TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ärikorralduse instituut

Hedi Remm

FINANTSKELMUSTE EEST HOIATAVA KOMMUNIKATSIOONI MÄRGATAVUS „EI, AITÄH!“ KAMPAANIA NÄITEL

Magistritöö

Õppekava juhtimine ja turundus, peaeriala äriprotsesside juhtimine digitaalühiskonnas

Juhendaja: Algis Perens, MBA

Tallinn 2022

Deklareerin, et olen koostanud lõputöö iseseisvalt ja
olen viidanud kõikidele töö koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 11 792 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Hedi Remm ……
(allkiri, kuupäev)
Üliõpilase kood: 204043TATM
Üliõpilase e-posti aadress: hediremm@gmail.com

Juhendaja: Algis Perens, MBA
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Finantspettuste tagajärjel kannatavad nii eraisikud kui ka ettevõtted märkimisväärset kahju. Seda vaatamata sellele, et nii ettevõtteid kui eraisikuid on pettustest ja nende erinevatest vormidest pidevalt teavitatud. Ettevõtted, sh finantsasutused ja makseteenuste pakkujad täiendavad pidevalt enda protsesse ja infrastruktuuri erinevate meetmetega, mis takistavad pettuste toimepanekut. Seeläbi püütakse kaitsta nii ennast kui ka kliente. Kuna aga paljud kelmused saavad võimalikuks tänu ohvri teadmatusele või tähelepanematusele, siis on oluline täiendada neid protsesse turunduslike meetmetega tõstes inimeste teadlikkust ning suurendades valmisolekut tuvastada aktiivsed kelmuste katsed. Kuigi suurem kelmuste laine näib olevat taandunud, tegutsevad kelmid edasi ja püüavad erinevate skeemide abil teenida tulu, millest levinumad on eri tüüpi õngitsuspettused, ettemaksupettused ja investeerimispettused.

Käesoleva magistritöö probleem on vähene arusaam pettustega seotud informatsiooni jõudmisest erinevate sihtrühmadeni. Magistritöö eesmärk on selgitada välja pettustealase kommunikatsiooni märgatavus ja teadlikkus pettustest erinevate sihtrühmade lõikes. Uurimisküsimustele vastamiseks kasutati kvantitatiivset uurimisviisi. Andmete kogumiseks viidi läbi anonüümne küsitlus ning andmeid analüüsiti kasutades kirjeldavat statistikat ning korrelatsioonanalüüsi. Analüüsiti nii Pangaliidu poolt korraldatud „Ei, aitäh!“ kampaania mõju kui ka üleüldist teadlikkust pettustest.

Teadlikkus pettustest hõlmab endas inimeste finantsalaseid teadmisi, arusaama andmekaitse olulisusest ja digihügieenist. Töö tulemusena selgus, et olenemata sellest, kas mäletati kampaaniat või mitte, siis teadlikkus pettustest oli vastanute hulgas kõrge ning ollakse küllaltki enesekindlad enda oskuses pettused reaalses ohuolukorras tuvastada. Enamasti saadakse pettuste kohta infot mitmest allikast. Olulisemateks infoallikateks on sotsiaalmeedia ja meediaväljaanded. Kõige vähem said uuringus osalejad infot tööandjalt.

Märksõnad: kommunikatsioon, teavituskampaania, finantspettused

SISSEJUHATUS

Finantspettuste tagajärjel kannatavad nii eraisikud kui ka ettevõtted märkimisväärset kahju. Euroopa Komisjoni läbi viidud uuringu kohaselt on ligi pooled EL elanikud viimase kahe aasta jooksul kogenud pettust ning kannatanud keskeltläbi kuni 500 euro suurust rahalist kahju. Euroopa Keskpanga viimase kaardipettuste raporti kohaselt oli SEPA riikides välja antud kaartidega tehtud ülekannete koguväärtus 5,16 triljonit eurot, millest 1,87 miljardit olid petturlikud ülekanded. Sõltuvalt pettuse liigist, keerukusest ja eesmärgist võivad kahjud olla tõsisemad kui ainult rahaliste vahendite kadu. Näiteks võib ettevõtetele pettuse ohvriks langemine või pettuste toimepaneku võimaldamine tähendada olulist mainekahju või lausa äritegevuse lõpetamist. Sageli soovivad kelmid saada pettuse abil ligipääsu mitte ainult ohvri finantsvaradele, aga ka andmetele ja ärisaladustele, mis võimaldavad tekitada kahju pikemaajaliselt, kuna ohver võib avastada pettuse alles mõne aja möödudes. Eraisikute jaoks võib kelmuse ohvriks langemine tähendada halvemal juhul keerulisse finantsolukorda sattumist, kuna kurjategijad ei võta ohvrite kontodelt mitte ainult vabasid vahendeid, vaid võivad sõlmida ohvri nimel laenulepinguid või survestada ohvrit juurde laenama.

Digitaliseeruvas maailmas püüavad kurjategijad leida uusi viise kelmuse toimepanekuks. Pettuseid on kahte liiki, mida kasutatakse enamasti paralleelselt: tehnilist laadi pettused ning manipuleerimisründed. Kui tehniliste pettustega kasutatakse ära turvanõrkused ohvrite seadmetes, siis manipuleerimisrünnete puhul kasutatakse ära ohvri heasoovlikkust, empaatiavõimet, usaldust ja teisi inimlikke omadusi. Ehkki ettevõtted ja eraisikud tajuvad pettuste ohtu hästi ning teatakse, kuidas end pettuste eest kaitsta, langevad siiski väga paljud ohvriks ja kannatavad moraalset või rahalist kahju. Ettevõtted, sh finantsasutused ja makseteenuste pakkujad täiendavad pidevalt enda protsesse ja infrastruktuuri erinevate meetmetega, mis takistavad pettuste toimepanekut püüdes kaitsta seeläbi nii ennast kui ka kliente. Kuna aga paljud kelmused saavad võimalikuks tänu ohvri teadmatusele või tähelepanematusele, siis on oluline täiendada neid protsesse turunduslike meetmetega tõstes inimeste teadlikkust ning suurendades valmisolekut tuvastada aktiivsed kelmuste katsed.

2021. aastal kasvas hüppeliselt telefonipettuste ja investeerimispettuste arv. 2021.a esimese seitsme kuuga registreeris politsei Eestis 313 kuritegu, mis on toime pandud „kõne pangast“ skeemi järgi, millega on tekitatud kahju kogusummas üle 1,2 mln euro. Ainuüksi juulis registreeris politsei 84 sellist kelmust, kahjusumma oli ligi 356 000 eurot. Investeerimispettuste ohvriks langes 2021. aasta esimese seitsme kuuga 184 inimest ning kogukahju oli üle 2 mln euro. (Politsei- ja Piirivalveamet 2021) Kelmid helistasid pangatöötajana esinedes inimestele ning survestasid neid jagama enda internetipanga kasutajatunnuseid ja paroole, mis võimaldas kelmidel varastada ohvrite kontodelt raha ning võtta nende nimel laenu. Investeerimispettuste puhul kasutasid kelmid enamasti võltsitud veebilehti, millel kuvati ohvrile investeeritud varade suur tootlikkus ning ühtlasi haarati ligipääs ohvri arvutile, mis võimaldas siseneda ohvri internetipanka.

Sellest ajendatuna viis Pangaliit 2021. aastal läbi kampaania „Ei, aitäh!“, mis hoiatas inimesi „kõne pangast“ jt pettuste eest. Kampaania kestis 2021. aasta augustist kuni septembri lõpuni. Selle aja jooksul said inimesed finantspettuste kohta infot tele, raadio- ja trükimeediast, otsepostituste brošüüridest ning internetist. Erilist rõhku pandi venekeelsele kommunikatsioonile, sest Politsei- ja Piirivalve ameti andmetel oli enamus telefonikõnede ohvreid just Eestis elavad igas vanuses vene keelt kõnelevad inimesed. (Politsei- ja Piirivalveamet 2021). Vaatamata teavitustööle kannatasid paljud inimesed pettuste tagajärjel siiski märkimisväärset kahju. Kuigi suurem kelmuste laine näib olevat taandunud, tegutsevad kelmid edasi ja püüavad erinevate skeemide abil teenida tulu, millest levinumad on eri tüüpi õngitsuspettused, ettemaksupettused ja investeerimispettused.

Käesoleva magistritöö probleem on vähene arusaam pettustealase kommunikatsiooni jõudmisest erinevate sihtrühmadeni. Magistritöö eesmärk on selgitada välja pettustealase kommunikatsiooni märgatavus ja teadlikkus pettustest erinevate sihtrühmade lõikes. Selleks püstitati järgmised uurimisküsimused:

1) Millisel määral on Pangaliidu kampaaniat märgatud?
2) Millistest allikatest saavad inimesed infot finantspettuste kohta?
3) Milliseid pettusi ollakse võimelised enda hinnangul tuvastama?

Andmete kogumiseks viidi läbi küsitlus. Küsimustiku koostamisel ja kampaania hindamisel võeti eeskujuks McGuire efektide hierarhia mudel, mida on varasemalt kasutatud

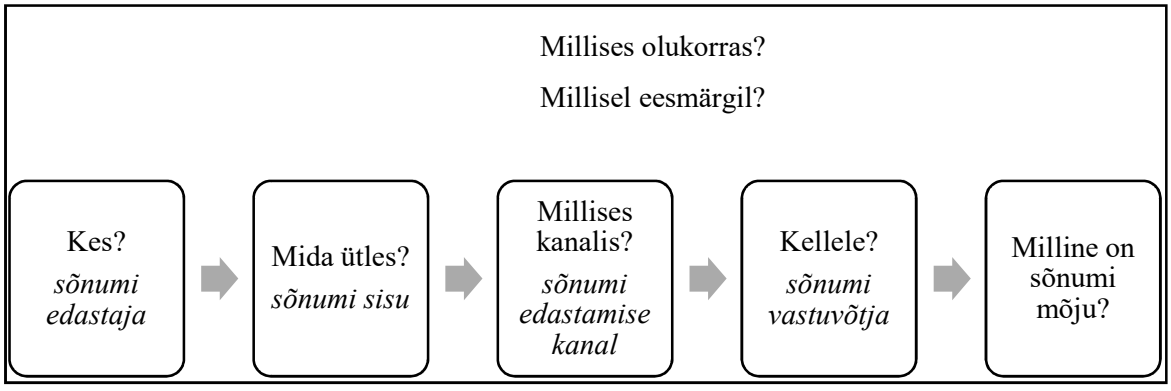
terviseedenduskampaaniate mõju hindamiseks inimeste tervisekäitumisele. Tulemuste analüüsimiseks kasutati kirjeldavat statistikat ja korrelatsioonanalüüsi.

Uurimistöö koosneb neljast peatükist: teoreetiline taust, metoodika kirjeldus, tulemuste analüüs ning arutelu ja ettepanekud. Teooria peatükis tehakse ülevaade kommunikatsiooni olemusest, teavituskampaania märgatavusest, eri liiki pettustest ja petuskeemide olemusest, ohvriks langemist ennustavatest teguritest ning pettuste ennetamise meetmetest. Uurimistöö teine peatükk kirjeldab metoodikat ja kolmas peatükk sisaldab kogutud andmete analüüsi. Neljandas peatükis analüüsitakse uuringu tulemusi vastavalt püstitatud uurimisküsimustele ja tehakse tulemustele tuginedes ettepanekuid pettuste ennetamise protsesside täiustamiseks ja inimeste teadlikkuse tõstmiseks.

