt läbi viidud rakendusuuringu alustel tulemused, järeldused ja ettepanekud.

2. IDA-VIRUMAA EAKATE KÜBERPETTUSTE ALANE TEADLIKKUS PANGATEENUSTE VALDKONNAS JA SELLE TÕHUSTAMISE VÕIMALUSED

2.1 Ida-Virumaa küberpettuste keskkonna iseloomustus

Arenev digitaaltehnoloogia on suurendanud nii kaudsete kui ka otseste ohtude hulka interneti kasutajale ning tema isikuandmetele. Justiitsministeeriumi statistika kohaselt kasvab küber- ja arvutikuritegude arv, mistõttu leidub üha rohkem inimesi, kes on kokku puutunud küberkuritegevusega. (Justiitsministeerium 2022). Kaitsepolitsei aastaraamat 2020-2021 märgib, et küberrünnakute ja -kuritegude puhul on suur oht inimlikele nõrkustele ja/või puudulikule küberhügieenile, mis võib ohustada kasutaja enda isikuandmeid. (Kaitsepolitsei aastaraamat 2020–2021)

Viimastel aastatel on kogu maailmas olnud palju rohkem küberrünnakuid pankade vastu. Mitmete selliste juhtumite korral peavad inimesed taluma nende olukordade tagajärgi, milleks võivad olla häired neile pakutavate teenuste töös. Eesti pangandus on peaaegu täielikult digitaalne, mis seab küberturvalisusele siinmail eriti kõrged nõudmised. (Eesti Pangaliidu veebileht 2022) Justiitsministeeriumi statistika kohaselt kasvas 2021. aastal küberkuritegude arv. Arvutikuritegusid registreeriti 63% rohkem kui 2020. aastal, millest 31% moodustasid petukõned. (Justiitsministeerium 2022)

Sagenenud on telefonipettuste arv, kus Eesti elanikele helistavad aktiivselt petturid, kes tutvustavad end pangatöötajana ning suudavad sellega välja petta suuri summasid. Ründajad üritavad telefonikõne teel inimeste pangakontole ligi pääseda või pakuvad neile investeerimisvõimalusi, mida uskudes teevad ohvrid ise petturite kontodele ülekandeid. Uuringud näitavad, et keskmisest vähem tunnevad küberturvalisuse ohumärke vene rahvusest ja madalaima sissetulekuga inimesed. (Eesti Pangaliidu veebileht 2022)

Ida-Viru maakond asub Eesti kirdeosas, koosnedes Soome lahe lõunarannikust, Narva jõest ja Peipsi järve põhjaosast. Pärast 2017nda aasta haldusreformi moodustavad Ida-Viru maakonna Jõhvi vald, Kohtla-Järve vald, Toila vald, Narva linn, Narva-Jõesuu linn, Sillamäe linn, Alutaguse vald ja Lüganuse vald. (Ida-Viru Maakonna Arengustrateegia 2019 – 2030)

Vastavalt rahvastikuregistri andmetele on 01.01.2022. aasta seisuga Ida-Viru maakonna kohalike omavalitsuste rahvaarv 131 757 inimest. Eakad vanuses 65 aastat ja enam moodustavad 26% Ida-Virumaa rahvaarvust ning nende osakaal on kasvav (Tabel 2).

Tabel 2. Ida–Virumaa elanike demograafiline struktuur seisuga 01.01.2022

Kohalik omavalitsus	**lapsed 0-6a.**	**lapsed 7-18a.**	**Tööealised 19-64a.**	**Eakad 65+**	**Elanike arv kokku**
Alutaguse vald	254	940	2 763	1 105	4 659
Jõhvi vald	729	2 264	6 224	2 920	11 144
Kohtla-Järve linn	1 674	6 718	18 213	8 497	32 273
Lüganuse vald	404	1 539	4 516	2 392	8 203
Narva linn	2 872	11 168	30 792	13 867	53 979
Narva-Jõesuu linn	224	908	2 751	1 215	4 714
Sillamäe linn	549	2290	6 925	3 366	12 168
Toila vald	288	1028	2 675	1 059	4 617
Kokku maakonnas	**6 994**	**26 855**	**74 859**	**34 421**	**131 757**

Allikas: Rahvastikuregister. Autori koostatud.

Tuginedes Eesti Statistika andmetele 01.01.2022. aasta seisuga räägivad Ida-Virumaal eesti keelt emakeelena ainult 14,5% rahvastikust ehk umbes 18 000 inimest, ülejäänud kasutavad igapäevaelus vene keelt. (Statistikaamet 2022)

Eesti Pangaliidu küberturvalisuse infokampaania "Ei, aitäh" algas 2021. aastal, mille eesmärk oli aidata tuvastada pettused ja ennetada seeläbi uusi küberkuritegevuse ohvriks langemise võimalusi. Kampaania raames said inimesed teavet finantspettuste kohta televisioonist, raadio- ja trükimeediast, brošüüridest ja internetist veebilehel - http://eiaitah.ee/. (Eesti Pangaliidu veebileht 2022) Erilist olulisus on keskendatud venekeelsele kommunikatsioonile, sest Politsei- ja Piirivalveameti andmetel on enamik telefonikõnede ohvreid just Eestis elavad igas vanuses vene keelt kõnelevad inimesed. (Politsei- ja Piirivalveamet veebileht 2022)

Eesti Pangaliidu poolt tellitud Norstati uuring "Ei, aitäh" küberturvalisuse infokampaania näitab millised on Kirde-Eesti elanike ohumärgid, mis teeb nad haavatavamaks panganduspettustele: (Norstati Uuring 2021)

- informeeritus ja teadlikkus küberkuritegevuste teemal on madalal tasemel;
- inimeste käitumine pettusekahtluse korral on kõhklev, sest ei teata, kuidas tegutseda.

Küberturvalisuse teabekampaaniat korraldavad ja toetavad järgmised suured pangad Ida-Virumaal:

- Swedbank AS - mille kodulehel on infoblogi "Kuidas kaitsta oma raha pettuste eest?" nii eesti kui ka vene keeles. Esitatud on väga põhjalikud pettuste liigid ja juhised,

mida klient saab järgida oma turvalisuse huvides. Panga esindused asuvad Jõhvis ja Narvas ning ööpäevaringselt on avatud infotelefon. (Swedbank AS veebileht 2022);

- AS SEB Pank - mille kodulehel on esitatud erinevad küberturvalisuse artiklid, näiteks „ Kuidas vältida pettust?" nii eesti kui ka vene keeles. Panga esindused asuvad Jõhvis ja Narvas ning ööpäevaringselt töötab infotelefon. (AS SEB pank veebileht 2022);
- Coop Pank AS - mille kodulehel on küberturvalisuse blogi, kus on soovitused turvameetmete kohta erinevatel pangakanalitel ning töötab eesti ja vene keelne elektrooniline vorm: ''Teata õngitsuslehest.'' Panga esindus asub ainult Narvas ja infotelefon töötab esmaspäevast reedeni hommikul kella poole üheksast kuni õhtul kella seitsmeni. (Coop Pank AS veebileht 2022).

Keskkriminaalpolitsei on 2020. aastal loonud küberturvalisuse tõstmiseks ja küberkuritegudele kiiremini reageerimiseks teabe ja teadete edastamise veebilehel - https://cyber.politsei.ee/ Selleks on kompaktne ja struktureeritud elektrooniline vorm – „Edasta teade kuriteost," mis on saadaval nii eesti kui ka vene keeles. Veebilehel on esitatud ennetavaid nõuandeid, kuidas vältida pettuse ohvriks langemist kui ka informatsiooni selle osas, kuidas käituda kui see on juba inimesega juhtunud. (Politsei ja Piirivalveameti veebileht 2022)

Alates 2019. aastast on alanud küberturvalisuse infokampaania "Ole IT-vaatlik", mis on viinud Riigi Infosüsteemi Ameti poolt loodud küberturvalisuse portaali valmimiseni - https://www.itvaatlik.ee/. Teavitamine portaalis on mõeldud vene ja eesti keelt kõnelevatele inimestele, kes ühel või teisel viisil puutuvad kokku kaugtöö või -õppega. "Ole IT-vaatlik" kampaania kordab arvutikasutajatele, et nad peavad kontrollima, kellega nad e-posti teel suhtlevad, uuendama oma kaugtööseadmete tarkvara, vältima kahtlaseid manuseid ja linke ning hoolitsema oma isikuandmete turvalisuse eest. (RIA veebileht 2022)

Küberturvalisuse aastaraamat 2022 näitab, et eakate küberhügieen on endiselt madalamal tasemel kui noorematel inimestel. Uuringud kinnitavad, et küberhügieeni taset mõjutab rahvus. Eestlased teevad rohkem tööd oma küberturvalisuse tugevdamiseks kui teiste rahvuste elanikud. Vaatamata mitmesuguste küberturvalisuse meetmete väljatöötamisele ja tõstmisele ei vähenenud pettuste arv. (Küberturvalisuse aastaraamat 2022)

Viimastel aastatel on Ida-Virumaa pangandusteenuste valdkonnas olnud raske küberturvalisuse keskkond. Küberpettused on muutunud mitmekesisemaks, olles keskendunud vene keelt kõnelevatele inimestele, kes elavad suurel hulgal Ida-Virumaal. Selleks et parandada olukorda ja suurendada teadlikkust küberjulgeoleku aluspõhimõtetest, tehakse selles küsimuses rohkem uuringuid.

Järgnevas alapeatükis esitab autor uuringu metodoloogia.

2.2 Eakate küberpettuste teadlikkuse uurimise metoodika ning kogum ja valim

Lõputöö rakendusuuringu abil selgitatakse välja, milliseid probleeme on eakad kogenud seoses digitaalteenuste kiire kasvuga pangandusteenuste valdkonnas ja millised on ohumärgid, mis teevad nad küberpettuste suhtes haavatavamaks. Uuringu tulemustele tuginedes on saab järeldusi teha ning pakkuda välja ettepanekuid, kuidas on võimalik täiustada eakate elanike kaitset küberkuritegevuse eest.

Uuringu läbiviimiseks valis autor kvalitatiivse uurimisviisi. Kvalitatiivse tunnetusliku meetodina on kasutuses tekstianalüüs, mille abil on võimalik analüütiliselt tõlgendada suulisi ja kirjalikke sõnumeid. Andmete kogumiseks kasutatakse avatud lõpuga küsimusi, millele intervjueeritaval on võimalik oma sõnadega vastata. (Lepik jt. 2014) Tekstilised andmed võivad pärineda individuaal- või fookusgrupi-intervjuudest, vaatluspäevikutest, erinevatest dokumentidest, uuritavate omaloomingust ja kõikvõimalikest meediaväljaannetest. (Kalmus jt. 2015)

Kvalitatiivsete uuringute abil tegeletakse inimeste isikliku kogemuse või sotsiaalsete olukordade uurimise, sõnastamise ning tõlgendamisega. Kvalitatiivsete uuringute abil püütakse ennekõike mõista kindlaks määratud osalejate maailmavaadet kui et kontrollida mõne eelnevalt püstitatud hüpoteesi täpsust. (Laherand 2008: 20)

Lõputöö uuringu liigiks on juhtumiuuring, mis aitab mõista kindlaksmääratud üksust põhjalikult läbi süvaanalüüsi. Üksuseks, võib olla sealhulgas inimene, inimestest moodustunud grupp, aset leidnud või eesootav sündmus, ka projekt, või asutus. (Strömpl 2014) Juhtumi sihtgrupp on Ida-Virumaa vene keelt kõnelevad eakad inimesed, kes on kõige haavatavamad investeeringute ja pangapettuste suhtes ning hakkasid aktiivsemalt kasutama digitaalkanalites pangateenuseid pandeemia ajal, viimase kahe aasta vältel.