1. TEOREETILINE TAUST

1.1. Kommunikatsiooni olemus

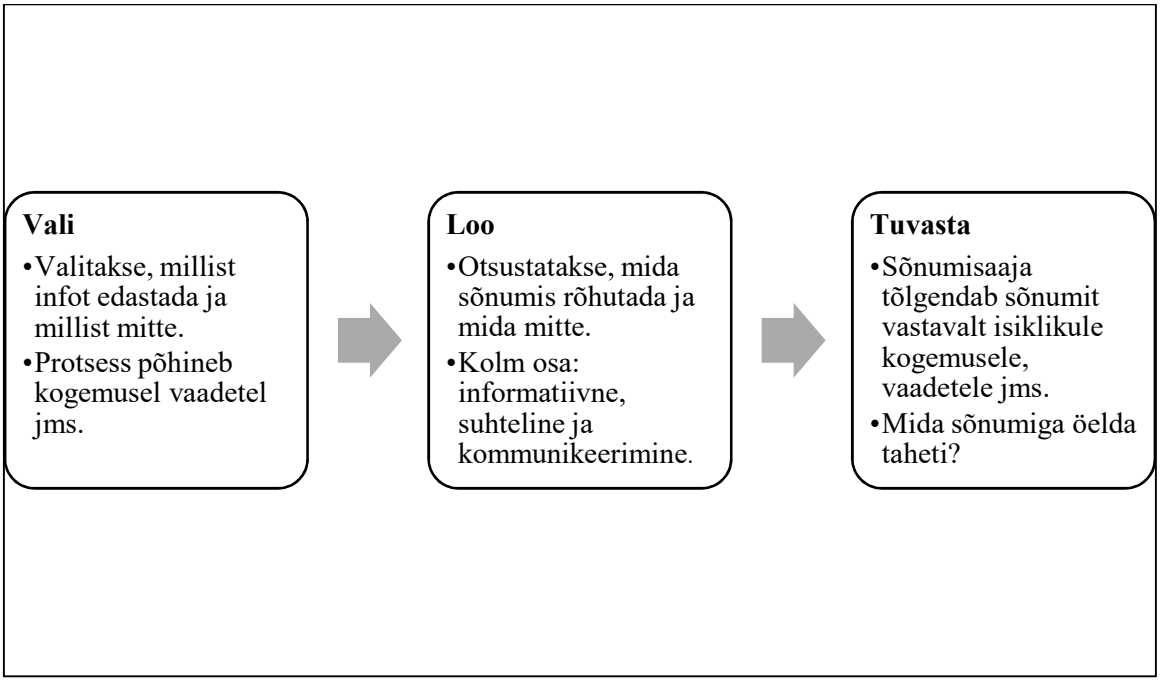
Kommunikatsioonil on ühiskonnas kolm rolli. Esiteks täidab kommunikatsioon keskkonnaseire rolli, millega avalikustatakse ühiskonda mõjutavad võimalused ja ohud. Teiseks mõjutab kommunikatsioon ühiskonna reageerimist muutustele ning kolmandaks antakse kommunikatsiooni abil edasi sotsiaalset pärandit. Kommunikatsiooniprotsessi analüüsimisel tuleb mõista, kes millist sõnumit millist meediakanalit kasutades millisele sihtrühmale edastada on soovinud ja milline on olnud selle sõnumi mõju. (Lasswell 1948) Lisaks sellele tuleb aru saada, millises olukorras on sõnum edastatud ja mis on olnud sõnumi edastamise eesmärk (McQuail, Windahl 2015 viidatud Braddock 1958) (Joonis 1).



Joonis 1. Braddocki mudel
Allikas: McQuail, Windahl (2015) viidatud Braddock (1958)

Kommunikatsiooni võib vaadelda kui lineaarset protsessi. Shannon-Weaver mudeli järgi on kommunikatsiooniprotsess analoogne info edastamisega elektroonilistes kanalites. Protsess algab sõnumi tootmisega infoallikas, millele järgneb edastaja abil sõnumi muutmine signaalideks. Need

signaalid adapteeritakse kanalisse, mis viib sõnumi sõnumisaajale ning sõnumisaaja rekonstrueerib sõnumi sõnumisignaalist. Oluline on siinkohal mõista, et sõnumisignaal on müra suhtes haavatav, eriti siis kui sõnumi edastamise kanalis on mitu signaali samaaegselt. Selle tõttu võib edastatav sõnum erineda saadud sõnumist ning sõnumi allikast saadetud sõnumil ei pruugi olla sõnumisaaja jaoks sama tähendus. See on põhjus, miks kommunikatsioon võib ebaõnnestuda. (Shannon 1948; McQuail, Windahl 2015) Kommunikatsiooni võib käsitleda ka sotsiaalteooria osana. Sellisel juhul koosneb kommunikatsiooniprotsess sammudest vali, loo ja tuvasta. (Joonis 2) Valimise etapis tehakse otsus, millist sõnumit kommunikeerida ja millist mitte. Sõnumi loomise etapis luuakse sõnumi sisu. Sõnum koosneb kolmest osast: informatiivne osa, suhteline osa ja tegelik kommunikatsioon. Tuvastamise etapp sisaldab endas sõnumi tõlgendamise prosessi. Sõnumisaaja tõlgendab sõnumit tuginedes enda elukogemusele, minevikusündmustele, väärtustele, minapildile jms ning tal tekib küsimus, mida selle sõnumiga öelda sooviti? Sõnumi tõlgendamine sõltub sellest, kuidas sõnumisaaja sõnumit mõistab, kas sõnumisaaja aktsepteerib sõnumit ning kas sõnum kõnetab teda või mitte. Tõlgendamise eesmärk on seega luua sõnumile tähendus, mis on seotud nii mineviku, oleviku kui ka tulevikuga. (Johannessen 2021)



Joonis 2. Kommunikatsioon kui sotsiaalteooria osa
Allikas: Johannessen (2021)

Teavituskampaaniate kavandamiseks ja analüüsimiseks kasutatakse sageli McGuire veenva kommunikatsiooni maatriksit (McGuire 2012). Maatriks koosneb sisendmuutujatest, millele kampaania üles ehitatakse ning väljundmuutujatest, mis kujutavad kampaania esile kutsutud käitumise muutust (Tabel 1). Mudelit kasutatakse tavaliselt tervisekäitumisega seotud kampaaniate analüüsimisel, et hinnata, kas kampaania tagajärjel on esinenud muutusi inimeste tervisekäitumises, kuid maatriks on rakendatav ka teistes valdkondades.

Tabel 1. McGuire veenva kommunikatsiooni maatriks

Sisendtegurid (kommunikatsioon)	Väljundtegurid (mõju)
1. allikas (allikate arv, demograafilised tegurid, atraktiivsus, usaldusväärsus jne) 2. sõnum (meeldivus, kaasamine või väljajätmine, organisatsioon, stiil, kordused jne) 3. kanal (modaalsus, otsekohesus, kontekst jne) 4. vastuvõtja (demograafilised tegurid, võimekus, iseloom, elustiil jne) 5. eesmärk (kohene või viivitusega, ennetamine või tagajärgedega tegelemine jne)	1. häälestamine (kokkupuude kommunikatsiooniga) 2. suhtlemises osalemine 3. meeldimine, huvi säilitamine 4. konteksti mõistmine (õppimine) 5. seoste loomine 6. uute oskuste õppimine 7. seisukohaga nõustumine (suhtumise muutus) 8. uue seisukoha omaksvõtmine ja mäletamine 9. uue seisukoha kasutamine olukorras, kus see osutub vajalikuks 10. otsus käituda vastavalt uuele omandatud seisukohale 11. tegutsemine 12. uue käitumisviisi omaksvõtt 13. teiste inimeste veenmine käitumaks samamoodi

Allikas: McGuire (2012)

Näiteks Solovei ja Van den Putte (2020) on uurinud sellele maatriksile tuginedes inimestevahelise suhtluse rolli erinevate mitte-terviseteemaliste informeerivate kampaaniate efektiivsuse saavutamisel. Eesmärk oli selgitada välja, kas inimestevaheline kommunikatsioon on soodustanud kampaania märkamist erinevates meediakanalites ning kuidas see on mõjutanud teadlikkust, teadmisi, suhtumist, kavatsusi ning käitumist seoses kampaania eesmärgiga. Autorid leidsid, et on olemas kaudne seos kampaaniasõnumi märkamise ning kampaania tulemuste vahel. Teisisõnu, kui inimesed märkavad kampaaniasõnumit, siis suurema tõenäosusega arutatakse seda teemat kellegi teisega ning suhtluse tulemusena (mitte niivõrd kampaania märkamise tagajärjel) suurenevad nende teadlikkus, teadmised,

suhtumine, kavatsused ja käitumine konkreetse teema suhtes. Küll aga on inimestevahelisel suhtlusel teisigi muutujaid, nagu näiteks inimeste isiklik huvi konkreetse teema vastu, kuna sageli arutatakse neid teemasid omavahel ka kampaaniaväliselt. Võttes aluseks veenva kommunikatsiooni maatriksi (McGuire 2012) hinnatakse antud uurimistöö käigus „Ei, aitäh!“ kampaania sõnumi allika, sõnumi kanali ja vastuvõtja mõju inimeste teadlikkusele probleemist ehk kui hästi ollakse kursis erinevate kelmuste liikidega ning kas enda hinnangul ollakse võimelised pettuse katse tuvastama ja kahju ennetama.

1.2. Teavituskampaania märgatavus

„Ei, aitäh!“ kampaania võib liigitada teavituskampaaniate alla. Teavituskampaania (PSA - *public service advertisements/announcements*) on reklaam, mis adresseerib ühiskonnas esinevaid probleeme eesmärgiga suurendada avalikkuse teadlikkust probleemidest ja nende võimalikest lahendustest. Lisaks püütakse PSA-de abil mõjutada avalikkuse uskumusi, suhtumist ning käitumist vastava probleemi suhtes. Enamasti viivad PSA kampaaniaid läbi mittetulunduslikud organisatsioonid või avalik sektor kasutades selleks massimeediat. (O’Keefe, Reid 1990) Euroopa Komisjoni (2020) poolt läbiviidud uuringu tulemused näitasid, et umbes 67% EL elanikest suudavad meenutada viimase kahe aasta jooksul nähtud pettuste eest hoiatavat kampaaniat. Eestis on see näitaja aga kõrgem, sest hoiatuskampaaniaid suudab meenutada ligi 80% küsitletutest. Uuring tõi välja, et pettusega kokku puutunud inimesed suudavad mõnevõrra paremini meenutada hoiatava reklaami nägemist.

Selleks, et PSA mõjutaks inimeste käitumist ning suhtumist soovitud suunas, on oluline, et PSA meeldiks inimestele. Seda, kuidas PSA reklaamsõnumi tonaalsus mõjutab probleemi suhtumist, on uurinud Dillard ja Peck (2000). Autorid leidsid, et positiivse sõnumiga PSA reklaam suudab suhtumist mõjutada, kuid negatiivse alatooniga sõnumi puhul seoseid ei leitud. Seejuures PSA meeldivus ennustab teatud olukordades sõnumi veenvust. Sellele tulemusele tuginedes on Nan (2008) uurinud, kuidas on omavahel seotud PSA mõju sõnumi saaja probleemi tajumisele, teadlikkus probleemist ning sõnumi tonaalsus. Lisaks sellele, et autor kinnitas Dillard ja Pecki (2000) uuringu tulemusi, leidis Nan (2008) tugeva positiivse seose PSA-sse suhtumise ning PSA-s esitatud probleemi suhtumise vahel.

Seejuures mõju kipub olema tugevam siis, kui sõnumi saaja probleemi tajumine ja teadmised sellest probleemist on pigem madalad.

Reklaamikampaania edu võib mõõta mitut moodi. Et PSA sõnumi levitamiseks kasutatakse kommertsreklaami tööriistu (O'Keefe, Reid 1990) on asjakohane „Ei, aitäh!" kampaania märgatavuse analüüsimisel tuua paralleele sellega, mida teatakse toodete reklaamimisest ning kuidas viia reklaamsõnum inimeste teadvusesse. Palju on uuritud, kuidas teabekanalite vahel sünergiat luues on võimalik jõuda reklaamsõnumiga võimalikult laia publikuni. Reklaamijal on tarvis otsustada, milliseid teabelevi kanaleid ta reklaami esitamiseks kasutab, kuna erinevad inimesed puutuvad sõltuvalt vanusest, elukohast, ametialast, soost jt omadustest ühtede kanalitega ja reklaamiliikidega rohkem kokku kui teistega. Kui jäetakse vastavale kontingendile sobiv edastusviis valimata, kaotatakse suur hulk inimestest, kelleni reklaamteatega jõuda tahetakse. (Bachmann 2009) „Ei, aitäh!" kampaanias rakendati nii telereklaami, trükimeediat kui ka sotsiaalmeediat. (Politsei- ja Piirivalveamet 2021)

Digikanalites reklaami kordamise puhul on leitud, et internetis, mobiilis ja televisioonis samaaegselt reklaami kordamine on efektiivsem kui ainult ühte kanalit kasutades. Interaktiivse meedia ajastul täiendavad mitteinteraktiivsed kanalid (nagu näiteks televisioon) interaktiivseid digimeedia platvorme, misläbi luuakse tänapäeva meediaplaneerimise lahutamatuks osaks kujunenud kanalite vaheline sünergia. (Lim *et al.* 2015) Rolli mängivad ka tarbijate meedia kasutamise harjumused. Meediakasutus on ennustatav sihtrühma demograafiliste tunnuste alusel, mis aitab reklaamikampaaniale tehtavaid kulutusi optimeerida. (Dens *et al.* 2018) Ehkki sünergiaefekt on end õigustanud, siis meediaplaneerimisel tuleb silmas pidada, et nõrga sünergia korral võib tekkida dubleerimine, mis vähendab reklaamsõnumi usaldusväärsust. Oluline on veel teada, et reklaamide vahel olev ajavahemik määrab tarbijate võime sõnumite vahel seoseid luua. (Dong, Chang, Fan 2017)

On teada, et reklaami äratundmine on efektiivsem kui meenutamine. Kui inimene peaks meenutama, millist reklaami ta seoses mingi kaubaga näinud on, satuks ta enamikul juhtudel raskustesse. Ent kui talle esitatakse reklaam ja ta peab ütlema, kas ta on seda näinud või ei ole, siis saab ta selle ülesandega paremini hakkama. (Bachmann 2009) Leitud on tõendeid selle kohta, et digitaalsetes kanalites esitatud reklaam soodustab reklaamsõnumi meenutamist. Inimesed, kes puutuvad reklaamiga kokku

digikanalites, suudavad tõenäolisemalt reklaami hiljem meenutada võrreldes nendega, kes puutuvad reklaamiga kokku muudes kanalites. Rolli mängib ka reklaamiga kokkupuutumise sagedus – mida sagedamini reklaamiga digikanalites kokku puututakse, seda tõenäolisemalt on sõnumisaaja võimeline reklaami hiljem meenutama. (Romberg *et al*. 2020) Vaatamata sellele, et kommertsreklaamidel ja PSA-del on erinevad eesmärgid ja edastajad, kasutatakse mõlemat formaati selleks, et edastada vaatajale olulist sõnumit. Seetõttu on tarvis reklaamiloojatel leida viise, kuidas muuta reklaamsõnum meeldejäävaks. Üks tõhusamaid viise selleks on luua toote reklaamimiseks või PSA edastamiseks loomingulise sisuga reklaam, mis köidab sõnumisaaja tähelepanu, eristab reklaami ülejäänud infomürast ning mille sisu oleks sõnumisaaja võimeline omandama teiste igapäevaste tegevuste kõrvalt. (Shen *et al.* 2020)

Kampaaniate planeerimiseks ja analüüsimiseks on kasutatud McGuire efektide hierarhia mudelit (HOE – *hierarchy of effects*), mis on töötatud välja reklaami ja turunduse teooria osana. Hierarhia moodustub kampaania lähtemuutujate ning kampaania tulemuste põhjuslikest seostest. Näiteks võivad lähtemuutujatena olla defineeritud teadlikkus kampaaniast ja võime kampaaniasõnumit meenutada, mille tulemusena muutuvad inimeste ootused, suhtumine ja käitumine konkreetse probleemi suhtes. (Bauman *et al.* 2008 viidatud McGuire 1984; Kite *et al*. 2018) Kampaania tulemusele võivad avaldada mõju vahemuutujad, nagu näiteks mõistmine, teadmised, suhtumine, sotsiaalsed normid, eneseusk muutuste elluviimiseks ning kavatsused käitumise muutmiseks. (Kite *et al.* 2018). (Tabel 2)

HOE mudelit on testitud terviseedenduskampaaniate analüüsimisel, mille tulemused on toetanud selle mudeli kasutatavust PSA-de mõju hindamisel. Üks esimesi selleteemalisi uuringuid viidi läbi Craig, Bauman ja Reger-Nash (2009) poolt, kes uurisid, kuivõrd sobitub füüsilist aktiivsust propageeriva kampaania mõju HOE mudeli raamistikku. Kampaania kestis 30 aastat ning selle aja jooksul edastati erinevaid, kuid teineteist toetavaid kampaaniasõnumeid. Küsitlused viidi läbi aastatel 1981, 1988 ning 2002-2004, seejuures teadlikkust kampaaniast mõõdeti 1981. aastal ning ootuste, suhtumise, valmisoleku ning tulevikukavatsuste kohta viidi küsitlused läbi hilisematel aastatel. Füüsilist aktiivsust mõõdeti paralleelselt kõigi kolme küsitlusega. Selgus, et kampaania mõjutas füüsiliselt mitteaktiivsete inimeste käitumist – teadlikkus mõjutas ootusi füüsilise aktiivsuse mõjule, ootused mõjutasid positiivset suhtumist füüsilisse aktiivsusesse, positiivne suhtumine mõjutas valmisolekut

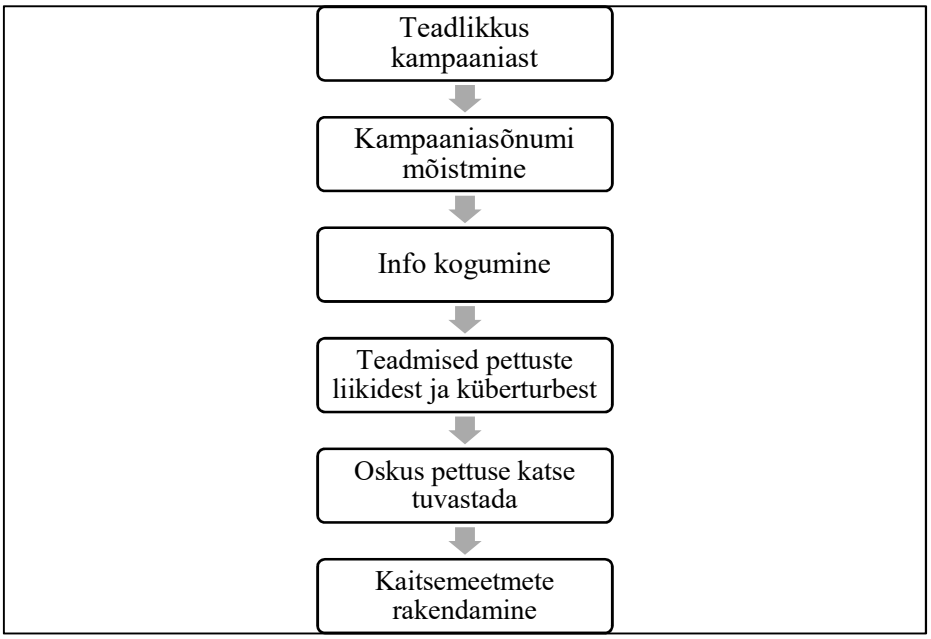
olema füüsiliselt aktiivne, valmisolek mõjutas tulevikukavatsusi ning tulevikukavatsused viisid füüsilise aktiivsuse suurenemiseni. Teisisõnu, kampaaniasõnumite järjepidev esitamine oli seotud füüsilise aktiivsuse sagenemisega varasemalt füüsiliselt mitteaktiivsete inimeste hulgas. Sarnasele tulemusele jõudsid ka Bauman *et al*. (2008) ja Kite *et al.* (2018), kes uurisid samuti terviseedenduskampaaniate mõju inimeste tervisekäitumisele. Leiti, et kampaania tagajärjel suurenenud teadlikkus ja arusaam tervislikest eluviisidest soodustasid positiivseid muudatusi inimeste tervisekäitumises.

Tabel 2. Näide HOE mudelist

HOE samm	Muutuja
kokkupuude kampaaniaga	kampaania märkamine
mõistmine	kampaaniasõnumit oli lihtne mõista
	teadmised füüsilise aktiivsuse soovitustest
	teadmised toitumissoovitustest
suhtumine ja sotsiaalsed normid	väikeste muudatuste elluviimine aitab ennetada kroonilisi haigusi
	väikeste muudatuste elluviimine toitumises aitab ennetada kroonilisi haigusi
	enamik minu pereliikmeid liigub vähemalt 30 minutit päevas
	enamik inimesi, keda tean, liiguvad vähemalt 30 minutit päevas
	üha enam inimesi teevad tervislikke toiduvalikuid
enesehinnang ja kavatsused	ma tean, et suudan enda tervisliku seisundi parandamiseks suurendada füüsilist aktiivsust
	ma tean, et suudan enda tervisliku seisundi parandamiseks vähendada rämpstoidu tarbimist
	plaanin olla järgmise kuu jooksul füüsiliselt aktiivsem
	tõenäoliselt vähendan järgmise kuu jooksul rämpstoidu tarbimist
käitumise hindamine	proovisin suurendada füüsilist aktiivsust
	proovisin vähendada rämpstoidu tarbimist

Allikas: Kite *et al.* (2018)

„Ei, aitäh!“ kampaania eesmärk oli tõsta inimeste teadlikkust finantspettustest jagades infot ning käitumisjuhiseid olukordadeks, kus inimene on tuvastanud pettuse katse või langenud ohvriks. Seega, kui analüüsida „Ei, aitäh!“ kampaaniat HOE mudeli raamistikus, tuleb selgitada välja, kuivõrd on kampaania märkamise tagajärjel inimesed võimelised rakendama asjakohaseid kaitsemeetmeid. Sarnaselt eelpool viidatud autoritega, on „Ei, aitäh!“ kampaania lähtemuutujana defineeritud teadlikkus kampaaniast ning tulemuseks käitumise muutus. Vahemuutujateks on kampaaniasõnumi mõistmine, info kogumine ja teadmised pettuste liikidest ning küberturbest. (Joonis 3)



Joonis 3. Kohandatud HOE mudel
Allikas: autori koostatud Bauman *et al.* (2008) ja Kite *et al.* (2018) põhjal

Teadlikkus kampaaniast tähendab seda, kas inimesele meenub selline kampaania. Kampaaniasõnumi mõistmise etapis püütakse selgitada välja, kuivõrd on inimesed mõistnud kampaania sisu ning kas kampaania tagajärjel on vastajate endi hinnangul tõusnud teadlikkus finantspettustest. Sõnumi mõistmisele järgneb info kogumise etapp, kus inimene kas uurib ise kampaanias viidatud allikatest infot pettuste kohta või ta saab seda infot muudest allikatest. Info kogumise tulemusena tõuseb eeldatavasti inimeste teadlikkus pettuste liikidest ja küberturbest, mille tulemusena ollakse võimelised pettuse katsed tuvastama. Olles tuvastanud pettuse, on inimene motiveeritud olema tulevaste pettuste katsete suhtes tähelepanelikum ning pöörab eeldatavalt senisest enam tähelepanu enda andmete ja seadmete turvalisusele.

1.3. Finantskelmuste liigid

Reurnik (2018) on kaardistanud peamised finantspettuste tüübid, milleks on valede finantsandmete avaldamine, kliendile mittesobivate finantstoodete müük ning finantskelmused (Tabel 3). Valede finantsandmete avaldamise all mõistetakse finantsasutuse poolt avaldatud valeinfot selle tegeliku

finantsolukorra kohta kasutades enda huvides ära informatsiooni asümmeetriat. Kliendile mittesobivate finantstoodete teadlik müük tähendab seda, et ohvrile müüakse manipulatsiooni abil sellist finantstoodet või -teenust, mida ta ei vaja või mis talle ei sobi ning võib tekitada kliendile suurt rahalist kahju. Valede finantsandmete avaldamist ja mittesobivate toodete müüki ühendab see, et sageli tegelevad pettusega legitiimsed organisatsioonid. Antud uurimistöös keskendutakse aga kolmandale pettuse tüübile, mille Reurnik (2018) on nimetanud finantskelmuseks. Finantskelmused on skeemid, kus vale identiteedi all esinevad isikud mõjutavad ohvreid läbi usalduse loomise, veenmise, mõjutamise ja eksitamise kurjategijatele vabatahtlikult üle andma raha või avaldama informatsiooni, mis võimaldab neile ligipääsu ohvrite finantsvarale. Sellised skeemid on juba eos petturlikud, kuna nende taga on spetsiaalselt kelmuse toime panemiseks loodud kuritegelikud ühendused.