Lõputöö intervjueerimisel saadud andmeid on analüüsitud kvalitatiivse sisuanalüüsi meetodiga. Kodeerimine on kvalitatiivse analüüsi põhitegevus, mille käigus jagatakse andmed osadeks, et teksti põhjalikult uurida ja mõista. Selle meetodi jaoks on tähtis leida ning omavahel luua seoseid selliste kategooriate ja koodidega, mis ühildaksid analüüsitava teksti ja uurimisküsimuste peamisest seisukohast saadavad olulised tähendused. Kvalitatiivset süvaanalüüsi iseloomustab delikaatsus ja täpsus, mis võimaldab pöörata harvaesinevatele ja haruldasetele sündmustele või asjaoludele. (Kalmus jt. 2015)

Kvalitatiivse uurimisviisi üks levinumaid andmete kogumise meetodeid on intervjuu. Andmekogumise meetodiks valis autor poolstruktureeritud intervjuu. Poolstruktureeritud intervjuu puhul on kasutuses kahte lähenemist: ühelt poolt on kasutuses intervjuukava, mis on eelnevalt vormistatud, ning teisest küljest võib muuta küsimuste järjekorda ja nende esinemist ning ühtlasi küsida lisaküsimusi. (Lepik jt. 2014)

Kogumi moodustamiseks viis autor telefoni teel läbi ekspertintervjuu Eesti Pangaliidu tegevdirektoriga, kes vastutab küberturvalisuse kampaania "Ei, aitäh" läbiviimise eest pangandussektoris, kus sihtrühmana on määratletud just eelkõige eakad venekeelt emakeelena kõnelevad elanikud. Ekspertintervjuude tegemine on üks laialt levinud kvalitatiivse uuringu meetodeid, mis annab uurijale tihti rohkem infot intervjueeritavate isiklike vaadete kohta. Uuring leiab aset selliselt, et vastaja vestleb uurijaga kahekesi ja sellepärast on võimalus pidada arutelusid delikaatsetel uuringuteemadel ja ühtlasi privaatsust nõudvates sihtrühmades (Flick 2019: 174).

Eesti Pangaliidu tegevdirektori abitöötajad andsid autorile viimase Norstati poolt tellitud uuringu käigus küberturvalisuse kampaanias kasutatud andmed, et nende tulemuste põhjal saaks autor oma uuringuga sügavale minna ja inimesi täpsemalt intervjureerida.

Uuringu kogum moodustati järgmiste tunnuste põhjal:

1) asukoha järgi - Kirde-Eesti elanikud on pangandus- ja investeerimispettustele kõige haavatavamad.
2) rahvuste järgi - vene rahvusest ja madalaima sissetulekuga elanikud vähem tunnevad pettuste ohumärke.
3) teadlikkuse järgi – elanike informeeritus kübegrkuritegevuste teemal ja käitumisest pettusekahtluse korral on madalal tasemel.

Autori lai suhtlusring aitas leida inimesi, kes võiksid intervjuust osa võtta. Valimi moodustamiseks kasutas autor mugavusvalimi meetodit. Mugavusvalimi korral uurija valib sellised uuritavad välja, keda lihtne uurimusse saada, näiteks sugulased, tuttavad, õpilased või kesklinna korterelamute alumiste korterite elanikud. Sel juhul ei saa teha rangeid üldistusi, sest nende vastused peegeldavad vaid lähimasse tutvusringi kuuluvate isikute ja uurijale kergemini kättesaadavate inimeste hinnanguid. (Rämmer 2014)

Valimi moodustamisel ehk intervjuus osalejate valiku tegemisel lähtuti sellest, et inimesed kasutavad või on kasutanud pangateenuseid ja muid internetivõimalusi seoses digitaalkanalite kiire kasvuga. Määravaks sai asjaolu, et intervjueeritavad on aastatel 2020–2022 kandnud rahalist kahju küberkuritegevuse tõttu. Tingimusteks oli see, et inimesed

peavad elama Kirde-Eestis Ida-Viru valdkonnas; olema vanuses 65 või vanem aastat ning kõnelema emakeelena vene keelt. Autor laiendab vanuserühma uuringu kogumit, kuna Eesti Pangaliiduga Norstati poolt tellitud uuring oli piiratud kuni 64-aastaste elanike haavatavuste väljaselgitamisega.

Valimisse kuuluvate eakate elanikele intervjuuks koostas autor kokku kümme küsimust, mis on seotud küberturvalisuse ja küberkuritegevuste teemaga pangateenuste valdkonnas eakate elanike jaoks. Kõik küsimused on avatud ja vajavad eakate elanike põhjalikku vastust. Intervjuu küsitluse sihtrühmaks on valitud vene keelt kõnelevad inimesed ning seepärast koostati intervjuu küsimused nii eesti kui ka vene keeles. Intervjuu küsimused on esitatud lisas 1.
Järgnevas alapeatükis esitab autor uuringu läbiviimise informatsioon.

2.3 Ekate küberpettuste teadlikkuse uuringu läbiviimine

Uuringut ette valmistades vestluse jaoks nõusoleku saamiseks võttis autor telefoni teel ühendust osalejate lähedastega, kellega oli varem selle uuringu osas kokku leppinud. Autorile edastati informantide telefoninumbrid, selleks et leppida kokku uuringu läbiviimise tingimustes ja saada nõusolek otse informantidelt. Vestluses informantidega autor tutvustas ennast ja andis intervjuu kohta üldinfot ning lepiti kokku kohtumise toimumise kuupäev ja kellaaeg. Eeldati, et intervjuu toimub isiklikul kohtumisel, näiteks avalikus kohas, kuid see ei sobinud kõigile informantidele. Kolme informantidega lepiti kokku isikliku kohtumise vormis intervjuude korraldamine. Ülejäänutega saavutati lepe, et intervjuu toimub telefoni teel.

Intervjuud toimusid ajavahemikul 07. - 27. märts 2022. Mõned kokkulepitud intervjueerimise ajad muutusid mitmeid kordi. Venemaa poolt Ukraina vastu algatatud sõja tõttu olid Ida-Virumaa eakad vene kodukeelega elanikud hirmul maailma poliitilist ja informatiivset olukorda jälgides. Informandid olid sellest olukorrast häiritud. Mõningaid intervjuude ja korralduste ajakavasid ja kuupäevi tuli kohandada, aga igal juhul kõik kokku lepitud intervjuud said läbi viidud.

Intervjuude kestus oli keskmiselt 40 minutit. Intervjuu alguses tutvustas lõputöö autor uuesti ennast, lõputöö teemat ja uuringut. Kõige olulisem oli informantide jaoks see, et kohtumisel saadud vastused ja konfidentsiaalsed andmed ei kuulu otseselt isiklikude andmete avalikustamisele, ning et isikliku kohtumise vormi puhul on täidetud tingimused, mis on

seotud Covid-19 levimise ettevaatusabinõudega, nii maski kandmisega kui ka sotsiaalse füüsilise distantsi säilitamisega.

Kolm intervjuud viidi läbi telefoni teel ja kolm intervjuud toimusid otse kohtumise puhul kohvikus. Intervjueerides esitas autor küsimused suuliselt vene keeles ja tegi iga küsimuse kohta kirjalikud märkmed arvutisse, et oli lihtsam intervjuu salvestusi tekstis transkribeerida.

Andmete töötlemisetapis tõlgiti eesti keelde intervjuerivate vastused, mis esitatakse uuringu tulemuste alapeatükis ning saadud vastused informantidelt, mis oli transkribeeritud ja sisesestanud tabelisse (vt. lisa 2), kus vastamise järjekord vastab intervjuus esitatud küsimuste järjestusele. Grupeerimise kriteeriumiks oli vastuste struktureerimine ja teatavate aspektide filtreerimine, et leida olulisi tekstiteemasid ja leida nendevahelisi seoseid. Seejärel andmeid analüüsiti kvalitatiivse sisuanalüüsi meetodil.

Intervjuu käigus keskendus lõputöö autor Ida-Virumaa eakatele järgmistele teemadele: informatsiooni saamise allikad küberturvalisuse, küberohtude ja levinud finantspettuste liikidest ja digitaalsete tehnoloogiate kasutamine igapäevaelus, oskuste ja tehniliste oskuste hindamine. Lisaks sai autor intervjuu käigus küsitletud isikutelt teavet selle kohta, kuidas nad ise olid pettuse ohvriks langenud, ning sellega seotud alateemadest: küberpettuste liigid, esmane kontakt ohvriga, küberpettuse ohvrile mõju avaldamise meetodid, tagajärjed ja tegevused küberpettuste kahju korral.
Järgnevas alapeatükis esitab autor tema poolt läbi viidud uuringu tulemused.

2.4 Eakate küberpettuste alase teadlikkuse uuringu tulemused

Intervjuu käigus saadud vastused avatud küsimustele on esitatud tabelis (Lisa 2). Need andmed on kodeeritud ja seejärel koodid grupeeritud ning moodustati kategooriad. Andmete analüüsimisel moodustati kategooriad, mille alusel kogutavad andmed esitatakse järgmiste teemade kaupa:

- informatsiooni saamise allikad küberturvalisuse, küberohtude ja levinud finantspettuste liikidest,
- digitaalsete tehnoloogiate kasutamine igapäevaelus, oskuste ja tehniliste kompetentside hindamine,
- küberpettuste liigid, esmane kontakt ohvriga,
- küberpettuse korral ohvrile mõju avaldamise meetodid,
- tagajärjed ja tegevused küberpettuste kahju korral.

Informatsiooni saamise allikad küberturvalisuse, küberohtude ja levinud finantspettuste liikidest. Intervjuu küsimus: „Millistest allikatest saate Teie infot küberturvalisuse, küberohtude ja kõige levinumate finantspettuste kohta?''

Uuringu tulemused näitavad, et eakate inimeste informeeritus teemades küberturvalisus, küberähvardus, ja küberpettuste liigid on küllaltki halb tasemel. Enamasti saadakse informatsiooni lähedastelt ja vähem internetist, raadiost ning ajalehtedest.

> Informant 4*: ,,Ei saa vastata sellele küsimusele. Mulle tundub, et ajalehtedes midagi vilkus pettusest viimasel ajal läbi. Taksos sõites raadiost vist kuulsin, et ei tohi kellelegi enda paroole öelda. Üldiselt ise sellesse teemasse ei süvenenud põhjalikult. Kui on küsimusi, siis helistan lastele, nemad selgitavad ja aitavad.''*[1]

Digitaalsete tehnoloogiate kasutamine igapäevaelus, oskuste ja tehniliste kompetentside hindamine. Intervjuu küsimused: „Milliseid internetipanga teenuseid või muid digitaalseid lahendusi, programme või rakendusi olete viimase kahe aasta jooksul oma igapäevaelus kasutanud? Millisel eesmärgil?" ja „Kuidas Te hindate oma arvuti või telefoni digitaalset oskust ja kuhu pöördute tehniliste probleemide või raskuste ilmnemisel?"

Uurimus näitas, et kõik küsitletud küsitletavad kasutavad internetipanka, nii arvutis kui ka telefonis, kommunaalmaksete maksmiseks ning ülekannete tegemiseks, ka lähedastega suhtlemiseks kasutatakse rakendusi ning tehakse veebioste.

> Informant 5: *,,Viimaste aastate jooksul õppisin selgeks, kuidas on vaja teha ülekandeid arvuti kaudu ise, oskan korteri eest maksta ja vaadata kontojääki. Enne maksin tavaliselt kõike sularahas ja käisin kontoris kohapeal. Hetkel enam pangad sularahaga ei tegele - oli vaja midagi välja mõelda. Iga kord paluda lapsi või naabreid appi on ebamugav ja ma ei taha neid segada.''*[2]

[1] Информант 4: ,,Не могу ответить на этот вопрос. Мне кажется, в газетах что-то мелькало про мошенников в последнее время. По радио слышала в такси наверное, что нельзя никому свои пароли говорить. В целом сама этот вопрос не изучала подробно, если что, так я детям звоню, они объясняют и помогают.''

[2] Информант 5: ,,За последние несколько лет научилась делать переводы сама через компьютер, квартиру оплатить или выписку по счету посмотреть умею. Раньше платила в основном наличными все ходила в контору, сейчас они не работают с наличными деньгами, пришлось выкручиваться – каждый раз детей или соседку просить не будешь – неудобно, да и мешать не хочется.''