Tabel 3. Pettuste tüübid

Pettuse tüüp	Pettuse olemus	Ettevõtte olemus	Keelavad õigusaktid
valede finantsandmete avaldamine	valed, faktide ebatõesel kujul esitamine	legitiimne	avalikustamisnõuded, üldised pettustega seotud seadused
finantskelmused	valed, faktide ebatõesel kujul esitamine	ebaseaduslik	avalikustamisnõuded, üldised pettustega seotud seadused
klientidele mittesobivate finantstoodete teadlik müük	eksitava mulje loomine	legitiimne või ebaseaduslik	hoolsuskohustus, sobivus nõuetele

Allikas: Reurnik (2018)

Finantskelmuste skeeme on oluline tunda selleks, et oleks võimalik rakendada asjakohaseid meetmeid kahjude ennetamiseks. Finantskelmuste tagajärjel kannatavad kahju nii eraisikud, ettevõtted, finantsasutused kui ka maksevahendajad. Tihtipeale kulub ohvritel palju aega ja raha pettuse tagajärgedega tegelemiseks. Skeemidesse kaasatud ettevõtted teevad tavapäraselt suuri investeeringuid pettuste tuvastamise süsteemidesse ning võivad kahtluse korral jätta aktsepteerimata reaalsete klientide poolt tehtud maksed, mille tulemusena võib langeda ettevõtte käive ja kasum. Finants- ja makseasutused, kes on aidanud kelmuse toimumisele tahtmatult kaasa võimaldades investeeringuid petturlikesse fondidesse ja pakkunud kurjategijatele arvelduslahendusi, kannatavad pettuse tagajärjel eelkõige mainekahju ning nende üle teostatakse tihedamat kontrolli, mis võib langetada ettevõtte väärtust. (Reurnik 2018)

Finantskelmus koosneb tavaliselt kolmest etapist. Esiteks hangitakse ohvrilt tema internetipanga sisselogimise paroolid, milleks kurjategijad kasutavad õngitsuskirju ja -veebilehti ning pahavara. Seejärel hangitakse raha ülekandmiseks kinnituskood helistades ohvrile kui pangatöötaja või kasutades jällegi pahavara. Viimaks kantakse ohvri käest saadud raha rahamuula pangakontole, kes võtab raha esimesel võimalusel sularahas välja ning annab kurjategijatele üle. (Leukfeldt, Jansen 2015) Rahamuulaks võib sattuda ka küberkuriteo ohver endale teadmata võimaldades kurjategijatel kanda enda kontole üle ebaseaduslikul teel teenitud raha. (Cotoc *et al.* 2021) 2020. aastal pälvis Eesti Rahapesu Andmebüroo (RAB) tähelepanu võrdlemisi uus pangateenus VIBAN (*virtual* IBAN), mille puhul väljastab krediidiasutus oma kliendile personaliseeritud IBAN-konto numbreid, mida klient saab oma klientidest lõpptarbijale edasi jagada. VIBAN-kontod on väliselt sarnased Eestis väljastatava IBAN-kontoga, mis võimaldab neid kasutada kuritegude toimepanemiseks Eesti finantssüsteemi kaudu. VIBAN konto abil liigutatakse ohvri makstud raha kiiresti kas virtuaalvääringu rahakotti või mõnele välisriigi makseasutusele. (Rahapesu Andmebüroo 2021)

See, kas kuritegelik grupeering kasutab manipuleerimisrünnet või pahavara, sõltub konkreetse organisatsiooni tehnilisest võimekusest. Reeglina kasutavad vähem võimekad grupeeringud manipuleerimisrünnet ning võimekamad grupeeringud pahavara. Et manipuleerimisrünne on küllaltki ressursimahukas, püütakse manipuleerimisründe korral ohvrilt saada ühe korraga kätte võimalikult suur summa. Seevastu pahavaralise ründe korral, kus ülekanded automatiseeritud, ohvreid on palju ning maksed jäävad sageli ohvritele mõneks ajaks märkamatuks, kantakse pikema ajaperioodi jooksul üle väiksemad summad ning kuritegelik organisatsioon võib teenida väga suurt tulu. (Leukfeldt, Jansen 2015).

1.3.1. Investeerimispettused

Finantskelmuseid on peamiselt kahte tüüpi: investeerimispettused ning identiteedivargused. Investeerimispettuste korral pakutakse ohvrile konkreetset investeerimisvõimalust, mida ei ole olemas või mis kindlasti investori ootustele ei vasta. Selliste investeerimisvõimaluste alla käivad võltsitud ettevõtete osad, aktsiad või võlakirjad, mida kelm esitleb kui uut populaarset toodet, tehnoloogiat või ärivõimalust. Alternatiivina võivad investeerimisskeemid pakkuda ohvritele võimalust osaleda ühisrahastusprogrammides, kinnisvaraprojektides või kindlustuse skeemides. (Reurnik 2018) Tüüpilisi investeerimispettuse skeeme iseloomustavad madala või riskivaba investeeringute

pakkumised, garanteeritud tootlus, liiga järjepidev tootlus, keerulised strateegiad või registreerimata väärtpaberid. Investeerimispettuste näideteks on ettemaksupettus, Ponzi skeemid, püramiidskeemid ja turuga manipuleerimisega seotud pettused. (FBI 2022) Tihtipeale võimaldab ohver ka ligipääsu enda arvutile ning avaldab petturile enda isikuandmeid, sh finantsandmeid. Tüüpiliselt leiab ohver info investeerimisvõimaluse kohta sotsiaalmeediast, peale millega tutvumist saab ohver kõne kelmilt. Kelmid kasutavad osavaid manipuleerimistehnikaid, loovad ohvriga usaldusliku suhte ning kasutavad ära tema impulsiivset käitumist. (Lacey *et al.* 2020)

Investeerimispettuseid on erinevaid. Mõnel juhul koguvad kurjategijad raha kokku ning seejärel kaovad. Sageli kasutatakse selleks salastatud jurisdiktsioonis registreeritud variettevõtet. Enamikel juhtudel on investeerimispettuste elutsükkel pikem ning nendest saab Ponzi skeem. Ponzi skeemides tekib investeeringu tulu uute investorite kaasamisest, mitte investeeringu enda edust. Sageli pakuvad kelmid esimestele investoritele väärtpaberid, mis on reinvesteeritud järgmisesse investeerimistsüklisse ning ohvrile näidatakse paberil tema investeeringu tootlust. Ponzi skeemid kukuvad kokku tavaliselt siis, kui uusi investoreid ei suudeta kaasata või kui esimesed investorid soovivad enda väärtpabereid realiseerida. (Reurnik 2018) Sarnast mustrit jälgivad ka püramiidiskeemid, kus skeemi vanemad osalised saavad tulu uute osaliste pealt. Erinevus seisneb selles, et püramiidiskeemis saavad ohvrid vahendustasu uute liikmete värbamiselt. (FBI 2022)

Investeerimispettuste korral on saanud Eestis tavapäraseks praktikaks, et kurjategijad kasutavad ära ühisrahastusplatvorme heausklikelt investoritelt raha välja petmiseks. Näiteks kogutakse investoritelt raha, mis investeeritakse platvormi kodulehel reklaamitud projektidesse. Väidetavalt pakutakse investoritele võimalust investeerida Euroopa väikeettevõtetesse ja *start-up* projektidesse teenides nii märkimisväärset tulu. Platvormi haldajad saavad investeeringu endale väidetavalt selleks, et projekte ellu viia ning hakkavad seda järk-järgult tagasi maksma nagu tavalist laenu. Investorid saavad väidetavalt iga kuu tagasi osa oma investeeringust koos teenitud intressituluga. Lisaks reaalsetele projektidele võidakse esitada klientidele ka näilisi investeeringuobjekte. (Rahapesu Andmebüroo 2021) Investeerimispettuseks loetakse ka turuga manipuleerimisega seotud pettust, mis loob kunstliku ostusurve konkreetsele väärtpaberile, mis on emiteeritud börsivälisel väärtpaberiturul ja mis on kelmide kontrolli all. Kunstlikult suurendatud kauplemismahu abil suurendatakse väärtpaberi hinda, millega väärtpaber hiljem maha müüakse ning investoritele tekitatakse seeläbi kahju. Selle skeemi

kaasaegne variant kujutab endast ligipääsu haaramist ohvrite veebi-vahenduskontodele, mida kasutatakse väärtpaberite koordineeritud ostmiseks, et mõjutada manipulatsiooni abil väärtpaberi turuväärtust. Samal ajal müüvad petturid olemasolevad väärtpaberid maha ning teenivad sellest ebaseaduslikku tulu. (FBI 2022)

Ettemaksupettuste alla kuuluvad näiteks abipalved põgenikult, raskelt haigelt või muus keerulises olukorras olevalt inimeselt või esinetakse pangaametnikuna, kes on avastanud suure summa sularaha. Edasise väidetava uurimise käigus selgub, et vara omanik on surnud ning ametnik ei soovi, et raha satuks pahatahtlike ametnike kätte. Levinud on ka teated loteriivõidust ning tööpakkumised, mis on liiga head, et olla tõsi. Ettemaksupettusi ühendab kelmi poolt antud lubadus pakkuda ohvrile vastutasuks suurt rahalist tulu ning ohvri empaatiavõime ärakasutamine. (Freiermuth 2011) Ettemaksupettuse tunnustega on ka armupettused, kus kurjategija loob võltsitud isiksuse abil ohvriga veebikeskkonnas pettuste eesmärgil armusuhte. Tavaliselt saadakse ohvriga kontakt kohtingukeskkonnas ning hiljem liigub suhtlus mõnda teise suhtluskeskkonda, kus ühel hetkel küsib kelm ohvrilt suure summa raha. Sarnaselt ettemaksupettusega pannakse ohver uskuma, et ta saab raha maksmisest hiljem ise rahalist kasu, kuigi enamasti on peaeesmärgiks väidetavalt siiski suhte loomine, mitte raha. Pettus lõpeb siis, kui ohver mõistab, et tegu on pettusega ning lõpetab raha andmise. (Whitty 2013)

1.3.2. Identiteedivargus

Identiteedivarguse all mõistetakse erinevaid liiki kuritegusid, mille käigus omandatakse ja kasutatakse pettuse teel või pettuse abil ebaseaduslikult teise isiku andmeid majandusliku kasu saamiseks (The United States Department of Justice 2022). Identiteedivargusi võib kompositsiooni alusel jagada kaheks: manipuleerimisründed (*social engineering*) ning tehnilised ründed (*technical subterfuge schemes*). Tehnilise ründe puhul saadetakse ohvrile näiteks e-kiri, mille avamisel installeeritakse ohvri arvutisse pahavara või suunatakse ohver IP aadressi muutmise abil võltsitud veebilehele, mille tulemusena jõuavad ohvri andmed kurjategijani, ilma et ohver sellest teadlik oleks. Tehniliste rünnete alla kuuluvad sellised meetmed, nagu näiteks andmelõikus (*Pharming*) ja maksekelmused. (Reurnik 2018) Maksekelmuseid sooritatakse ohvrilt varastatud pangakaardiga või läbi internetipanga (CNP – *card not present*). CNP tüüpi pettused on alates 2008. aastast tõusnud moodustades 2019. aastal 80% kõikidest SEPA piirkonnas tuvastatud pangakaardipettustest. CNP pettus on kaardipettus, kus

kurjategija käes ei ole mitte füüsiline pangakaart, vaid pangakaardi andmed. CNP pettuste osakaalu suurenemise on teinud võimalikuks sagenenud kaardimaksed internetikaubanduses. SEPA riikides välja antud kaartidega tehtud ülekannete koguväärtus oli 2019. aastal 5,16 triljonit eurot, millest 1,87 miljardit olid petturlikud ülekanded. (Euroopa Keskpank 2021)