> Informant 6*: ,,Ülekandeid teen, väljavõtet vaatan, isegi pangakaardi kunagi aktiveerisin ise. Hiljuti tegin kodukindlustuse, pangatöötajate abiga - helistasin telefoni teel, kõike selgitati kiiresti ja arusaadavalt . ''*[3]

Informantidelt 5 ja 6 saadud andmed aitavad mõista, et mõnede inimeste jaoks oli üleminekuks sularaha operatsioonidelt digitaalsetele teenustele põhjuseks pangaesinduse teenindamismudeli muutus.

Suurem osa intervjueerituist aktiivselt kasutavad niisuguseid rakendusi nagu Viber, Skype ja e-mail oma lähedastega suhtlemiseks ja informatsiooni küsimiseks ning saamiseks.

> Informant 3*: „Kasutan Viber'i lähedastega suhtlemiseks, nad saadavad seal fotosid ja videoid mulle.''*[4]

> Informant 2: *,,Kasutan elektronposti, saades ja jälgides poodide igasuguseid reklaam postitusi.''*[5]

Eakad omandavad aktiivselt internetist ostmise kogemust ja küsitlejate seas jagunes arvamus kaheks: pool nendest kasutavad välismaalt kauba tellimiseks niisuguseid rakendusi nagu Aliexpress, Joom, Ebay, teine grupp niisugustest võimalustest ei ole kuulnud või ei pea seda igapäevaelus vajalikuks.

> Informant 1: *„Jah, sain Aliexpressi ja Joomi kasutamise selgeks. Pension ei ole suur, sellega seoses on soov tellida kodu jaoks esemeid ja endale riideid odavamalt.''*[6]

> Informant 5: *„Ei, sellega ei tegele ega soovi praegu ka süveneda. Piisab sellest, mis on eluks vajalik, pension ka ei ole nii suur, et tellida midagi.''*[7]

Enda arvuti ja telefoni kasutamise oskusi suurem osa informandid ei oska hinnata või kuidagi kommenteerida. Tehniliste küsimuste tekkimisel pöörduvad nad otse lähedaste poole.

[3] Информант 6: ,,Переводы делаю, выписку смотрю, даже карту банковскую сама как-то активировала. Не так давно страховку делала на квартиру, правда с помощью работников банка – звонила по телефону, все быстро и грамотно объяснили.''

[4] Информант 3: ,,Пользуюсь Viber для общения с близкими, фотографии мне туда присылают или видео''

[5] Информант 2: ,,Пользуюсь электронной почтой, слежу за всякими рекламными рассылками магазинов.''

[6] Информант 1: ,, Да, освоила Aliexpress и Joom. Пенсия небольшая, поэтому хочется что-то заказать для дома или из одежды подешевле.''

[7] Информант 5: ,, Нет, таким не занимаюсь и вникать пока не хочу. Хватает того, что необходимо для жизни, да и пенсия у меня не такая большая, чтобы заказывать что-то.''

> Informant 1: „*Olid probleemid telefoni seadistamisega, kuhugi telefoni ettevõttesse poeg isegi läks kui käis siin.''*[8]

> Informant 3: „*Kui tekib probleem, siis lapselaps tuleb ja aitab seda lahendada. Ta on minu IT spetsialist.''*[9]

Mõned informandid, nende seas 1 ja 5 hindavad oma arvuti ja telefoni oskust heal tasemel, kuid ainult üks neist teab, kuhu võib pöörduda tehniliste probleemide või teiste küsimuste korral.

> Informant 6*: „Tehniliselt poolelt kommenteerida ei saa, ise ei ole kogemustega häkker. Tavaliselt kord aastas viin sülearvuti puhastusse arvuti firmasse, ja telefon on garantiiga - ei muretse selle üle.''*[10]

Küberpettuste liigid, esmane kontakt ohvriga. Intervjuu küsimus: „Kuidas Te sattusite küberpettuste ohvriks ja kuidas tekkis esmane kontakt petturitega?"

Uurimuse käigus selgus, et petturite esmane kontakt toimus enamasti telefonikõne kaudu. Kahes juhtumis toimus esmane kontakt elektronposti ja Viber rakenduse läbi, edasine kontakt oli telefonikõne.

Petturid tutvustasid end pangatöötajatena, politseina, Google kompanii esindajana, investeerimiskonsultandina või huvitatud ostjana. Enamus juhtumeid ühendab fakt, et petturid kasutasid manipuleerides ära mingisugust juhtumikirjeldust, kus ohvritel oli tekkinud probleem, mis vajas kohest lahendamist.

> Informant 1: „*Mees helistas Google'i tehnilisest toest, kuna minu telefonil avastati mingi probleem.''*[11]

> Informant 4: „*Pangatöötaja ütles, et sellel nädalal on viimane võimalus uuendada enda kontaktandmeid ning peale seda aega ei ole võimalik teha ülekandeid ja kasutada muid teenuseid.''*[12]

---

[8] Информант 1: ,, Были проблемы с настройкой телефона, куда-то сын даже ходил в телефонную компанию, когда приезжал.''

[9] Информант 3: ,, Если есть проблемы, внук приходит помогает разобраться – он у меня ИТ специалист.''

[10] Информант 6: ,,С технической стороны комментировать не могу, сама я не такой хакер опытный. Обычно раз в год ношу ноутбук почистить в компьютерную фирму, да и телефон на гарантии – не переживаю за этот счет. Работает всегда все исправно, как часы.''

[11] Информант 1: ,, Мужчина звонил из службы технической поддержки Google, потому что на моем телефоне обнаружили какую-то проблему.''

[12] Информант 4: ,, Работник банка сказал, , что на этой неделе последний срок обновления контактных данных в интернет-банке и что после окончания срока невозможно будет пользоваться переводами и другими услугами.''

> Informant 5: „*Mees politseist ütles, et eeldatavasti on see pettus ning minu andmetega üritab keegi inimene minu nimele laenu võtta - politsei tegeleb selle küsimusega praegu panga palvel.''*[13]
>
> Informant 6*: ,,Pangatöötaja teatas, et minu pangakontolt toimuvad kahtlased tehingud päringuga minu kaardile ja nimetas mingisugust veebipoodi, mille nime ma ei olnud varem kuulnud. ''*[14]

Informantide 2 ja 3 juhtumeid võib vaadata sellest seisukohast, et esmane huvi oli neil endil. Üks neist soovis saada investeerimise konsultatsiooni, teine müüa kaupa internetis.

> Informant 2*: „E-postile tuli kiri teemal investeerimine krüptorahasse. Kirja lõpus oli link ankeedile, ning teave, et kui on lisaküsimusi, võtab teiega ühendust investeerimise osakonna spetsialist. Jätsin enda andmed igaks juhuks, ei mõelnud, et keegi mulle helistab.''*[15]
>
> Informant 3*: ,,Panin müüki diivani, kuna planeerisin endale uue osta. Mõtlesin, et äkki keegi tahab seda endale suvilasse. Minuga võttis ühendust mees, kes oli nõus ostma, kuid palus maksta minul kinni transpordikulud, et olla kindel selles, et teda ei peteta. Ütles, et saadab transpordikulude maksmise juhendi läbi Viber'i ja helistab, et aidata.''*[16]

Küberpettuse korral ohvrile mõju avaldamise meetodid. Intervjuu küsimused: „Millist isiklikku teavet Te petturitele vestluse ajal edastasite ja mis teie otsust mõjutas?" ja „Milliseid emotsioone või tundeid Te petturitega suheldes kogesite?"

Kogutud uuringu andmetest võib saada aru, et petturid kasutavad edukalt psühholoogiliste mehhanismide mõjusid. Kõikides juhtumites väljendus informantide enesetundes rahu ja kindlustunne, et nad suhtlesid oma ala päris esindajatega.

> Informant 6*: ,,Oli kindlus, et suhtlen panga esindajaga (tagaplaanil oli kontori, klaviatuuri heli, mingisugused printeri hääled tundusid.)''*[17]

---

[13] Информант 5: ,, Мужчина из полиции сказал, что видимо это мошенничество и с моими данными тот человек пытается на мое имя кредит оформить – вот полиция занимается сейчас этим вопросом по просьбе банка.''

[14] Информант 6: ,, Сотрудник банка сообщил, что с моего счета идут подозрительные сделки с запросом на мою карту и назвал какой-то интернет магазин Американский, о названии которого я ранее не слышала.''

[15] Информант 2: ,, На электронную почту мне пришло письмо на тему инвестирования в криптовалюту. В конце письма была ссылка на анкету, если есть дополнительные вопросы, то с вами свяжется специалист инвестиционного отдела. Я данные оставил на всякий случай, хотя не думал, что мне кто-то позвонит. ''

[16] Информант 3: ,, Выставила на продажу диван, поскольку свой планировала обновлять, может кто купит себе на дачу. Со мной связался мужчина и согласился купить, но опросил оплатить доставку, чтобы быть уверенным в том, что его не обманывают. Сказал, что отправит инструкцию по оплате доставки в Viber и позвонит чтобы помочь.''

[17] Информант 6: ,,Была уверенность, что я разговариваю с сотрудником банка (на фоне был звук офиса, клавиатуры, какие-то шумы принтер напоминало).''

Informant 5: *,,Ta avaldas tähelepanu, hoolivust, headust ja kiitis mind, kui kõike õnnestus kinnitada.''*[18]

Informant 2*: ,,Ma tundsin kindlust, et suhtlen oma ala professionaaliga.''*[19]

Kõikides juhtumites, vaatamata pettuste liigile, esitasid informandid oma isiklikke kontakte ja panga andmeid, mida petturid nõudsid. Petturid kasutasid veenmise oskust ja mõningates juhtumites pakkusid tehnilist lahendust, seoses sellega ohvritel ei tekkinud kahtlust nende osas.

Informant 1: „*Suhtluse käigus mees, kellega rääkisin oli rahulik ja enesekindel, mul puudus kahtlus tema osas. Meie vestluse keskel mees ütles, et on olemas kiire lahendus, selleks et kaitsta enda telefoni - programm nimega "Anydesk", mida on vaja telefoni paigaldada koheseks andmete kaitseks."*[20]

Informant 2: *,,Ta ütles, et neil kehtib väljatöötatud programm "AnyDesk", mille kaudu nad aitavad algajatel teha esimesi investeerimisi ja selleks, et seda teha, on vaja vastav programm paigaldada arvutisse.''*[21]

Tegelikkuses pole programm "AnyDesk" pettuslik nuhktarkvara. Tegu on üldkättesaadava programmiga, mis on kasutamiseks kõikidele kasutajatele nii arvutis kui ka telefonis. See programm teostab kaugjuhtimisseadme funktsiooni, mis võimaldab täielikult kontrollida oma seadmeid ükskõik, milliselt kaugusest.

Tagajärjed ja tegevused küberpettuste kahju korral. Intervjuu küsimused: „Miks ja millisel hetkel Te taipasite, et Teid petetakse?", „Millised tegevused järgnesid pettusekahtlusekorral, kui kiiresti ja kuhu Te abi saamiseks pöördusite?", „ Kas pärast Teiega juhtunut vajasite psühholoogilist abi või muud abi?", „Kas Te jätkate digitaalteenuste kasutamist oma igapäevaelus? Mis õppetunni olete enda jaoks õppinud ja mida saate ise teha, et seda olukorda tulevikus vältida?"

Tuginedes uurimise käigus saadud andmetele, võib öelda et enamus informandid mõistsid, et neid petetakse alles pärast vestluse lõppu petturiga. Mõned informandid hakkasid juba

[18] Информант 5: ,,Он проявлял внимательность, заботу, доброту и хвалил меня, когда все получилось подтвердить.''

[19] Информант 2: ,,Я чувствовал уверенность, что разговариваю с профессионалом своего дела.''

[20] Информант 1: ,,В ходе беседы мужчина был спокоен и убедителен, у меня не было сомнений. В середине нашей беседы мужчина сказал, что есть быстрое решение, чтобы защитить свой телефон – программа, ''Anydesk'' для защиты данных, которую нужно на телефон установить.''

[21] Информант 2: ,,Он сказал, что у них действует так же разработанная программа ''AnyDesk'', через которую они помогают новичкам делать первые инвестиции и что ее будет необходимо установить на компьютер.''

vestluse käigus kahtlustama, et midagi võib väga valesti olla, kuid üks neist avastas enda jaoks juhtunu alles järgmisel päeval.

Emotsionaalses plaanis sattusid enamus informandid paanikasse, neil tekkis hirmutunne ja nad hakkasid muretsema.

> Informant 1: „*Ma ehmusin nii palju, et mul hakkasid käed värisema kui telefon jätkas helistamist. Mees jätkas sõnumite kirjutamist mulle Viber'is.''*[22]
>
> Informant 2*:,,Ma hakkasin närveerima, sattusin paanikasse ja ei suutnud mõnda aega saada aru, mis toimub.''*[23]
>
> Informant *3: ,,Mul hakkas närvidest pea ringi käima.''*[24]
>
> Informant 6: *,,Kui vestlus lõppes ei saanud ma pikalt aru, mida ma just olin kogenud ja milleks ma neid asju kinnitasin. Ei suutnud oma peas paika panna, kellega ma suhtlesin, petturiga või pangatöötajaga.''*[25]

Tõenäoliselt, inimese seisund pärast petturitega suhtlemist ja eelnev vajalikke teadmiste puudumine küberturvalisusest mõjutasid seda, milliselt nad reageerisid pärast kahju juhtumit.

Enamus informandid üritasid esmalt võtta ühendust oma lähedastega, et küsida abi neilt või saada selgitusi selle osas, mida antud olukorras tegema peaks. Pärast nõu saamist suundusid nad oma pangakontorisse, selleks et lahendada tekkinud probleemi ja saada vajalikke instruktsioone edasisteks tegevusteks. Ainult üks informant võttis oma pangaga ühendust infoliini kaudu, kuna viibis haiglas.

> Informant 4*: „Poeg andis mulle panga telefoninumbri ja mina helistasin ning jutustasin kogu situatsiooni, mis minuga juhtus. Mulle blokeeriti, nagu ma aru sain, ligipääs panka ja samuti pangakaart ning broneeriti aeg kontorisse järgmiseks nädalaks kui haiglast välja saan, et teha vajalikke avaldusi ja taastada ligipääs internetipanka.''*[26]

[22] Информант 1: ,, Я так сильно напугалась, что у меня затряслись руки и телефон продолжал звонить. Мужчина продолжал писать мне сообщения в Viber.''

[23] Информант 2: ,, Я очень разнервничался, запаниковал и не мог понять какое-то время, что происходит.''

[24] Информант 3: ,,У меня от нервов закружилась голова.''

[25] Информант 6: ,, Когда разговор закончился я долго не могла понять, что я сейчас делала и зачем подтверждала. Я не могла уложить в своей голове, то с кем я разговаривала с мошенником или работником банка.''

[26] Информант 4: ,,Сын дал мне номер телефона банка, и я позвонила рассказала всю ситуацию, что произошло. Мне заблокировали как я поняла доступ в банк и карту и записали в контору на след. неделю, когда я уже выйду из больницы, чтобы сделать необходимые заявления и восстановить доступ в интернет-банк.''

Uurimuse käigus selgus, et enamus informandid, kes osutusid petturite ohvriks, vajasid psühholoogilist abi või nad keeldusid digilahenduste kasutamisest oma igapäevaelus.

> Informant 5: *,,Arsti juures ei käinud, kuid vist oleks vaja olnud. Abi tol hetkel ei olnud üleliigne, kuid ei tea kuhu pöördudagi, igal pool on järjekorrad ja pealegi kõik need teenused on tasulised arvatavasti.''*[27]

> Informant 4: *,,Kuna ma olin haiglas, olin võimeline ainult paluma arstidel anda mulle midagi rahustavat. Kogu see nädal olin nii mures, et puudus söögiisu.''*[28]

> Informant 2*: ,,Jah ma pöördusin oma arsti poole ja isegi palusin teda , et ta kirjutaks mulle välja rahusti, kuna ei suutnud normaalselt magada nädala jooksul. Ei saanud oma lähedastele sellest rääkida, kuna mind korduvalt hoiatati telefonipettuste osas. Mul oli ja on siiamaani raske vaatamata sellele, et ma rääkisin oma tütrele, mis oli minuga juhtunud.''*[29]

Mõned informandid eelistasid lõpetada digitaalsete seadmete igapäevase kasutuse pärast juhtunud intsidenti.

> Informant 2: „*Praeguseks olen kandnud oma kokkuhoitud raha tütrele ja palusin teda mõnda aega maksta minu kommunaalmakse. Mõnede firmadega tegin pangakontoris maksete automaatsed lepingud.''*[30]

> Informant 4: *,, Praegu teeb peamiselt kõike, mis puudutab rahalisi küsimusi, minu eest poeg - tegin pangakontoris tema nimele volikirja. Üritan eemal hoida igasuguste programmide kasutamisest telefonis, mul on juhtumist vaja aega taastuda.''*[31]

Järgmises alapeatükis teeb autor uuringu tulemuste põhjal järeldusi ja toob välja ettepanekud küberpettuste alaste teadmiste tõhusamaks levitamiseks eakate hulgas.

[27] Информант 5: ,,К врачу не ходила, но, наверное, надо было. Помощь бы в тот момент не помешала, а не знаешь куда и обращаться, везде такие очереди, да и платные, наверное, все эти услуги.''
[28] Информант 4: ,,Поскольку я находилась в больнице я лишь могла попросить врачей дать мне что-то успокоительное. Всю это неделю я так переживала, что не было даже аппетита. ''
[29] Информант 2: ,,Да, я обратился к своему врачу и даже попросил его выписать другое успокоительное, потому что не мог спать нормально в течение недели. Я не мог рассказать эту историю своим близким, ведь меня неоднократно предупреждали о телефонном мошенничестве. Мне было тяжело и тяжело до сих пор несмотря на то, что я рассказал все-таки дочери что у меня произошло.''
[30] Информант 2: ,,Вообще нет. Сейчас я перевел все сбережения дочери и попросил ее какое-то время платить за коммунальные расходы. С некоторыми фирмами сделал в конторе банка договора автоматической оплаты.''
[31] Информант 4: ,, Сейчас в основном за меня все делает сын, что касается финансовых вопросов – я оформила в конторе банка на него полную доверенность. Стараюсь сама избегать использования каких-либо программ в телефоне, нужно время отойти.''

2.5 Uuringu järeldused ning ettepanekud eakate küberpettuste ärahoidmiseks

Läbi viidud uuringu tulemused kinnitavad, et eakatel on madal teadlikkus küberturvalisusest, küberohudest ja levinud küberpettuste liikidest ning madal tehniline teadlikkus kasutatavatest digitaalseadmetest. Samuti uuringus selgus, et küberpettuste psühholoogiline mõju jätab tagajärgi, nii tervisele kui ka digitalsete seadmete edaspidisele kasutamisele igapäevaelus. Whitty (2019) ja Blackwood-Brown jt (2019) oma uurimustes viidavad, et küberkuritegevuse ohvrite sotsiaaldemograafilist profiili on vanuse ja hariduse osas väga vähe uuritud ja paljud uurimused kinnitavad, et küberpetturid on orienteeritud eakatele nagu kõige haavatavamaid internetikasutajate rühmi küberrünnakute puhul, sest ründajatel on nendega lihtne manipuleerida, mis on suuresti tingitud nende piiratud teadmistest ja oskustest küberjulgeoleku valdkonnas.

Läbiviidud uurimuse järeldused ja ettepanekud küberpettuste alase teadlikkuse täiustamiseks pangandusteenuste valdkonnas tuginevad teoreetilistele seisukohtadele ja uuringu tulemustele. Uuringu järeldused ja ettepanekud on jagatud neljaks osaks: eakate küberpettuste alase teadlikkuse tõstmine pangateenuste valdkonnas, eakate tehnilise teadlikkuse tõstmine digisedamete kasutuses, küberpettuste ohvriabi programmide väljatöötamine ning pankade klienditeeninduse mudelite muutmine ja tehnilise lahenduse väljatöötamine.

Eakate küberpettuste alase teadlikkuse tõstmine pangateenuste valdkonnas

Küberturvalisus ja küberohud on omavahel seotud, ilma üheta ei saa olla teist - küberturvalisuse teadlikkust ei ole võimalik tõsta ilma küberturvalisuse ohtudest aru saamata. Chang ja Coppel (2020) toovad esile küberturvalisuse teadlikkuse suurendamise probleemi aktuaalsust ja oletavad et uute tehnoloogiate sisseviimine ja kiire digimaailma muutumine soodustavad küberpettuste arengut. Mihaela (2020) arvates küberturvalisus - on üldine termin preventiivsete ja vastas meetmetele, mis on koondatud konfidentsiaalsusel, terviklikkusel ja informatsiooni kättesaadavusel, mitte potentsiaalsetel haavuvustel. Zakira ja Zainal (2019) kinnitavad, et küberohud ja küberrünnakud muutuvad keerulisteks ja hävitatavateks puudutates kõiki sektoreid. Sebai, Harjan jt (2020) arvates finants tehnoloogiad muutuvad tähtsamateks ja turvaliste küberturvalisuse mehhanismide vajadus suureneb. Autori läbiviidud läbi viidud rakendusuuringu tulemuste põhjal saab kinnitada, et küberturvalisuse olukordade mõistmiseks ja otsuste vastuvõtmiseks eakad toetuvad oma nooremate lähedastele, kuulavad nende soovitusi.

Wang et al. (2021: 2) väidavad oma uurimustes, et küberohusi võib vaadata kui küberpettuste liiki, mille rakendamisel küberkuritegija kasutab ära inimese haavatust mõjutamisega , veenmisega, kelmuslike tegevustega, manipuleerimise eesmärgiga omandada vajaliku informatsiooni. Leonov, Vorobyev jt (2019: 2) arvates sotsiaalse manipulatsiooni rünnakud põhinevad inimesest informatsiooni kogumisel isiklikul vestlusel, elektronpostil või teise suhtlemiskanalil. Autori läbiviidud uuringute tulemuste põhjal saab järeldada, et petturid edukalt kasutavad ära sotsiaalse manipuleerimise meetodid telefoni kõnede kaudu, kasutades eakate haavatust, sest esitlevad ennast usaldusväärsete organisatsioonide, antud juhul konkreetseete pankade, erinevate ametnikena, ametlike esindajatena. Olles harjunud oma panku usaldama, langevad eakad pettuse ohvriks.

Selleks, et täiustada eakate küberpettuste alane teadlikkust on vaja kompleksselt lähineda küberturvalisuse teemale - arusaamiselt kuni igapäevaelus rakendamiseni, nii panganduse sektorites kui ka teistes kasutamise harudes. Peamiselt, on vaja väljatöötada küberturvalisuse informeerimise ja teadlikkuse suurendamise programme, individuaalsete koolituse läbiviimise kujul, et informatsioon oleks kättesaadav lihtsate sõnadega, vältides rasket terminoloogiat ja kinnitades näidetega elust, mis soodustab kvaliteetsemat tajumist. Eakad inimesed peavad aru saama, kuidas mitte sattuda küberkelmide nõksudesse ja omama teadmist tegevuste järjekorrast juhul kui langesid pettuste ohvriks. Selleks on vaja luua vastavad koolituskavad ja materjalid ning valmistada ette koolitajad-nõustajad. Eesti Pangaliit võiks sellega hakkama koostöös kohalike omavalitsusega ja rahvaülikoolidega.

Eakate tehnilise teadlikkuse tõstmine digisedamete kasutuses

Juarez jt (2018) märgivad, et eakate elanikkond demonstreerib aktiivset soovi tutvustada uusi internetitehnoloogiaid, ning leitakse, et eakad on üks kõige haavatavamaid Interneti-kasutajaid küberrünnakute puhul ja Morisson ja Benjamin (2020) rõhutavad oma uuringus inimeste tugistruktuuride kaotust, kui varem omandatud küberturvalisuse alased teadmised muutuvad vananenuks ning uute teadmiste omandamine ja kohanemine muutustega toob vanematele inimestele kaasa riskantseid otsuseid, kuna tugineb vananenud arusaamadele. Hijji ja Alam (2021) kinnitavad, et tehnilised ja sotsiotehnilised manepileerimisründe liikid kasutavad ründajad, et koguda vajalikku teavet ja suurendada eduka küberrünnaku võimalusi.