Erinevalt tehnilisest ründest, kus ohver ei pruugi teadlik olla andmete vargusest, on manipuleerimisründe õnnestumiseks oluline ohver meelitada skeemis osalema ning enda isikuandmeid vabatahtlikult üle andma. Kõige enam levinud manipuleerimisründe meetod on õngitsemine (*Phishing*). Laiema definitsiooni kohaselt on õngitsemise näol tegu vastavalt konkreetsele olustikule kohandatava pettusega, mille puhul esinetakse teabe hankimiseks kellegi teisena (Lastdrager, 2014). Levinumad kanalid, mille abil ohvriga ühendust võetakse on e-kiri ja SMS, kuid lisaks võidakse kasutada kiirteavitusi, sotsiaalmeedia võrgustikke, blogisid, foorumeid, mobiilirakendusi ning telefoni- ja veebikõnesid. (Aleroud, Zhou 2017) Klassikalise õngitsusskeemi järgi saab ohver näiliselt e-kirja kas pangalt või mõnelt muult krediidiasutuselt, milles antakse ohvrile korraldus viivitamatult asutuse veebikeskkonda siseneda eesmärgiga ennetada edasisi kahjusid. Kelmi eesmärgiks on panna ohver ähvardusi kasutades ja toimingu kiireloomulisusele rõhudes enda isikuandmeid võltsitud veebilehe sisestama, enne kui ohver jõuab pettuse katse tuvastada. (Reurnik 2018)

Eestis viimase paari aasta jooksul laialt levinud „kõne pangast“ kelmused võib liigitada õngitsuskõneks (*Vishing*) ehk telefoni teel toimepandud manipuleerimisründeks, mille eesmärk on hankida ohvrilt tema isikuandmeid ja autentimisvahendi paroole, et oleks võimalik tema kontolt raha üle kanda. Sageli esineb kurjategija ohvri kodupanga või mõne muu maineka organisatsiooni töötajana ning palub ohvril kiiret sekkumist nõudval põhjusel veebikeskkonda sisse logida. Reaalajas toimuva suhtluse käigus võib kurjategija muuta kasutatavat veenmistehnikat vastavalt olukorrale, mis eeldab kurjategijaga koostöö tegemist. Enam levinud veenmismeetmed, mida kurjategijad kasutavad selleks, et panna ohver endaga koostööd tegema, on autoritaarsus, ohvri näiline aitamine (*social proof*) ja tähelepanu kõrvalejuhtimine. Õngitsuskõne koosneb mitmest sammust, mis jätab ohvrile rohkem võimalusi pettuse avastamiseks võrreldes näiteks õngituskirjaga, kus ohvril tarvitseb vaid klikkida veebilehe lingile või e-kirja manusele. Põhjuseks on tavaliselt see, et kurjategija suudab panna ohvri

uskuma koostöö tegemisest saadavasse kasusse ning kasutab ära tema emotsionaalset hetkeseisundit. (Jones *et al.* 2021)

1.4. Ohvriks langemist ennustavad tegurid

Pettuse ohvriks langemist ennustavad mitmed tegurid, nagu näiteks potentsiaalse ohvri sotsiaaldemograafilised näitajad, finantskirjaoskuse tase, erinevad psühholoogilised iseärasused, IT-alased teadmised, internetikasutus jt igapäevased harjumuspärased tegevused ning teadlikkus küberturbest. Küberkuritegude analüüsimisel on laialdast kasutust leidnud rutiinsete tegevuste teooria (RAT – *routine activities theory*), mille abil on selgitatud välja, milliste asjaolude kokkulangevusel õnnestub kübermaailmas kuriteo toimepanek. RAT kohaselt on kuritegude toimumiseks on vaja motiveeritud ründajat, sobivat sihtmärki ning järelvalve puudumist. Kuritegude toimepaneku teevad võimalikuks inimeste igapäevased, rutiinsed tegevused. Kuritegude ennetamiseks piisab sellest, kui üks eelnimetatud elementidest on puudu. Näiteks kurjategijate ja sihtmärkide arv võivad olla ajas enam-vähem samal tasemel, kuid muutused rutiinsetes tegevustes võivad luua kuritegude toimepanekuks rohkem võimalusi. Seetõttu on kontrollil ja järelvalvel rutiinsetes tegevustes oluline roll – kontrolli suurenedes kuritegude arv väheneb ja vastupidi. (Cohen, Felson 1979)

Ohvriks langemist ennustavaid tegureid on uuringutes vaadeldud alati koos mõne teise teguriga. Üksnes sotsiaaldemograafiliste tunnuste alusel on keeruline üheselt mõistetavalt potentsiaalse ohvri profiili luua, kuna eri tüüpi skeemide sihtmärkideks ja ohvriteks on erinevate tunnustega inimesed. Küll aga on leitud, et üleüldiselt langevad mehed ja kõrgemalt haritud inimesed sagedamini pettuste ohvriks kui naised ja madalamalt haritud inimesed lükates ümber üldlevinud väite, et ainult „rumalad“ inimesed kannatavad kahju (Whitty 2020).

1.4.1. Vanuse roll pettuse ohvriks langemisel

Vanus võib olla üheks, aga mitte ainsaks pettuse ohvriks langemise teguritest, mis on seotud inimese psühholoogiliste iseärasustega, igapäevaste tegevustega ning varasema ohvriks langemise kogemusega. Näiteks on vanemad inimesed küberkurjategijatele atraktiivsemaks sihtmärgiks kui nooremad inimesed, mille põhjuseks peetakse vanemate inimeste paremat finantsseisundit ning nende

vajadust erinevate finantsteenuste järgi. Samal ajal on noored inimesed kuritegude suhtes haavatavamad, kuna nad teevad igapäevaselt selliseid tegevusi, mille tõttu on nad küberkuritegudele avatumad, samas kui vanemad inimesed rakendavad veebis erinevaid kaitsemeetmeid. (Whitty 2019) Euroopa Komisjoni (2020) läbiviidud uuringu tulemused näitasid, et tihe internetikasutus on üks olulisemaid pettusega kokkupuutumist ennustavaid tegureid lisaks vanusele ja haridusele. Tõenäosus pettusega kokku puutuda suureneb 25 protsendipunkti, kui internetti kasutatakse vähemalt korra nädalas, võrreldes nendega, kes kasutavad internetti väga harva või üldse mitte.

Ka pettuse kanal sõltub ohvri sotsiaaldemograafilisest tunnustest ning internetikasutusest. Internetis aktiivsemad, nooremad ja kõrgema haridustasemega inimesed on avatud enamasti veebikelmustele, samas kui internetis vähem aktiivsed, vanemad ja madalama haridusega kogevad pigem telefonikelmust. See on seotud konkreetse demograafilise rühma käitumisega, mitte niivõrd sellega, et kurjategijad otsiksid kontakti kindlate demograafiliste tunnustega inimestega. Identiteedivarguse tagajärjel toime pandud pangakaardipettuse ohvriteks langevad enamasti vanemad ja keskealised inimesed, kuid sõltuvalt konkreetsest pettuse tüübist võib ohvriks langemise tõenäosus olla mõnevõrra erinev. (Copes *et al.* 2010) Seevastu investeerimispettuste puhul on leitud seos vanuse, soo ning ohvriks langemise vahel – investeerimispettuste ohvrid on sagedamini vanemaealised mehed (Whitty 2020; Deliema, Shadel, Pak 2020). Kõige enam haavatavad on pensionärid, kelle finantsalased teadmised on puudulikud ning kes kardavad, et neil ei jätku pensionipõlveks piisavalt raha. (Lokanan 2014)

Vanusel on ennustav roll ohvriks langemisel veel koos eelneva pettuse kogemusega. Korduvohvrite puhul ei ole küll täheldatud seost ei psühholoogiliste ega sotsiaaldemograafiliste teguritega (Whitty 2019), ent eelnev kokkupuude pettustega muudab vanemad inimesed pettuste suhtes ettevaatlikumaks ning nad suudavad paremini tuvastada pettuse katse kui nooremad inimesed. Selle põhjuseks võib olla asjaolu, et vanemate inimeste jaoks on pettusega kokkupuude meeldejäävam kui nooremate inimeste jaoks, kuna neil on rohkem finantsvarasid, mida kaotada. Nooremad inimesed seevastu võivad suhtuda pettuse katsesse kergekäeliselt, kuna usuvad, et pettused neile reaalselt ohtu ei kujuta. Seetõttu on ka vanemad inimesed motiveeritumad kasutama erinevaid kaitsemeetmeid. Vanemad inimesed on ühtlasi kahtlustavamad ning enesekindlamad õngitsuskirjade tuvastamisel, mis võib aga muuta

vanemad inimesed hiljem haavatavamaks, kuna nad võivad eirata asutuste nõudeid vahetada paroole jms. (O'Connor *et al.* 2021)

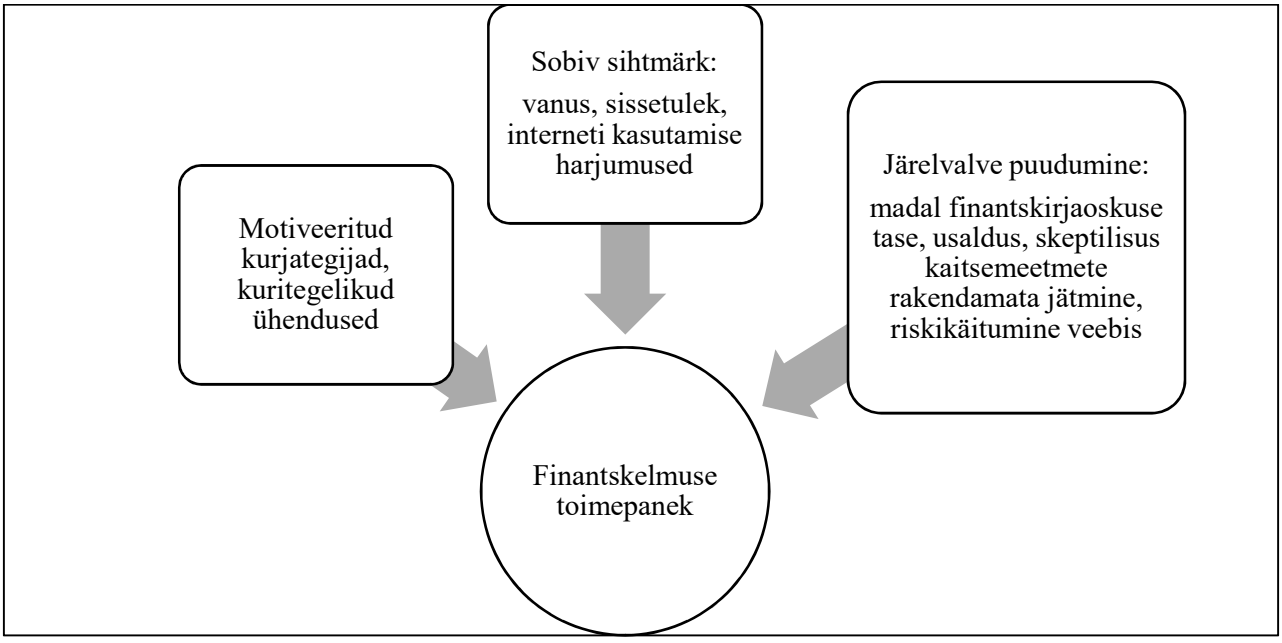
1.4.2. Teiste tegurite roll pettuse ohvriks langemisel

Investeerimispettuste ohvriks langemise juures mängivad olulist rolli inimese isikuomadused. USA-s läbiviidud uuringu tulemused on näidanud, et investeerimispettuse ohvrid on tavaliselt materialistlikumad ning eeldavad, et reguleerimata investeeringud toovad suuremat kasu. Kurjategijad kasutavad seda ära lubades ohvrile ebareaalselt suurt kasumit, mis tavapäraste investeerimistoodetega ei ole võimalik. Inimesed, keda motiveerib raha, võivad ignoreerida asjaolu, et näidatud kasum ei ole võimalik või usuvad, et potentsiaalne kasu kaalub üles kaotuse. (Deliema, Shadel, Pak 2020) Investeerimispettuse ohvriks langemist soodustab sageli ka ohvri rahulolematus enda finantsolukorraga (Kadoya, Khan 2020). Identiteedivarguse tagajärjel toime pandud krediitkaardipettuse ohvriks langemise kõrgemat määra on täheldatud naiste hulgas, seejuures madalama haridustasemega inimeste seas on ohvriks langemise tõenäosus väiksem. Põhjus võib siin peituda selles, et madalama haridusega inimestel on ühtlasi madalam sissetulek. Need inimesed, kes on rahaliselt keerukamas olukorras, on pettustele vähem avatud, kuid pettusega kokku puutudes on neil suurem risk kannatada rahalist kahju võrreldes inimestega, kelle finantsseisund on stabiilne. (Euroopa Komisjon 2020) Madalama sissetulekuga inimesed on vähem haavatavamad identiteedivarguse suhtes, kuna nende rahaline olukord ei muuda neid kurjategijate jaoks atraktiivseks sihtmärgiks. (Copes *et al.* 2010)

Ohvriks langemist ennustavad psühholoogiliste ja sotsiaaldemograafiliste tegurite seos inimese rutiinsete, igapäevaste tegevustega. Näiteks kõrgemalt haritud inimesed on küberkuritegudele küll avatumad, ent rakendavad vastavaid kaitsemeetmeid. (Whitty 2019) Inimesed, kes on viimase kahe aasta jooksul pettusega kokku puutunud, on pettuste suhtes ettevaatlikumad. Küll aga ei ole täheldatud, et need inimesed, kes on kannatanud pettuse tagajärjel kahju, oleksid oluliselt ettevaatlikumad võrreldes nendega, kes on küll pettuse katse tuvastanud, kuid ei ole kahju kannatanud. (Euroopa Komisjon 2020) Olulist rolli mängib pettuste tuvastamise oskuse juures ka inimese finantskirjaoskuse tase – mida kõrgem on inimese finantskirjaoskus, seda tõenäolisemalt suudab ta pettuse katse tuvastada ning edasist kahju ära hoida (Engels, Kumar, Dennis 2020).