Käesoleva autori uurimuse andmete alusel kasutavad eakad inimesed pangatehingute teostamiseks kaasaegseid lahendusi rakenduste ja veebilehtede näol arvutis ja telefonis.

Sagedased on kommunaalteenuste eest maksmine ja ka teised ülekanded. Eakad kasutavad tänapäeva suhtluskanaleid ja veebis ostlemise võimalusi, et mitte tunda end isoleerituna ühiskonnast ja lähedastest. Uuringu tulemustest selgus, et eakatel on head digioskused, aga nad kardavad kui juhtuvad tehniilised tõrkeid digitaalsete seadmete kasutusel ja seadmete küberhügieen on üsna madalal tasemel, kui nad edastavad petturitele isiklikud ja konfedetsiaalsed andmed ning esitavad sissepääse oma seadmetele kaugjuhtimise programmi paigaldamise kaudu. Nagu näitab uurimus loodavad enamus eakaid probleemide tekkimisel arvutis, telefonis või tahvelarvutis lähedaste abile ning ainult mõningad neist pöörduvad abi saamiseks spetsialiseeruvate firmade poole.

Autori arvates, et eakate tehnilise teadlikkuse tõstmiseks digisedamete kasutuses on vaja arendada kanaleid, kuhu eakad inimesed saavad pöörduda abi saamiseks individuaalsete konsultatsioonide näol järgnevatel teemadel:

- seadme tarkvara uuendamine (rakendused, veebibrauser);
- viirusetõrje programmide paigaldamine ja seadistamine arvuti kaitseks;
- seadmete küberhügieen (ohutute paroolide kasutamine, failide ja andmete ohutus seadmes ja informatsiooni konfidentsiaalsus).

Tehniline ja informatiivne toetus aitab eakatel elanikel töötada välja tegevusplaani, mida on vaja teha isikliku informatsiooni ja finantsinformatsiooni kaitseks, arvuti või mobiiltelefoni kasutamise ajal, et vältida kaasaegseid küberohtusid.

Küberpettuste ohvriabi programmide väljatöötamine

Cross (2020) oletab, et küberpettuste sihipärilik huvi eakate vastu on otse seotud kognitiivsete protsesside kahanemisega, nagu näiteks vaimuannete halvenemine, oletatavate rahaliste kogumuste kütkestavus, sotsiaalsed põhjused, nagu näiteks üksindus. Alapeatükkis 1.4 teoreetilises osas ,,Küberpettuste psühholoogilised meetodid,, uurimus Alkis ja Temizel (2015) и Li jt (2020) viidab enamikule mõjutamise printsiibidele, rünnaku meetoditele ja inimeste haavavustele, millele toetuvad küberrünnakud sotsiaalse manipuleeritavuse. Washo (2021) kinnitab, et veenmise meetodid avaldavad tugevat mõju ründava ja ohvri vahel, mis omab kinnitust Montanez jt (2020) uurimuses, kus tõekspidamine ilmneb, nagu küberturvalisuse kognitiivse psühholoogia võtme mõiste, mis on vajalik käitumise ja inimlikke tunnete arusaamiseks. Leonov, Vorobyev et al. 2019: 2 kinnitavad, et manipuleeritakse inimloomusega, kasutades ära selliseid omadusi nagu ahnus, hirm, kiirustamine ja kergemeelsus, et saada ohvrilt vajalikku teavet või tekitada teatud kahju.

Autori arvates on vaja tegema rohkem sihipärast teavitust eakatele sobivatel viisidel, sest eakad kipuvad rohkem petturite psühholoogilistele manipulatsioonidele alistuma. Rakendusuuringu tulemuste põhjal selgus, et enamik neist vajaks pärast petturitega kokkupuutumist psühholoogilist abi ning nad eelistasid lõpetada pankade digiteenuseid kasutamist.

Autori arvates on vaja psühholoogiliste tugiprogrammide väljatöötamine küberpettuste ohvritele, kuhu kaasata koolitatud spetsialistid nendele inimestele abi osutamiseks, kes on langenud küberpettuste ohvriks. Esiteks seetõttu, et osutada psühholoogilist abi neile. Teiseks, et rünnaku ohvrid ei muudaks oma digitaalsete seadmete kasutamisharjumust ning ühtlasi oma edasist digitaalsete seadmete oskuste arendamist, mis nagu uurimus näitas, kergendab elu paljudele. Digitaalne kasutusoskus lihtsustab elu mitte ainult finantsiliste seadmete kasutamise valdkonnas, kuid ka kommunikatsioonis (rakenduste kasutamine suhtlemiseks) ning ostude tegemises (internetis tehtavad ostud). Eesti Pangaliit võiks seda korraldada koostöös asutustega, kes pakkuvad psühholoogilise või kriisiabi eakatele.

Pankade klienditeeninduse mudelite muutmine ja tehnilise lahenduse väljatöötamine

Uuringu tulemuste põhjal järeldas autor, enamikus pettusejuhtumites tutvustasid küberkurjategijad end ametliku esindajana, kasutades telefonikõnes eelkõige veenmise oskust. Enamikus juhtumites tuvastasid petturid end pangatöötajana. Pankadele võib soovitada muuta klienditeeninduse mudelit ja vähendada omal algatusel tehtavaid telefonipäringuid klientidele, paludes näiteks klientidel vajadusel endal pangaga telefonitsi ühendust võtta panga avalikul telefoninumbril. See suurendab pangatöötajate töökoormust, ent võib-olla õigustab see ennast, tõstes pankade usaldusväärsust. Teadaolevalt teevad pangandustöötajad ise aktiivselt telefoni teel erinevaid kõnesid, eesmärgiga edastada kliendile vajalikku teavet. Selletõttu võib vastava skeemi tõhusus olla selle taga, et inimesed, tundes hirmu ja segadust, ei suuda aru saada, kellega nad tegelikult räägivad, kas siis pangatöötajaga või petturiga.

Uuring näitas, et enamik eakaid kasutavad telefonis pangandusteenuseid ja nende digitaalsed oskused on piisavalt head. Autori arvates võib pankadele teha ettepaneku töötada välja oma mobiilirakenduste kaudu tehniline lahendus, mis saaks petturitelt saadud kõnesid telefoninumbri järgi filtreerida. Nii ei jõua petukõned abonentideni. Selleks on vaja luua petturite telefoninumbrite andmebaas koos politsei ja küberkaitse osakonnaga, et pidevalt uuendada ja täiendada numbritest koosnevat andmebaasi. Selline lahendus annab inimestele turvatunde pangandusteenuste kasutamisel ning aitab vähendada küberohtude riske.

KOKKUVÕTE

Küberturvalisus, sealhulgas panganduspettused, on muutunud oluliseks teemaks pangandusteenuste valdkonnas, sest see puudutab inimeste vara. Kui pangateenused on liikunud digitaalsete kanalite suunas, on ka petturid hakanud tegutsema uutel viisidel, nagu investeerimispettused, pettukõned ja sõnumid.

Lõputöö teema aktuaalsus seisnes selles, et viimastel aastatel on märkimisväärselt kasvanud digitaalsete teenuste kasutamine pangandussektoris, eriti eakate inimeste seas, kes hakkasid uute tehnoloogiate ja teenuste kättesaadavuse tõttu rohkem huvi nende kasutamise vastu tundma.

Eesti Pangaliit korraldab sotsiaalseid infokampaaniaid küberturvalisuse teemadel, et ennetada küberpettusi, sest organisatsiooni eesmärgiks on toetada ja tõhustada inimeste informeeritust ning teadlikkust küberkuritegevuse teemadest. Infokampaaniad on suunatud valdavalt eakatele Eesti elanikele, kelle emakeeleks on vene keel. Nemad on pangandus- ja investeerimispettuste suhtes kõige haavatavamad ja vähem informeeritud pettuste ulatusest ning sellest, kuidas õigesti käituda, kui kokkupuude küberpettusega on ilmnenud.

Lõputöö eesmärk oli teha kindlaks küberpettuste alane teadlikkus Ida-Virumaa vene keelt kõnelevate eakate seas ning teha ettepanekuid, kuidas neid paremini kaitsta küberpettuste eest.

Lõputöö koosneb inglisekeelsest resümeest, sissejuhatusest, teoreerilisest osast, rakenduslikust osast, kokkuvõttest, kirjanduse loetelust 64 allikatest ning kahest lisadest.

Lõputöö teoreetilises osas määratles autor küberohtude ja küberturvalisuse olemust ning nende omavahelist seost. Analüüsiti peamised ja tänapäeval kõige levinumad küberpettuste liigid. Selgitati küberpettuste psühholoogilisi manipuleerimisründe meetodeid ja mõjutamismehhanisme ning eakate teadlikkust mõjutatavaid tegureid küberturvalisuse vallas. Teoreetiline käsitlus tugineb peamiselt Leonovi, Changi, Zakira, Wangi ja Washo töödele. Lõputöö praktilises osas iseloomustas autor Ida-Virumaa küberpettuste keskkonna ning moodustas uuringu läbiviimiseks kogumi ja valimi. Uuringu teostamiseks kasutas autor sobivat metoodikat, misjärel saadud andmed analüüsiti, et teha järeldusi ja ettepanekuid.

Autor viis läbi ekspertintervjuu Eesti Pangaliidu esindajaga ning kasutatas kogumi moodustamisel nende küberturvalisuse infokampaania uuringu andmeid. Autor kasutas

mugavusvalimi meetodid intervjuus osalejate valiku tegemisel.Valimisse kuulus 6 kuus inimest, kes oli valitud kindlate tunnuste kohaselt. Intervjuud toimusid ajavahemikul 07. - 27. märts 2022.

Intervjuu käigus esitatud avatud küsimustele saadud vastused sisestati tabelisse. Need andmed kodeeriti ja seejärel koodid grupeeriti ning moodustati kategooriad, mille alusel kogutavad andmed esitati järgmiste teemade kaupa:

- informatsiooni saamise allikad küberturvalisuse, küberohtude ja levinud finantspettuste liikidest,
- digitaalsete tehnoloogiate kasutamine igapäevaelus, oskuste ja tehniliste kompetentside hindamine,
- küberpettuste liigid, esmane kontakt ohvriga,
- küberpettuse korral ohvrile mõju avaldamise meetodid,
- tagajärjed ja tegevused küberpettuste kahju korral.

Toetudes teoreetilistele mitmete autorite seisukohtadele, kellest peamised on Chang ja Coppel, Mihaela, Zakira ja Zainal, Sebai, Wang, Leonov, Juarez, Hijji ja Alam, Cross, Alkiz ja Temizel, Li, Washo, Montanez ja läbiviidud uuringu tulemustele koostas autor ettepanekud eakate küberpettuste alase teadlikkuse täiustamiseks pangandusteenuste valdkonnas ning kaitseks küberkuritegevuse eest. Uuringu järeldused ja ettepanekud on jagatud neljaks osaks: eakate küberpettuste alase teadlikkuse tõstmine pangateenuste valdkonnas, eakate tehnilise teadlikkuse tõstmine digisedamete kasutuses, küberpettuste ohvriabi programmide väljatöötamine ning pankade klienditeeninduse mudelite muutmine ja tehnilise lahenduse väljatöötamine.

Uuringute tulemuste põhjal saab järeldada, et petturid edukalt kasutavad ära sotsiaalse manipuleerimise meetodid telefoni kõnede kaudu, kasutades eakate haavatust, sest esitlevad ennast usaldusväärsete organisatsioonide, antud juhul konkreetseete pankade, erinevate ametnikena, ametlike esindajatena. Olles harjunud oma panku usaldama, langevad vanurid pettuse ohvriks.

Läbi viidud uuringust selgus, et küberturvalisuse olukordade mõistmiseks ja otsuste vastuvõtmiseks eakad toetuvad oma nooremate lähedastele, kuulavad nende soovitusi. Selleks, et täiustada eakate küberpettuste alane teadlikkust on vaja töötada välja ja pakkuda küberturvalisuse koolitusi ja informeerimise programme, kus eakad saavad vahetult osa võtta. Samuti tuleks võimaldada individuaalseid konsultatsioone, et informatsioon oleks kättesaadav lihtsas sõnastuses, vältides keerulist teitedrminoloogiat, tuues näited elust

enesest, mis soodustab vajalike teadmiste omandamist. Selleks on vaja luua vastavad koolituskavad ja materjalid ning valmistada ette koolitajad-nõustajad. Eesti Pangaliit võiks sellega hakkama koostöös kohalike omavalitsusega ja rahvaülikoolidega.

Uuringu tulemustest selgus, et eakatel on head digitaalsed oskused, kuid nad kardavad digitaalsete seadmete kasutusel tekkivaid tehnilisi tõrkeid ja nende küberhügieen on üsna madalal tasemel. Nad edastavad petturitele isiklikke ja konfidentsiaalseid andmeid ning annavad ligipääsu oma seadmetele kaugjuhtimise programmi paigaldamise kaudu. Nagu näitab uurimus, loodavad enamus eakaid arvutis, telefonis või tahvelarvutis tekkinud probleemide lahendamisel lähedaste abile ning ainult mõningad neist pöörduvad abi saamiseks spetsialiseerunud ettevõtete poole. Autori arvates on eakate tehnilise teadlikkuse tõstmiseks digiseadmete kasutusel vaja tugikanalite arendamist ehk asukohti, kuhu eakad inimesed saavad individuaalsete konsultatsioonide saamiseks pöörduda ja kus nad saavad abi järgnevalt nimetatud teemadel: seadme tarkvara uuendamine, viirusetõrje programmide paigaldamine ja seadistamine ning seadmete küberhügieeni alane konsultatsioon.

Lõputöö autor on arvamusel, et tehniline ja informatiivne toetus aitab eakatel elanikel välja töötada kasulikku tegevusplaani ja aitab mõista, mida tuleb teha arvuti või mobiiltelefoni kasutuse ajal, et tagada oma isikliku informatsiooni ja finantsinformatsiooni kaitse ning seeläbi vältida tänapäevaseid küberohtusid.

Uuringu käigus selgus, et eakad kipuvad petturite psühholoogilistele manipulatsioonidele alistuma. Enamik neist vajaks pärast petturitega kokkupuutumist psühholoogilist abi ning nad eelistasid lõpetada digitaalsede seadmete igapäevast kasutamist. Seepäst on vajalik küberpettuste ohvriabi programmide väljatöötamine, kuhu kaasata koolitatud spetsialistid nendele inimestele abi osutamiseks, kes on langenud küberpettuste ohvriks. Esiteks selleks, et anda ohvritele psühholoogilist abi, mis aitaks taastada nende emotsionaalne ja tervislik heaolu pärast juhtumit. Teiseks, et säilitada nende digitaalsete seadmete edasine kasutamine korrektses võtmes. Kolmandaks, et vältida kahju tekkimist võimalike järelkontaktide kaudu, mida petturid võivad püüda teha. Eesti Pangaliit võiks seda korraldada koostöös asutustega, kes pakkuvad psühholoogilise või kriisiabi eakatele.

Uuringu tulemuste põhjal järeldas autor, et enamikus pettusejuhtumites tutvustasid küberkurjategijad end pangatöötajana, kasutades telefonikõnes eelkõige veenmise oskust. Pankadele võib soovitada muuta klienditeeninduse mudelit ja vähendada omal algatusel tehtavaid telefonipäringuid klientidele, paludes näiteks klientidel vajadusel endal pangaga

telefonitsi ühendust võtta panga avalikul telefoninumbril. See suurendab pangatöötajate töökoormust, ent võib-olla õigustab see ennast, tõstes pankade usaldusväärsust. Teadaolevalt teevad pangandustöötajad ise aktiivselt telefoni teel erinevaid kõnesid, eesmärgiga edastada kliendile vajalikku teavet. Selletõttu võib vastava skeemi tõhusus olla selle taga, et inimesed, tundes hirmu ja segadust, ei suuda aru saada, kellega nad tegelikult räägivad, kas siis pangatöötajaga või petturiga.

Uringust selgus, et enamik eakaid kasutavad telefonis pangateenuseid ja nende digitaalsed oskused on pidevalt head. Autori arvates võib soovitada pankadele välja töötada oma mobiilirakendusele tehniline lahendus, mis saaks petturitelt saadud kõnesid telefoninumbri järgi filtreerida. Nii ei jõua petukõned abonentideni. Selleks on vaja luua petturite telefoninumbrite andmebaas koos politsei ja küberkaitse osakonnaga, et pidevalt uuendada ja täiendada numbritest koosnevat andmebaasi. Selline lahendus annab eakatele turvatunde pangandusteenuste kasutamisel ning aitab vähendada küberohtude riske.

Lõputöös esitatud järelduste arvestamine küberpettuste ennetamisel ning ettepanekute rakendamine aitab kaasa vene kodukeleega eakate kaitsmisele küberpettuste eest.

KASUTATUD KIRJANDUS

Chang, L., Coppel, N. (2020) Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security.* Available at https://doi.org/10.1016/j.cose.2020.101959, acessed 1 Detsember 2021

Mihaela, C.-L. (2020) Current Security Threats in The National and International Context. *Journal of Accounting and Management Information Systems*. Vol. 19, No. 1, pp. 351-378. DOI:http://dx.doi.org/10.24818/jamis.2020.02007

Janssen, M., Bruijn, H. (2017) Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly.* Vol. 34, Issue 1, pp. 1-7. Available at https://doi.org/10.1016/j.giq.2017.02.007, acessed 4 Detsember 2021

Pernik, P. (2017*) Cybersecurity education in Estonia: building competences for internal security personnel*. Proceedings Estonian Academy of Security Sciences, 18 : Security: from corner to corner, pp. 71-108. Avaiable at https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2301/Proceedings%202019_web.pdf?sequence=1&isAllowed=y acessed 2 Detsember 2021

Harjan, A. S.; Sebai, M. et al. (2020) *Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks.* International Journal of Research in Business and Social Science. Istanbul Vol. 9, Iss. 6, pp. 123-133. DOI:10.20525/ijrbs.v9i6.914

Narmatha, C. (2020) *Advancements, Merits & Demerits of Cyber Security: A Critical Study*. IEEE. DOI: 10.1109/ICCIT-144147971.2020.9213774

Homburger, Z. (2019) *The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace.* Global Soc., 33 (2) (2019), pp. 224-242. DOI: 10.1080/13600826.2019.1569502

Zakaria, N.; Zainal, A. et al. (2019) *Feature Extraction and Selection Method of Cyber-Attack and Threat Profiling in Cybersecurity Audit.* International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 2019, pp. 1-6. DOI: 10.1109/ICoCSec47621.2019.8970786

Bayard, E. (2019) The Rise of Cybercrime and the Need for State Cybersecurity Regulations. Rutgers Computer & Tech. LJ, Vol. 45, pp. 69-95. Avaiable at https://law-

journals-books.vlex.com/vid/the-rise-of-cybercrime-869427566 acessed 18 Detsember 2021

Li, Y., Liu, Q. (2021) *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*. Energy Reports (IF6.87), Vol. 7, pp. 8176-8186. DOI: 10.1016/j.egyr.2021.08.126

Sajal, S.; Jahan, I. et al. (2019) *A Survey on Cyber Security Threats and Challenges in Modem Society*. Conference: 2019 IEEE International Conference on Electro Information Technology (EIT), Vol. 6, pp.525-528. DOI:10.1109/EIT.2019.8833829

Halouzka, K.: Burita, L. et al. (2021) Overview of Cyber Threats in Central European Countries. Conference: 2021 Communication and Information Technologies (KIT). DOI: 10.1109/KIT52904.2021.9583621

Bobric, D-G. (2020) *Study Regarding the Cyber Threats to the National Security*. Journal: Scientific Bulletin, Vol. 25, pp. 18-25. DOI:https://doi.org/10.2478/bsaft-2020-0003

Kettani, H.; Wainwright, P. et al. (2019) On the Top Threats to Cyber Systems. 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Vol. 34. pp 175-179. DOI: 10.1109/INFOCT.2019.8711324

Sagiroglu, S.; Bilgehan, A. et al. (2019) Fighting with Cyber Terror and Terrorism: Threats and Precautions. In 2019 4th International Conference on Computer Science and Engineering (UBMK). IEEE, 2019. pp. 239-244. DOI: 10.1109/UBMK.2019.8907049

Ali, M.A., Azad, M.A. et al. (2019) *Consumer-Facing Technology Fraud: Economics, Attack Methods and Potential Solutions*. Future Generation Computer Systems, 100, pp. 408-427. DOI: 10.1016/j.future.2019.03.041

Wang, Z., Zhu, H. et al. (2021) *Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods.* School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China. IEEE Access. Vol. 9, pp.11895 - 11910. DOI: 10.1109/ACCESS.2021.3051633

Leonov, P. Y.; Vorobyev, A. V. et al. (2019) *The Main Social Engineering Techniques Aimed at Hacking Information Systems.* 2021 Ural Symposium on Biomedical Engineering,

Radioelectronics and Information Technology (USBEREIT). Yekaterinburg, Russia. DOI: 10.1109/ICRITO48877.2020.9198032

Hijji, M., Alam, G. (2021) *A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions*. Industrial Innovation and Robotics Center, University of Tabuk. IEEE Access. Vol.9, pp.7152 - 7169. DOI:10.1109/ACCESS.2020.3048839

Mattera, M., Chowdhury, M. MD. (2021) *Social Engineering: The Looming Threat*. 2021 IEEE International Conference on Electro Information Technology (EIT). East Stroudsburg, PA. pp. 56-61 DOI: 10.1109/EIT51626.2021.9491884

Wokabi, F. M. (2019). *Employee awareness on social engineering threats in the financial sector*. Faculty of Information Technology (FIT). Strathmore University. Avaiable at http://su-plus.strathmore.edu/handle/11071/6784, acessed 20 Detsember 2021

Asani, O. E.; Omotosho, A. et al. (2021) A maximum entropy classification scheme for phishing detection using parsimonious features. TELKOMNIKA Telecommunication, Computing, Electronics and Control. Oct 2021, Vol. 19 Issue 5, p1707-1714. 8p. DOI: 10.12928/TELKOMNIKA.v19i5.15981

Huseynov, F., Köse, B.Ö. (2021) *The Inclination of the Internet Users to Be Deceived By Social Engineering Attacks in Different Sectors.* In International Conference on Multidisciplinary Studies, Ankara, Turkey, 23-24 September. pp. 174-180. DOI: 10.3390/fi11040089

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020) *E-Fraud in Nigerian Banks: Why and How?*. Journal of Financial Risk Management, 9, 211-228. DOI: 10.4236/jfrm.2020.93012.

Li, T., Wang, X., Ni, Y. (2022) *Aligning social concerns with information system security: A fundamental ontology for social engineering*. Information Systems. Beijing University of Technology, China. Vol. 104. pp. 2-13. DOI: 10.1016/j.is.2020.101699

Boukari, B. E., Ravi, et al. (2021) *Machine Learning Detection for SMiShing Fraud*. 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). Las Vegas, NV, USA. DOI: 10.1109/CCNC49032.2021.9369640

Ahad Ahadi, S. A., Rakesh, N. at al. (2020) *Overview On Public Wi-Fi Security Threat Evil Twin Attack Detection.* 2020 IEEE International Conference on Advent Trends in

Multidisciplinary Research and Innovation (ICATMRI).Buldhana, India. pp 1-6. DOI:10.1109/ICATMRI51801.2020.9398377

Balim, C., Gunal, E. S. (2019) *Automatic Detection of Smishing Attacks by Machine Learning Methods*. 2019 1st International Informatics and Software Engineering Conference (UBMYK). Ankara, Turkey. DOI: 10.1109/UBMYK48245.2019.8965429

Park, G., Rayz, J. (2018*) Ontological Detection of Phishing Emails*. 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC).Miyazaki, Japan. pp. 2858 - 2863. DOI: 10.1109/SMC.2018.00486

Gupta, S., Bhattacharya, A. at al. (2021) *Analysis of Social Engineering Attack on Cryptographic Algorithm*. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). Amity University, Noida, India. pp.1 - 4. DOI: 10.1109/ICRITO51393.2021.9596568

Sharevski, F., Jachim, P. (2021) *Alexa in Phishingland: Empirical Assessment of Susceptibility to Phishing Pretexting in Voice Assistant Environments*. 2021 IEEE Security and Privacy Workshops (SPW). San Francisco, CA, USA. pp. 207 - 213. DOI: 10.1109/SPW53761.2021.00034

Montaтez, R., Golob, E., at al. (2020) *Human Cognition Through the Lens of Social Engineering Cyberattacks*. Frontiers in psychology, 11, 1755. DOI: 10.3389/fpsyg.2020.01755.