Veel on leitud, et arvutialaselt kõrgemate teadmistega inimesed on ühtlasi ka küberturbe alal teadlikumad ning rakendavad tõenäolisemalt meetmeid rünnakute ennetamiseks, eriti kui need meetmed on lihtsad ning kasutajale tuttavad. Mida enam spetsiifilisi teadmisi kaitsemeetmete rakendamine nõuab, seda enam võivad inimesed tunda ebakindlust nende rakendamisel ning seetõttu väheneb inimese huvi uurida täiendavate võimaluste kohta kaitsta end kübermaailmas. Seepärast on oluline inimesi järjepidevalt kübertube alal koolitada ja tõsta üleüldist teadlikkust erinevatest ohtudest ning nende ennetamise võimalustest. (Zwilling *et al.* 2020) On leitud, et aktiivsed nutitelefoni kasutajad langevad suurema tõenäosusega küberkuritegude ohvriteks, kuna nad on kurjategijatele kättesaadavamad, nad puutuvad rohkem pettuse katsetega kokku ning avaldavad suure tõenäosusega internetis enda kohta tundlikku informatsiooni. Nutitelefoni sõltlasi iseloomustavad kehv vaimne tervis ning madal sotsiaalne seotus, mistõttu on nad küberkuridegude suhtes eriti haavatavad. (Herrero *et al.* 2021)

Kokkuvõtvalt võib öelda, et küberkuritegude ohvriks langemisel peavad kokku langema mitmed asjaolud. Sihtmärk peab olema kurjategijale samaaegselt atraktiivne ning ligipääsetav ning omama teatavaid isikuomadusi. (Joonis 4)



Joonis 4. Finantskelmuse ohvriks langemist ennustavad tegurid RAT teooriale tuginedes
Allikas: autori koostatud viidatud allikate põhjal

Kõrgema sissetulekuga inimesed pakuvad kurjategijatele enam huvi, mis on mõnevõrra ennustatav inimese demograafiliste näitajatega – on tõenäolisem, et kõrgemalt haritud vanemal inimesel on pangakontol rohkem finantsvahendeid kui nooremal ja madalama haridusega inimesel. Kui demograafilised andmed võivad olla kurjategijatele mingil moel ligipääsetavad, siis inimese isikuomadused mitte. Skeptilisus, rahulolematus enda finantsolukorraga, hirm ebastabiilse tuleviku ees ja kehv finantskirjaoskuse tase võivad sihtmärgi panna käituma riskantselt ning liialt usaldavalt, mistõttu saab temast suure tõenäosusega küberkuriteo ohver.

1.5. Pettuste ennetamise meetmed

Kriminaalid otsivad pidevalt uusi alternatiivseid kanaleid kuritegelikul teel hangitud varade kasutamiseks. Tavaliselt kasutatakse rahapesu eesmärgil ära finantsasutuste infrastruktuuri, sealhulgas uute makselahendusteenuste pakkujate teenuseid, tänu millele liiguvad rahad maksesüsteemis kiiremini. Suurenenud on trend kasutada professionaalseid teenuseid, nagu näiteks raamatupidajaid, audiitoreid ja juriste. Nendest teenusepakkujatest on saanud samuti kohustatud isikud ning peavad monitoorima oma klientide tehinguid ning kasutama riskipõhist lähenemist. Finantsasutuste väljakutseks on leida tasakaal uute makselahenduste pakkumisel klientidele tagades samal ajal tehingute läbipaistvuse. Selle eesmärgi saavutamiseks tuleb informeerida kliente potentsiaalsetest riskidest ning koolitada rahapesuga võitlevaid töötajaid uuemate kriminaalsete meetodite, kahtlaste tehingute tuvastamise meetodite kohta ning tutvustada vastavaid ennetuse ja kontrolli tööriistu. (Cotoc *et al.* 2021)

1.5.1. Regulatsioonid ja organisatsioonidevaheline koostöö

Finantsasutused lähtuvad oma igapäevategevuses erinevatest seadustest, millest üks on Rahapesu ja Terrorismi Rahastamise Tõkestamise Seadus. Viienda ja kuuenda direktiiviga võeti vastu mitmed olulised muudatused, seahulgas anonüümsete makseviiside kasutuse piiramine, rahapesu- ja terrorismi rahastamise tõkestamise põhimõtete laienemine krüptovaluuta kasutamisele ja selle infrastruktuurile ning finantsjärelvalveasutuste omavahelise koostöö hõlbustamine. (Euroopa Komisjon 2017) Maksevahendajate tegevust reguleerib PSD2 (*Payment Service Directive*), mis ühest küljest lubab enamatel makselahenduste pakkujatel turul tegutseda, teisalt on seatud

maksevahendajatele kõrgendatud turvameetmete standard hõlmates endas tugevaid klientide autentimise meetmeid, mis peaks aitama vähendada toime pandud pettuste arvu (Euroopa Keskpank 2021). See kõik aitab võidelda kelmuste levikuga ja kuritegelikul teel teenitud raha peitmise ja legaliseerimisega.

Üks viis, kuidas võidelda rahapesu ja terrorismi rahastamisega ning skeemide levikuga, on koostöö erinevate osapoolte vahel. Näiteks osaleb RAB (RAB - Rahapesu Andmebüroo) rahvusvahelises projektis, mille eesmärk on ühendada eri riikide rahapesu andmebüroode teadmised ja praktika, et koondada lähenemisviisid piiriüleste rahapesuvoogude võrgustike ja mustrite tuvastamiseks ning töötada välja vahendeid, millega hõlbustada rahapesu tõkestamist. Välisriikidega tehakse koostööd ka rahajälje jälitamisel. RAB-il on võimalik esitada päringuid teiste riikide rahapesu andmebüroodele, et saada lisainfot kahtlaste tehingute kohta ning vajaduse korral seada välisriigis olevale varale käsutuspiirang. Välisriikidest päringutega sisse tulev info võib omakorda olla abiks Eesti finantssüsteemi ära kasutavate skeemide ja kurjategijate tuvastamisel. (Rahapesu Andmebüroo 2021) Rahvusvahelise koostöö tulemusena suudeti näiteks 2020. aasta septembris kinni pidada Rumeenias tegutsenud kolmeliikmeline rühmitus, keda kahtlustati õngitsuste läbiviimisel, mille tagajärjel üritati ohvrite kontodelt ära kanda üle 150 000 euro. Peale vahistamist saabus mõneks nädalaks pangaõngitsuste rindele kuu aega kestnud vaikus, kuid oktoobri lõpus hakkasid need taas levima. (Riigi Infosüsteemi Amet 2021)

Olulisel kohal on ka siseriiklik koostöö RAB-i ja kohustatud isikute vahel ning kahesuunaline teabevahetus õiguskaitseasutustega seoses rahapesu või terrorismi rahastamise või nendega seotud kuritegudega. Selliselt üles ehitatud operatiivse koostöö tulemusel on Rahapesu Andmebürool olnud võimalik piirata püüdeid kuritegelikku päritolu vahendeid kiiresti edasi toimetada ning need on kriminaalmenetluses arestitud. Lisaks sellele saadavad kohustatud isikud RAB-ile infot rahapesukahtlusega tehingute ja tegevuste kohta, mida koosöös Kaitsepolitseiametiga analüüsitakse järgmiste sammude planeerimiseks. (Rahapesu Andmebüroo 2021) Õngitsusründe korral teavitab RIA (RIA – Riigi Infosüsteemi Amet) intsidentide käsitlemise osakond veebimajutajat, kelle serveris õngitsusleht asub, ja palub selle eemaldada. 2020. aastal tuvastati küberruumi seire või mõne intsidendi lahendamise käigus mitmeid seni teadmata turvanõrkusi, millest teavitati toote omanikku või teenusepakkujat ja puudused eemaldati enne, kui suurem kahju jõudis sündida. Näiteks avastati

selliseid veebilehti, mis ei kontrollinud ID-kaardiga autentimisel kaardi sertifikaadi kehtivust või kas sertifikaat on SK ID Solutionsi poolt allkirjastatud. See tähendab, et kasutaja saanuks nendesse teenustesse logida ükskõik kellena ning võtta näiteks võõra inimese nimel kiirlaenu. (Riigi Infosüsteemi Amet 2021)

1.5.2. Tehnoloogilised võimalused

Kuigi teenusepakkujatel ja tarbijatel endil on väga suur vastutus turvalisuse tagamisel ja pettuste katsete tuvastamisel, on innovatiivsetel digilahendustel on üha suurem roll ebatavaliste tehingute tuvastamises. Vastutustundlik finantsinnovatsioon võimaldab aidata kaasa rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamisele. Ühe lahendusena on välja pakutud AI-põhiste (AI – *artificial intelligence*) tööriistade rakendamist, mis võimaldavad reaalajas, kiiret ja täpsemat andmete analüüsi. AI jäljendab inimese mõtlemisvõimet, et täita ülesandeid, mis tavaliselt nõuavad inimesele omast intelligentsust, nagu näiteks mustrite tuvastamine, soovituste tegemine või otsuste langetamine kasutades selleks täiustatud arvutustehnikaid ning erinevatest allikatest pärinevaid struktureeritud ja struktureerimata andmeid. On olemas mitut tüüpi tehisintellekte, mis töötavad erineva autonoomsustaseme juures. (Financial Action Task Force 2021)

Üks AI alamliike on masinõpe, mis õpetab arvutisüsteeme minimaalse inimsekkumisega andmetest õppima, mustreid tuvastama ja otsuseid langetama kasutades selleks eelnevaid kogemusi ja mustrituvastusalgoritme. Masinõppe suurimaks eeliseks on võime õppida olemasolevatest süsteemidest vähendades vajadust manuaalse monitoorimise järgi, vähendada valepositiivseid tulemusi, tuvastada keerulisi juhtumeid ning hõlbustada riskijuhtimist. Sarnaseid lahendusi kasutatakse kaarditehingute monitoorimisel. Algoritmide abil õpivad pangasüsteemid tundma kaardivaldaja varasemat ostukäitumist ning ühtlasi võetakse arvesse ka hilisemaid ja ajutisi kulutamisharjumusi. Pettus fikseeritakse siis, kui tuvastatakse oluline kõrvalekalle kaardivaldaja tavapärasest kaardi kasutamisest. (Nami, Shajari 2018) Seetõttu peetakse usaldusväärseks selliseid pettuste tuvastamise lahendusi, mis on õppimisvõimelised ning ei anna välja valehäireid aegunud andmete põhjal. Valehäiretega tegelemine on kaardiorganisatsioonidele kulukas, kuid ka kliendile piirav. Et petturid võivad tegutseda mitmel moel, näiteks tehakse kas ühekordseid suuri tehinguid või mitu väiksemat tehingut, peaksid süsteemid olema arendatud selliselt, et need suudaksid eristada petturlikke tehinguid kaardivaldaja poolt tehtud tehingutest. (Panigrahi *et al.* 2009)

1.5.3. Tarbijate teadlikkuse suurendamine

Kuna paljud skeemid toimuvad ohvri enda osalusel (nt paroolide sisestamisel), siis üksnes automatiseeritud lahendustest ei piisa ning pangad ei saa võtta täielikku vastutust klientide vara eest, mistõttu on oluline kasvatada klientide teadlikkust pettustest läbi teadmiste juhtimise ja jagatud vastutuse. (Barker 2018) Kõige enam tuleb panustada kõrgendatud riskirühma kuuluvate inimeste juhendamisele. Potentsiaalsed ohvrid peaksid (Drew, Farrell 2018):

- olema suutelised riske tuvastama;
- mõistma, milliste meetmetega on neil võimalik kelmustega võidelda;
- omama pettustega võitlemiseks tehnilist võimekust;
- mõistma, miks nad riskirühma kuuluvad.