Washo, A. H. (2021) *An interdisciplinary view of social engineering: A call to action for research.* Computers in Human Behavior Reports, 2021. Marywood University, USA. Vol.4. pp. 1 - 8. DOI:10.1016/j.chbr.2021.100126

Norris, G., & Brookes, A. (2021) *Personality, emotion and individual differences in response to online fraud.* Personality and Individual Differences, 109847. Department of Psychology, Aberystwyth University, Penglais Campus, Aberystwyth, U.K. Vol. 169. pp. 1 - 7. DOI:10.1016/j.paid.2020.109847

Alkis, N., Temizel, N. A. (2015) *The impact of individual differences on influence strategies*. Personality and Individual Differences. Department of Information Systems,

Informatics Institute, Middle East Technical University, Ankara, Turkey. Vol. 87. pp. 147-152. DOI: 10.1016/j.paid.2015.07.037

Li, M. (2021) *Environmental factors affect social engineering attacks.* Department of Computer and Information Technology West Lafayette, Indiana. pp 1-61. Avaiable at https://hammer.purdue.edu/articles/thesis/ENVIRONMENTAL_FACTORS_AFFECT_SOCIAL_ENGINEERING_ATTACKS/14810529/1, acessed 21 Detsember 2021

Kilby, L., Lennon, H. (2021) *When words are not enough: combined textual and visual multimodal analysis as a Critical Discursive Psychology undertaking*. Methods in Psychology. Vol. 5. pp. 1-9. DOI: 10.1016/j.metip.2021.100071

Chen, J. (2021) *"You are in Trouble!": A Discursive Psychological Analysis of Threatening Language in Chinese Cellphone Fraud Interactions*. International Journal for the Semiotics of Law - Revue international de Smartitude judicious, vol. 34, no. 4, pp. 1065–1092. DOI:10.1007/s11196-020-09765-y

Whitty, M.T. (2019). *Predicting susceptibility to cyber-fraud victimhood*. Journal of Financial Crime: 26(1), 277-292. Available at https://doi.org/10.1108/JFC-10-2017-0095, acessed 15 Detsember 2021

Blackwood-Brown C, Levy Y, D'Arcy J. (2019) *Cybersecurity awareness and skills of senior citizens: a motivation perspective*. J Comput Inf Syst. 2021;61(3):195–206. DOI: 1080/08874417.2019.1579076.

Cross, C. (2021) *Theorizing the impact of COVID-19 on the fraud victimization of older persons.* The Journal of Adult Protection, Vol. 23 No. 2, pp. 98-109. Available at https://doi.org/10.1108/JAP-08-2020-0035, acessed 17 Detsember 2021

Rodrigo Juárez, M. A., González, V. M., Favela, J. (2018) *Effect of technology on aging perception*. Health Informatics J. 2018 Jun; 24(2): 171-181. DOI:10.1177/1460458216661863

Morrison, Benjamin A., et al. (2020) *Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults*. Frontiers in Psychology. DOI: 10.3389/fpsyg.2020.00623

Norris, G., Brookes, A & Dowell, D. (2019) *The psychology of internet fraud victimisation : a systematic review*. Journal of Police and Criminal Psychology, vol. 34, no. 3, pp. 231-245. DOI: 10.1007/s11896-019-09334-5

Kaitsepolitsei aastaraamat 2020–2021 (2021) *Küberjulgeoleku tagamine.* https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat-2020-2021.pdf (viimati vaadatud 01.02.2022)

RIA (2022) Küberturvalisuse aastaraamat 2022. https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_kyberturvalisuse_aastaraamat_2022_est_veeb.pdf (viimati vaadatud 05.02.2022)

Ida-Viru Maakonna Arengustrateegia 2019 – 2030 (2019) https://ivol.ee/documents/9867329/19704180/Ida-Viru+arengustrateegia+kinnitamiseks.pdf/1217950d-b837-4d85-aa25-9f1897368d91 (viimati vaadatud 25.02.2022)

Lepik, K.; Harro-Loit, H. jt. (2014) Intervjuu. Sotsiaalse analüüsi meetodite ja metodoloogiate õpibaas. Tartu Ülikool. http://samm.ut.ee/intervjuu (viimati vaadatud 02.03.2022)

Kalmus V., Masso A. jt. (2015). Kvalitatiivne sisuanalüüs. Sotsiaalse analüüsi meetodite ja metodoloogiate õpibaas. Tartu Ülikool. http://samm.ut.ee/kvalitatiivne-sisuanalyys (viimati vaadatud 05.03.2022)

Laherand, M. L. (2008). Kvalitatiivne uurimisviis. Tallinn: M.-L. Laherand.
Strömpl, J. (2014) *Juhtumiuurimus.* Tartu: Tartu Ülikool http://samm.ut.ee/juhtumiuuri-mus (viimati vaadatud 06.03.2022)

Flick, U. (2019) *An introduction to qualitative research*. SAGE, 4th Edition. London. pp.171-175 DOI:10.14483/23464712.15330

Rämmer, A. (2014) Valimi moodustamine. Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas. Tartu: Tartu Ülikool http://samm.ut.ee/valimid (viimati vaadatud 06.03.2022)

ÕIGUSAKTID

Hädaolukorra seadus (2017) RT I, 2017 https://www.riigiteataja.ee/akt/117052020003 (viimati vaadatud 10.12.2021)

Küberturvalisuse seadus (2018) RT I, 2018 https://www.riigiteataja.ee/akt/122052018001 (viimati vaadatud 11.12.2021)

ANDMED

Eesti Pangaliidu veebileht 2022 https://www.pangaliit.ee/et

Justiitsministeeriumi veebileht 2022 https://www.just.ee/

Politsei- ja Piirivalveamet veebileht 2022 https://www.politsei.ee/index.html

Swedbank AS veebileht 2022 https://swedbank.ee/private

AS SEB pank veebileht 2022 https://www.seb.ee/

Coop Pank AS veebileht 2022 https://www.cooppank.ee/

Statistikaameti veebileht www.stat.ee.

RIA veebileht https://www.ria.ee/

Norstat Eesti (2021) Kampaania eelne uuring. Eesti Pangaliit.

LISAD

LISA 1. INTERVJUU KÜSIMUSED

Hea Ida-Viru elanik!

Tänan Teid nõusoleku eest anda intervjuu. Intervjuu kestab umbes 40 minutit. Vajadusel saame Teie soovi korral 5 minutit pausi teha.

Olen Tartu Ülikooli Narva Kolledži üliõpilane ja palun Teie abi lõputöö kirjutamisel ja andmete kogumisel.

Lõputöö raames viin läbi uurimist teemal „Küberpettuste alane teadlikkus pangateenuste valdkonnas Ida-Virumaa eakate näitel''. Intervjuu viiakse läbi Ida-Viru vene keelt kõnelevaid eakate elanike seas, kes kasutavad aktiivselt pangateenuseid ja muid internetivõimalusi seoses digitaalkanalite kiire kasvuga, kaotasid oma raha küberkuritegevusest või jäid viimase kahe aasta jooksul ohvriks pettuste kavadele pangateenuste valdkonnas.

Intervjuu on anonüümne ja selle käigus kogutud andmeid ei seostata Teie isikuga. Andmeid ja tehinguid, mis on seotud kodupangandusteenustega, sealhulgas kontojäägid, kontoväljavõtted, pangakaartide liik ja andmed, sisselogimise autentimise vahendid jne, ei täpsustata intervjuu käigus. Kas te annaksite nõusoleku intervjuu salvestamiseks? Intervjuu salvestus transkribeeritakse ehk salvestatakse vastused tekstina ja salvestus hävitatakse.

Aitäh!

1) Millistest allikatest saate Teie infot küberturvalisuse, küberohtude ja kõige levinumate finantspettuste kohta?
Из каких источников Вы получаете информацию о кибербезопасности, киберугрозах и наиболее распространённых схемах финансового мошенничества?

2) Milliseid internetipanga teenuseid või muid digitaalseid lahendusi, programme või rakendusi olete viimase kahe aasta jooksul oma igapäevaelus kasutanud? Millisel eesmärgil?
Какие виды услуг интернет-банкинга или других дигитальных решений, программы или приложения Вы используете в повседневной жизни в течение последних двух лет? Для каких целей?

3) Kuidas Te hindate oma arvuti või telefoni digitaalset oskust ja kuhu pöördute tehniliste probleemide või raskuste ilmnemisel?
Как Вы оцениваете свои навыки работы на компьютере или телефоне и куда вы обращаетесь при возникновении технических проблем или трудностей?

4) Kuidas Te sattusite küberpettuste ohvriks ja kuidas tekkis esmane kontakt petturitega?
Как Вы стали жертвой мошенников и каким образом произошел первоначальный контакт?

5) Millist isiklikku teavet Te petturitele vestluse ajal edastasite ja mis teie otsust mõjutas?
Какую личную информацию во время разговора с мошенниками Вы предоставили и что повлияло на это решение?

6) Milliseid emotsioone või tundeid Te petturitega suheldes kogesite?
Какие эмоции Вы испытывали или как себя чувствовали во время общения с мошенниками?

7) Miks ja millisel hetkel Te taipasite, et Teid petetakse?
Почему и в какой момент Вы осознали, что вас обманывают?

8) Millised tegevused järgnesid pettusekahtlusekorral, kui kiiresti ja kuhu Te abi saamiseks pöördusite?
Какие действия последовали в случае мошенничества, как быстро и куда Вы обратились за помощью?

9) Kas pärast Teiega juhtunut vajasite psühholoogilist abi või muud abi? Kuhu Te pöördusite probleemi lahendamiseks?
Требовалась ли Вам психологическая помощь или другая иная поддержка после случившегося инцидента? Куда вы обращались за решением проблемы?

10) Kas Te jätkate digitaalteenuste kasutamist oma igapäevaelus? Mis õppetunni olete enda jaoks õppinud ja mida saate ise teha, et seda olukorda tulevikus vältida?
Продолжаете ли Вы использовать дигитальные услуги в повседневной жизни? Какой урок вы для себя извлекли и что могли бы сделать, чтобы предотвратить эту ситуацию в будущем?