Küberpettuste alases hariduses tuleks ühendada tehnoloogiliste teadmiste ja nö „pehmete teadmiste" rakendamine, mis adresseeriks ühtlasi riskide keerukust ja mitmekesisust. Politseil peaks olema küberpettustega võitlemisel eelkõige ennetav roll (*Ibid*.) On leitud, et meeldetuletuste ja hoiatuste kasutamine ennetava meetmena on igati õigustatud eriti just vanemaealiste inimeste puhul. (O'Connor *et al.* 2021) Olulisel kohal on ka IT süsteemide turvalisuse tagamine, mille eest vastutavad nii tarbijad, regulaatorid kui ka teenusepakkujad. Teenusepakkujad peaksid uuendama kaitsemehhanisme ja enda kliente harima. Regulaatorite ülesanne on pakkuda koostööd võimaldavat platvormi, kus teenusepakkujad saaksid jagada enda kogemusi rünnakutega ja arutada omavahel süsteemide nõrku kohti. Lisaks sellele tuleks tarbijaid harida, et nad ei jagaks internetis oma andmeid tundmatutele isikutele. (Ali *et al*. 2019) „Ei, aitäh!" kampaanialehel on kättesaadavad viited Eesti pankade veebilehtedele, mis sisaldavad finantspettuste eest hoiatavat informatsiooni. Neis on toodud välja peamised pettuste liigid, millised on ohumärgid ja kuidas pettuse kahtluse korral käituda. (Eesti Pangaliit 2021) 2019. aastal viis RIA läbi kampaania „Ole IT-vaatlik", mis oli suunatud inimeste teadlikkuse tõstmisele digihügieenist. Kampaania veebilehel on kättesaadavad soovitused küberturvalisuse tõstmiseks nii eraisikutele, ettevõtetele kui ka avalikule sektorile. (Riigi Infosüsteemi Amet 2019)

Tarbijad langevad ohvriteks enamasti manipuleerimise ja seadmete haavatavuse tulemusena. Küberkurjategijad kasutavad tavaliselt mitut identiteeti ning oskavad võltsida legitiimsete institutsioonide, nagu näiteks pankade, sotsiaalkindlustusameti ja maksuameti identiteete. (Ali *et al.* 2019) Manipuleerimisründe puhul kasutavad kurjategijad sageli autoritaarsust. Et meie ühiskond on

autoritaarsusele üles ehitatud, on sellist tüüpi manipuleerimisrünnetega keeruline võidelda. Manipuleerimisründega võitlemise meetmetesse tuleks kaasata neli aspekti: protsessid, keskkond, tehnoloogia ja inimeste käitumine. (Bullée *et al.* 2018) Vaatamata sellele, et veebikeskkonnas on kasutajate identiteet erinevate meetmetega kindlaks tehtav, ei ole inimesed kursis nende meetmete toimimisega, mistõttu teadmatus on see, mis võib õngitsuse ja manipuleerimisründe ohvrite arvu suurendada. Enamgi veel, tänapäeval on telefonivõrgustikud (mobiiltelefon, lauatelefon ja internetikõned) saanud üheks kõige eelistatumaks suhtluskanaliks nii era- kui tööelus, mida kurjategijad osavalt ära kasutavad. Telefonivõrgustikku kasutatakse sageli isikliku informatsiooni jagamiseks, näiteks pangad identifitseerivad kliente telefoni teel. Telefonivõrgustikku peetakse küll turvaliseks, kuid kasutajal ei ole võimalik kindlaks teha, kes on teisel pool telefonitoru. (Ali *et al.* 2019)

Tarbijate teadlikkuse tõstmine erinevate institutsioonide koostöö tulemusena aitab tarbijaid kaitsta küberkuritegude eest. (Ali *et al*. 2019). Et enamasti kasutatakse kuritegude toimepanemisel pankade infrastruktuuri, on teadlikkuse tõstmises olulisel kohal pankadepoolne proaktiivne kommunikatsioon petuskeemide ja nende ennetamise viiside kohta (Barker 2020). Pankade pettuste ennetamise meetmed ja nende kommunikeerimine võimaldavad parandada kliendisuhete kvaliteeti, luua pikaajalisi ja lojaalseid kliendisuhteid ja suurendada kliendi kasumlikkust. Pettuste ennetamise kommunikeerimisel tuleks enam tähelepanu pöörata just vanemaealisele kliendigrupile, kuna nad on pettuste ennetamise meetmete suhtes enamasti skeptilisemad kui nooremad kliendid. Selleks, et luua tugevaid kliendisuhteid, peaksid pangad veenma kliente tegema nendega koostööd pettuste vähendamise eesmärgil, kuna hästi informeeritud kliendid avaldavad väiksema tõenäosusega konfidentsiaalset infot ning oskavad väärtustada panga püüdlusi neid pettuste eest kaitsta. (Hoffmann, Birnbirch 2020)

Üks inimrühm, kellele tuleks pettuste ennetamisel tähelepanu pöörata, on korduvohvrid, kuna nemad on tõenäoliselt halvasti kursis veebiturvalisusega seonduva infoga. Kuna ohvrid, eriti korduvohvrid on reeglina kiirelt tegutsevad elamusi otsivad inimesed, siis peaksid veebilehed (e-poed, kohtingusaidid jne) olema disainitud selliselt, et kasutaja oleks sunnitud kontrolle läbi viima. Ohvreid iseloomustab ka impulsiivne käitumine, mistõttu peab pettuste ennetamise kohta käiv informatsioon olema kokkuvõtlik, hästi ligipääsetav ja kaasahaarav. Üksnes skeemide olemasolust informeerimine ei pruugi muuta küberturbega seotud käitumist. Selle asemel võiksid veebilehed jagada praktilisi

nõuandeid selle kohta, mida kasutajad peavad enda kaitsmiseks tegema, millele erilist tähelepanu pöörama, milliseid täiendavaid kontrolle tegema ja kuidas pettuse avastamisel edasi tegutseda. Oluline on, et inimesed oskaksid teha vahet autentsel ja ebausaldusväärsel informatsioonil. (Whitty 2019) Ennetustöö keskmes peaks olema isiku reageerimine raha ja isikuandmete küsimusele petturi poolt, mitte niivõrd erinevate stsenaariumite tutvustamine. Ohvrid on enamasti kursis petuskeemide levikuga, kuid pettuse katse korral ei ole nad suutnud seost luua hoiatava informatsiooni ning reaalse ohuolukorra vahel. Teiseks, kelmid ei tegutse alati täpselt ettekirjutatud mustri järgi, vaid korrigeerivad enda suhtlust selliselt, et nad saaksid ohvrilt võimalikult suure hulga raha kätte. (Cross, Kelly 2016)

Eelnevat kokku võttes võib öelda, et inimeste harimisel küberpettustest tuleb tähelepanu pöörata mitmele asjaolule. Ühest küljest kaitsevad finantsasutusi ja tarbijaid rahvusvahelised seadused ning mitmete institutsioonide igapäevane tegevus pettuse katsete takistamisel ning tuvastamisel, kuid väga palju saab enda kaitseks ära teha lõpptarbija ise. Selleks, et lõpptarbija oleks suuteline ise ennast kaitsma, peavad tal olema piisavad teadmised ohtudest ja digihügieenist. Et kurjategijate skeemid muutuvad sama kiiresti, kui tehnoloogia meie ümber, siis peab tarbijateni jõudev info olema ajakohane, kättesaadav ja lihtsasti omandatav. Pettustega tegelemisel on suurem efekt nende ennetamisel, mitte hilisemate kahjudega tegelemisel, kuna kaotatud raha tagasi saamine on keerukas ning alati jääb võimalus, et ohver on enda varast lõplikult ilma jäänud põhjustades talle seeläbi nii emotsionaalset kahju kui ka viies ta rahaliselt haavatavasse olukorda.

2. METOODIKA

Käesoleva magistritöö käigus püütakse selgitada välja pettustealase kommunikatsiooni märgatavus ja selle mõju pettuste tuvastamisele oskusele. Andmete kogumiseks viidi läbi veebiküsitlus Google Forms keskkonnas. Küsimustikku jagati sotsiaalmeedias ning sellele oodati vastuseid alates 4. märtsist kuni 19. märtsini 2022. aastal. Küsimustik koosnes 16 valikvastusega küsimustest ning ühest avatud küsimusest. Küsimustik koostati tuginedes McGuire HOE mudelile, mida on varasemalt kasutanud Bauman *et al.* (2008), Craig, Bauman ja Reger-Nash (2009) ja Kite *et al.* (2018) selleks, et selgitada välja terviseedenduskampaaniate mõju inimeste tervisekäitumisele. Kampaania hindamiseks on sõnastatud kampaania sisendmuutujad, vahemuutujad ja kampaania tulemus.

Küsimuste koostamisel ja muutujate sõnastamisel lähtuti Kite *et al.* (2018) HOE mudeli tõlgendustest, kus mõõdeti kampaania tulemusi viie teineteisele järgneva sammu abil, milleks olid teadlikkust kampaaniast, kampaaniasõnumi mõistmine, suhtumine ja sotsiaalsed normid seoses tervisekäitumisega, enesehinnang ning kavatsused seoses tervislikuma eluviisi rakendamisega ning vastaja hinnang tehtud muudatusele tervisekäitumises. Analoogselt on „Ei, aitäh!“ kampaania hindamisel kaheks esimeseks sammuks teadlikkus kampaaniast ning kampaaniasõnumi mõistmine. Sellele järgnevad info kogumine, teadlikkus pettustest ja küberturbest ning kaitsemeetmete rakendamine. Muutujad on kohandatud vastavalt „Ei, aitäh!“ kampaania sisule, eesmärgile ning magistritöö uurimisküsimustele. (Tabel 4)

Tabel 4. Muutujad "Ei, aitäh!" kampaania hindamiseks

HOE samm	Muutuja	Küsimuse nr	Skaala
teadlikkus kampaaniast	kampaania märkamine	8	jah, ei
kampaaniasõnumi mõistmine	meenutamine, milliste pettuste liikide eest kampaania hoiatas	9a	jah, ei
	teadlikkus finantspettustest on suurenenud tänu kampaaniale	11	4p Likerti skaala
	oskus pettuse katse tuvastada	10a	4p Likerti skaala
	oskus pettuse korral ohumärke tuvastada	10b	4p Likerti skaala
	teadmine, mida teha pettuse tuvastamise korral	10c	4p Likerti skaala
	teadmine, mida teha kahju kannatamise korral	10c	4p Likerti skaala
info kogumine	allikad, kust saadakse infot pettuste kohta	7	mitu vastusevarianti
	kampaania veebilehe külastamine	9b	jah, ei
	kodupanga vastava veebilehe külastamine	9c	jah, ei
	enda lähedastega rääkimine pettuste teemal	9d	jah, ei
teadmised pettuste liikidest ja küberturbest	millist tüüpi pettused osatakse enda hinnangul ära tunda	13a-f	4p Likerti skaala
	millist tüüpi pettuseid on tuvastatud	14a-f	4p Likerti skaala
kaitsemeetmete rakendamine	andmete turvalisusele tähelepanu pööramine	13a	4p Likerti skaala
	seadmete turvalisusele tähelepanu pööramine	13b	4p Likerti skaala
	oskus tunda ära investeerimispettuse ohumärgid	13c	4p Likerti skaala
	oskus ära tunda telefonipettuse ohumärgid	13d	4p Likerti skaala
	oskus ära tunda õngitsuspettuse ohumärgid	13e	4p Likerti skaala
	oskus ära tunda püramiidiskeemi ohumärgid	13f	4p Likerti skaala
	oskus ära tunda armu- või pärimispettuse ohumärgid	13g	4p Likerti skaala