LISA 2. EAKATE VASTUSED INTERVJUU KÜSIMUSTELE

	Millistest allikatest saate Teie infot küberturvalisuse, küberohtude ja kõige levinumate finantspettuste kohta?	Milliseid internetipanga teenuseid või muid digitaalseid lahendusi, programme või rakendusi olete viimase kahe aasta jooksul oma igapäevaelus kasutanud? Millisel eesmärgil?	Kuidas Te hindate oma arvuti või telefoni digitaalset oskust ja kuhu pöördute tehniliste probleemide või raskuste ilmnemisel?	Kuidas Te sattusite küberpettuste ohvriks ja kuidas tekkis esmane kontakt petturitega?	Millist isiklikku teavet Te petturitele vestluse ajal edastasite ja mis teie otsust mõjutas?	Milliseid emotsioone või tundeid Te petturitega suheldes kogesite?	Miks ja millisel hetkel Te taipasite, et Teid petetakse?	Millised tegevused järgnesid pettusekahtlusekorral, kui kiiresti ja kuhu Te abi saamiseks pöördusite?	Kas pärast Teiega juhtunut vajasite psühholoogilist abi või muud abi? Kuhu Te pöördusite probleemi lahendamiseks?	Kas Te jätkate digitaalteenuste kasutamist oma igapäevaelus? Mis õppetunni olete enda jaoks õppinud ja mida saate ise teha, et seda olukorda tulevikus vältida?
Informant 1	Kodupanga veebilehelt	Internetipank arvutis ja telefonis - kommunaalmaksed ja ülekanded lähedastele. Mobiilsed rakendused:Viber, Skype, e-mail – suhtlemine lähedastega; Aliexpress, Joom - kauba tellimine.	Arvutioskused on head, sest töötasin varem raamatupidajana. Kasutasin nutitelefoni ainult kaks aastat. Tehniliste probleemide või raskuste korral pöördun oma poja poole. Kui panga mobiilirakendus ei töötanud, pöördusin kontorisse.	Mulle tehti petukõne. Pettur tutvustas ennast konsultandina Google'ist ja väitis, et turvakaalutlustel on vaja muuta paroole, et kaitsta minu telefonikontot häkkimise ohu eest.	Edastasin oma isiklikud andmed (eesnimi, perekonnanimi, sünniaeg), kontaktandmed (e-posti aadress), panga andmed (pangakaardi number) vestluse ajal. Pettur oli rahulik ja veenev.	Muretsesin, et võidakse kuritarvitada mu pangakaardi andmeid ja varastada kogu raha, kui telefon pole kaitstud. Oli usaldus, et räägin tõelise Google'i töötajaga.	Pettur palus alla laadida rakenduse AnyDesk ja juhend selleks saadeti Viber'i kaudu. Kui rakenduste installeerimine telefonil oli ebaõnnestunud, muutus tema hääletonaalsus närviliseks ja ütles, et hakkame arvutile installeerima. Programme arvutisse installeerides tekkis kahtlus, kuna algselt oli petturi sõnul probleem telefonikontoga.	Olin väga hirmunud ja proovisin pojaga telefoni teel ühendust võtta, aga ta ei vastanud. Sõitsin otse kodupanga kontorisse.	Abi oli vajalik, kuid ma ei pöördunud kuhugi. Me arutasime seda juhtumit pojaga.	Tavalise elustiili taastumine võtab aega. Nüüd ei telli ma internetist midagi ja olen üldiselt ettevaatlikum.
Informant 2	Internetist ja sotsiaalvõrgust	Internetipank arvutis - kommunaalmaksed ja ülekanded	Ma ei oska kommenteerida oma arvuti või	Sain petusõnumi e-mailile, millele oli märgitud teemaks „Krüptoraha	Edastasin oma isiklikud andmed (eesnimi, perekonnanimi,	Tundsin rahulikult, sest uskusin, et	Pettur palus arvutisse alla laadida AnyDeski rakenduse, et saaks	Pöördusin oma kodupanga kontorisse.	Pöördusin arsti juurde, sest	Hetkel üldse ei kasuta digiteenuseid.

		lähedastele. E-mail - kaupluste reklaamkirjade jälgimine.	telefoni oskusi. Kui kodusel arvutil tekivad tehnilised häired, pöördun spetsialiseerunud ettevõtte poole. Telefonil on veel garantiiaeg.	investeerimine," ning järelkontakt oli telefoni teel. Pettur tutvustas ennast investeerimiskonsultandina ja pakkus võimalust mind õpetada ning juhendada selles valdkonnas.	isikukood), kontaktandmed (e-posti aadress, telefoninumber, postiaadress), panga andmed (kasutajatunnus internetipanka sisselogimiseks) ja kinnitasin pangaparoolidega kõik, mis minult paluti. Pettur ütles, et kõik need andmed on kohustuslikud konto registreerimiseks investeerimisplatvormil.	suhtlen professionaalse ja investeerimist oskava inimesega.	demonstreerida mu arvuti ekraanil, kuidas rahad teenivad tulu ja liiguvad investeerimisplatvormil. Avastasin oma pangakontolt kahtlased tehingud alles järgmisel päeval.		tekkisid närviprobleemid.	Andsin tütrele ligipääsu pangakontole ja sõlmisin mõnede ettevõtetega automaatsed e-arve lepingud. Olen pettunud ühiskonnas ja tänapäeva tehnoloogias. Nüüd on raske kedagi usaldada.
Informant 3	Linnalehest, tuttavate ja lähedaste inimeste käest	Internetipank tahvelarvutis ja telefonis - kommunaal- ja elektritasud. Mobiilsed rakendused: Viber – suhtlemine lähedastega; Kaup24 - kaupade tellimine.	Ma kasutan peamiselt tahvelarvutit, teisi arvuteid mul pole. Tehniliste probleemide korral aitab lapselaps neid lahendada.	Tuli petusõnum ja tehti petukõne. Müüsin kaupa kohalikul veebilehel teadetetahvli kaudu, jätsin telefoni numbri kontakti ja tagasiside võtmiseks. Pettur võttis minuga Viber'i kaudu ühendust ja pakkus välja võimaluse maksta mulle kättetoimetamise eest otse veebilingi kaudu ja ütles, et juhendab mind telefoni teel, kui on vaja.	Sisestasin veebilingi kaudu vormi oma isiklikud andmed (eesnimi, perekonnanimi, isikukood), panga andmed (pangakaardi number, kasutajatunnus panka sisselogimiseks) ning kinnitasin pangaparoolidega kõik tehingud, mis minult paluti. Tundsin, et see on tavaline protseduur ja et mind õpetatakse esimest korda seda läbi tegema.	Tundsin end rahulikult, kui vestluse käigus selgitati kõike, mis oli arusaamatu.	Viimati, kui midagi pangaparoolidega kinnitasin, lõpetasin ma kõne. Olin hirmul ja sain aru, et suhtlen kolmanda isikuga ja sisestan hetkel isikuandmeid.	Hakkasin koheselt lapselapsele helistama ja olin ise sel ajal väga närvis. Ta soovitas mul koheselt kodupanga kontorisse minna.	Ei vajanud abi, aga olin väga mures, et petturid varastavad kogu raha.	Jah, kasutan internetipanga võimalusi ja teisi digiteenuseid, nagu ennegi. Tutvusin kodupanga veebilehel pettuseliikidega, et suurendada silmaringi.

Informant 4	Raadiost ja lähedastelt inimestelt	Internetipank telefonis - kommunaal- ja haiglaravimaksed. Mobiilsed rakendused:Viber - suhtlemine lähedastega; E-mail - suhtlemine välismaal elava sõbrannaga.	Ei oska hinnata oma digitaalseid oskuseid. Kasutan nutitelefoni, sest arvuti on vana ja halvas seisukorras. Tehniliste probleemide korral aitavad lapsed. Kui panga mobiilirakendus ei töötanud, pöördusin kontorisse.	Sain petukõne. Viibisin haiglas ja mulle helistas pettur, kes tutvustas ennast pangatöötajana. Tema sõnul oli vaja kiiresti reageerida ja uuendada internetipanga kontaktandmeid, et mitte saada pangateenuste kasutamise piirangut.	Edastasin oma isiklikud andmed (eesnimi, perekonnanimi, isikukood), kontaktandmed (e-posti aadress, postiaadress), panga andmed (kasutajatunnus panga sisselogimiseks) ja kinnitasin pangaparoolidega kõik, mis paluti, et uuendada andmeid. Pettur näitas minu suhtes üles tähelepanelikkust, hoolivust, lahkust ja kiitis mind, kui kõik oli kinnitatud.	Haiglas viibisin üksi haiglatoas. Oli väga mugav ning meeldiv tunne rääkida pangatöötajaga, sest polnud tekkinud kahtlust, et suhtlen petturiga.	Iga päev suhtlen pojaga telefoni teel ja meie omavahelise vestluse ajal sain aru, et olen langenud petturi ohvriks.	Helistasin pojale. Ta andis panga telefoninumbri ja ma võtsin nendega ühendust. Töötaja pani mu konto luku taha ja broneeris mulle aja kontorisse.	Ei olnud vaja, kuna viibisin haiglas sel hetkel. Selline juhtum pikendas mu tervise taastumise perioodi, sest tundsin end nädala jooksul halvemini ja isu süüa oli kadunud.	Hetkel tegeleb kõigi minu panga asjadega poeg. Vormistasin pangaesinduses tema nimele üldvolikirja. Väldin telefoni kaudu rakenduste kasutamist. On vaja aega, et taastada normaalne elurütm.

Informant 5	Lähedaste inimestes käest	Internetipank arvutis ja telefonis - ülekanded lähedastele, konto väljavõtte kontroll.	Ei oska rääkida oma digitaalsetest oskustest. Kasutan rohkem nutitelefoni, kui arvutit. Tehniliste probleemide korral aitavad lapsed.	Sain petukõne. Pettur tuvastas end politseinikuna ja väitis, et keegi kolmas isik üritab minu nimel laenu võtta. Ta suunas mind ka teisele telefoniliinile, kus teine pettur tutvustas end pangatöötajana ja kinnitas politseiniku eelnevat sõnumit ning vajadust kiire reageerimise järele, näiteks avalduse vormistamisele telefoni teel, kui mina selle laenuvõtuga seotud ei ole.	Edastasin oma isiklikud andmed (isikukood), panga andmed (kasutajatunnus panga sisselogimiseks) ja kinnitasin pangaparoolidega kõik, mis minult paluti. Tundsin ennast rahulikult, kui kõne alguses pettur ütles mulle oma isiklikud andmed ja politseiesinduse kontaktandmed, kust ta helistab. Petturid olid veenvad ja viisakad, kahtlusi nende suhtes ei tekkinud.	Olin murelik natuke, sest hiljuti tõesti kaotasin oma isikut tõendava dokumendi. Kahtlused tekkisid, kui pettur täpsustas, millist panka ma kasutan.	Ainult pärast kõne lõpetamist	Olin väga hirmunud ja proovisin esmalt lastega telefoni teel ühendust võtta. Pöördusin oma kodupanga kontorisse.	Abi oli vajalik, kuid ma ei pöördunud kuhugi. Lapsed toetasid mind selles juhtumis, aga tundsin end väga halvasti.	Jah, kasutan digitaalseid teenuseid nagu tavaliselt aga ma muretsen aeg-ajalt nüüd rohkem. Püüan olla teadlikum küberpettustest.

Informant 6	Internetist, raadiost ja ajalehest	Internetipank arvutis ja telefonis - ülekanded, konto väljavõtte kontroll, kindlustuslepingud, pangakaardid. Sotsiaalvõrgustikud: Facebook, Odnoklassniki, Instagram – suhtlemine ja tuttavate jälgimine. Mobiilsed rakendused: Viber, Messenger, Skype - suhtlemine lähedastega. Aliexpress, Joom, Ebay - kaupade tellimine.	Tunnen, et arvutioskused ja telefonioskused on väga head. Töötasin varem koolis õpetajana, mul on digitaalsete vahenditega hea ja sage kogemus. Tehniliste probleemide või raskuste korral pöördun tavaliselt selle valdkonna ettevõtte esindaja poole. Arvuti ja telefon töötavad alati korralikult, sest ma hoolitsen oma seadmete eest.	Petukõne. Ostsin õhtul internetis kaupu ja järgmisel hommikul helistas pettur ning väitis end olevat panga turvaosakonna töötajana. Ütles, et minu pangakontol on tehtud kahtlased tehingud, mis on seotud ühe USA kaupmehega ja võib-olla sattusid pangakaardi andmed kurjategijate kätte. Pakuti blokeerida kahtlaseid tehinguid ning kirjutada avaldus pangakontoris kohapeal või telefoni teel.	Edastasin oma isiklikud andmed (isikukood), panga andmed (kasutajatunnus panga sisselogimiseks) ja kinnitasin pangaparoolidega kõik, mis paluti teha. Tundsin usaldust, et rääkisin pangatöötajaga.	Tundsin vestluse ajal end rahulikult, kuna petturi tagaplaanil oli kuulda kontori helisid: klaviatuuri ja printeri helisid. Muretsesin, et tühistavad minu eelmised kaupade ostud.	Tundsin petturi kõnest midagi veidrat, nagu mittestandardne keele aktsent. Sain aru, kellega olin rääkinud pärast kõne lõpetamist.	Olin hirmunud, et petturid üritasid telefoni häkkida või seda pealt kuulata. Pöördusin oma kodupanga kontorisse.	Ma ei vajanud abi. Vastutan ise tagajärgede eest.	Jah, kasutan digitaalseid teenuseid, nagu tavaliselt, aga panin tähele, et jälgin konto väljavõtet rohkem. Plaan on pühendada rohkem aega küberturvalisuse teemadele ja olla alati kursis sellega, mis toimub.

Autori koostatud.