Allikas: autori koostatud tuginedes Bauman *et al.* (2008) ja Kite *et al.* (2018)

Küsimustik koosnes kolmest plokist. Esimene plokk (küsimused 1-5) koosnes küsimustest vastaja sotsiaaldemograafiliste tunnuste kohta (vanus, sugu, rahulolu enda finantsolukorraga, haridustase ja keelteoskus) Seejärel küsiti pangateenuste kasutamise kohta (küsimus 6) ning millistest allikatest on seni saadud infot finantspettuste kohta (küsimus 7). Plokk lõppes küsimusega „Ei, aitäh!“ kampaania mäletamise kohta (küsimus 8). Kui vastaja mäletas kampaaniat, avanes teine plokk „Ei, aitäh!“

kampaaniat puudutavate küsimustega (küsimused 9-11). Kolmas plokk koosnes küsimustest pettustega kokkupuutumise kohta (küsimused 12 ja 14), pettuste tuvastamise enesehinnangu kohta (küsimused 13 ja 15c-g) ja kaitsemeetmete rakendamise kohta (küsimus 15a ja 15b), sealhulgas kas ja millise pettuse tagajärjel on kannatatud kahju (küsimus 16). Ehkki „Ei, aitäh!“ kampaania keskendus teadlikkuse tõstmisele investeerimis- ja telefonipettuste kohta, küsiti lisaks teiste levinud pettuste, nagu õngitsuspettuse, püramiidiskeemi ning armu- ja pärimispettuse tuvastamise kohta. Kõikidele küsimustele vastamine oli kohustuslik, välja arvatud viimasele küsimusele, milles paluti nimetada, millise pettuse ohvriks on vastaja langenud. Vastajatel paluti valida vastusevariantide „ei“ ning „jah“ vahel, valida etteantud variantidest üks vastusevariant või märkida mitu vastusevarianti. Enamikele küsimustele paluti vastata Likerti 4p skaalal. Küsimustik on leitav Lisas 1.

Küsitlusele vastas kokku 107 inimest. Enim vastanuid oli vanuserühmades 25-34 (36%) ning 45-54 (21%). 79% vastanutest olid naised. Enda finantsolukorda pidasid pigem mitterahuldavaks 24%, pigem rahuldavaks 59% ning rahuldavaks 17%. Viimase lõpetatud haridustaseme osas jagunesid vastajad kaheks: 48% oli kesk- ja/või kutseharidusega ning 52% kõrgharidusega. Enamik vastanutest valdas suhtlustasemel vähemalt ühte võõrkeelt ning kuus inimest märkis ainsana eesti keele. Valdav enamus vastajaid kasutab pangateenuste kasutamiseks mobiilipanka (92%) või internetipanka (87%). „Ei, aitäh!“ kampaaniat mäletas 35% vastanutest. (Tabel 5)

Tabel 5. Valim

Tunnus		Arv	Osakaal
vanus	18-24	17	16%
	25-34	38	36%
	35-44	16	15%
	45-54	22	21%
	55-…	14	13%
sugu	mees	22	21%
	naine	85	79%
rahulolu finantsolukorraga	ei ole rahul	0	0%
	pigem ei ole rahul	26	24%
	pigem olen rahul	63	59%
	olen väga rahul	18	17%
haridus	põhiharidus	0	0%
	kutseharidus ja/või keskharidus	51	48%
	kõrgharidus	56	52%
keelteoskus	ainult eesti keel	6	6%
	inglise keel	90	84%
	vene keel	55	51%
	muu	16	15%
enim kasutatavad pangakanalid	mobiilipank	98	92%
	internetipank	93	87%
	muu	5	5%
on märganud "Ei, aitäh!" kampaaniat	jah	37	35%
	ei	70	65%

Allikas: autori koostatud kogutud andmete põhjal

Tulemusi analüüsiti vanuserühmade, haridustasemete ning kogu valimi lõikes. Analüüsist jäeti välja võrdlus sugude alusel, kuna mehi oli vastanute seas alla 30. Samal põhjusel ei analüüsitud igat vanuserühma eraldi, vaid liideti vanuserühmad 18-24 ja 25-34 ning 35-44, 45-54 ja üle 55-aastased. Vanuserühmas 18-34 oli vastanuid 55 ning vanuserühmas 35-... oli vastanuid 52. Eraldi ei analüüsitud vastuseid ka finantsolukorraga rahulolu põhjal, kuna finantsolukorraga rahul olevaid inimesi oli valimis 18 ja pigem mitte rahulolevaid 26.

Andmete analüüsimiseks kasutati MS Excel programmi ning Real Statistic tööriista. Kõiki 107 vastust oli võimalik analüüsis kasutada. Kõigepealt andmed korrastati ning Likerti skaala väärtused kodeeriti numbrilisteks väärtusteks: 1 – ei nõustu, 2 – pigem ei nõustu, 3 – pigem nõustun, 4 – nõustun, 0 – ei

oska öelda. Uuringus osalejate vastused koondati risttabelitesse, mille abil võrreldi erinevate sihtrühmade antud vastuseid. Seose pettustega kokkupuute, turvameetmete rakendamise ning pettuse tuvastamise oskuse enesehinnangu vahel on leitud korrelatsioonanalüüsiga kasutades selleks Spaermani korrelatsioonikordajat (ρ). Olulisuse tõenäosuse (*p-value*) piiriks loeti 0,05, ehk kui olulisuse tõenäosus oli väiksem kui 0,05, loeti seos statistiliselt ebaoluliseks.

Kvantitatiivset uurimisviisi otsustati kasutada vastajate anonüümsuse tagamiseks. Kvalitatiivse uurimisviisi rakendamise eelduseks oleks olnud pettuste ohvrite leidmine, mis oleks osutunud keerukaks magistritöö teema delikaatsuse tõttu. Kvalitatiivne uurimisviis oleks olnud sobilik üksikjuhtumite analüüsimiseks, kuid käesoleva magistritöö eesmärk oli mõista pettustealase kommunikatsiooni märgatavust ja teadlikkust pettustest erinevate sihtrühmade lõikes, mistõttu otsustati küsitluse ja kvantitatiivse meetodi kasuks.

3. TULEMUSTE ANALÜÜS

3.1. Kampaania märgatavuse analüüs

Pangaliidu finantskelmuste eest hoiatavat kampaaniat „Ei, aitäh!“ mäletas 37 inimest ehk 35% kõikidest vastanutest. Kampaania märgatavus oli 15% võrra kõrgem vanemas vanuserühmas võrreldes noorema vanuserühmaga ning 24% võrra kõrgem kõrgharidustega inimeste hulgas võrreldes kesk- või kutseharidusega inimestega. (Tabel 6)

Tabel 6. Kampaania mäletamine vanuserühmade ja haridustasemete lõikes

Demograafiline tunnus	"Ei, aitäh!" kampaaniat mäletanute osakaal
18-34-aastased	27%
üle 35-aastased	42%
kesk- või kutseharidus	22%
kõrgharidus	46%

Allikas: autori koostatud kogutud andmete põhjal

Nendelt, kes mäletasid „Ei, aitäh!“ kampaaniat, küsiti lisaks kampaania tulemusi puudutavaid küsimusi, st milliseks hinnatakse enda finantspettustealaseid teadmisi. 86% vastanutest mäletas, milliste pettuste eest kampaania hoiatas ning 89% on seda infot jaganud enda lähedastega. 62% on külastanud enda kodupanga pettuste eest hoiatavat veebilehte ning 24% on külastanud „Ei, aitäh!“ kampaania veebilehte, mis mõlemad sisaldavad kokkuvõtvat informatsiooni erinevate pettuste liikide kohta. 51% vastanutest pigem nõustus, et nende üleüldised teadmised pettuste kohta paranesid tänu kampaaniale. 24% pigem ei olnud sellega nõus, 16% nõustus täielikult ning 8% ei nõustunud üldse. Pettuste ohumärkide tuvastamise osas olid kampaaniat mäletanud inimesed enesekindlad – 57% vastanutest oli pigem nõus, et suudavad ohumärke tuvastada ja 30% oli sellega täielikult nõus. Sarnaselt hinnati ka enda oskust reaalne pettuse katse tuvastada. 49% olid pigem nõus, et teavad, kuidas pettuse katse korral tegutseda ning 41% oli selles täiesti kindel. Kahju kannatamise korral

tegutsemise oskust hinnati mõnevõrra madalamalt. 41% oli pigem nõus, et teavad, mida teha kahju kannatamise korral, 32% oli täielikult nõus ning 14% sellega pigem ei nõustunud. (Tabel 7)

Tabel 7. Kampaania tulemuste kokkuvõte

Kampaania tulemus		Arv	Osakaal
Kampaania info	mäletab, milliste pettuste eest hoiatas	32	86%
	info kampaania veebilehelt	9	24%
	info kodupangast	23	62%
	info lähedastele	33	89%
Teadlikkuse suurenemine	ei nõustu	3	8%
	pigem ei nõustu	9	24%
	pigem nõustun	19	51%
	nõustun	6	16%
Oskus pettuse ohumärke tuvastada	ei oska öelda	2	5%
	ei nõustu	2	5%
	pigem ei nõustu	0	0%
	pigem nõustun	21	57%
	nõustun	11	30%
Hinnang pettuse katse tuvastamise oskusele	ei oska öelda	1	3%
	ei nõustu	2	5%
	pigem ei nõustu	0	0%
	pigem nõustun	21	57%
	nõustun	12	32%
Oskus pettuse korral õigesti tegutseda	ei oska öelda	1	3%
	ei nõustu	2	5%
	pigem ei nõustu	1	3%
	pigem nõustun	18	49%
	nõustun	15	41%
Oskus kahju kannatamisel õigesti tegutseda	ei oska öelda	2	5%
	ei nõustu	2	5%
	pigem ei nõustu	5	14%
	pigem nõustun	15	41%
	nõustun	12	32%

Allikas: autori koostatud kogutud andmete põhjal

Kui võrrelda kampaaniat mäletanud ja kampaaniat mitte mäletanud inimeste vastuseid andmete ja seadmete turvalisuse tagamise osas, siis kampaaniat mitte mäletanud inimeste seas on rohkem neid, kes on pigem nõus või täielikult nõus väitega turvameetmete rakendamise kohta. (Tabel 8)

Tabel 8. Turvameetmete rakendamine vastavalt kampaania mäletamisele

Kampaania mäletamine	Andmete turvalisus				Seadmete turvalisus			
	ei nõustu	pigem ei nõustu	pigem nõus	nõus	ei nõustu	pigem ei nõustu	pigem nõus	nõus
ei mäleta	0%	5%	43%	46%	0%	14%	43%	41%
mäletab	6%	13%	49%	30%	4%	23%	41%	30%

Allikas: autori koostatud kogutud andmete põhjal

„Ei, aitäh!“ kampaania hoiatas inimesi telefonipettuste eest, aga ka investeerimispettuste eest. Kui võrrelda kampaaniat mäletanud ja kampaaniat mitte mäletanud inimeste vastuseid pettuste tuvastamise enesehinnangu kohta, siis telefonipettuse tuvastamise oskuse osas olulisi erinevusi ei esinenud. Küll aga oli kampaaniat mäletanud inimeste seas 16% enam neid, kes olid kindlad enda oskuses tuvastada investeerimispettus ning 8% vähem neid, kes selle väitega pigem ei nõustunud. (Tabel 9)

Tabel 9. Pettuste tuvastamise oskus vastavalt kampaania mäletamisele

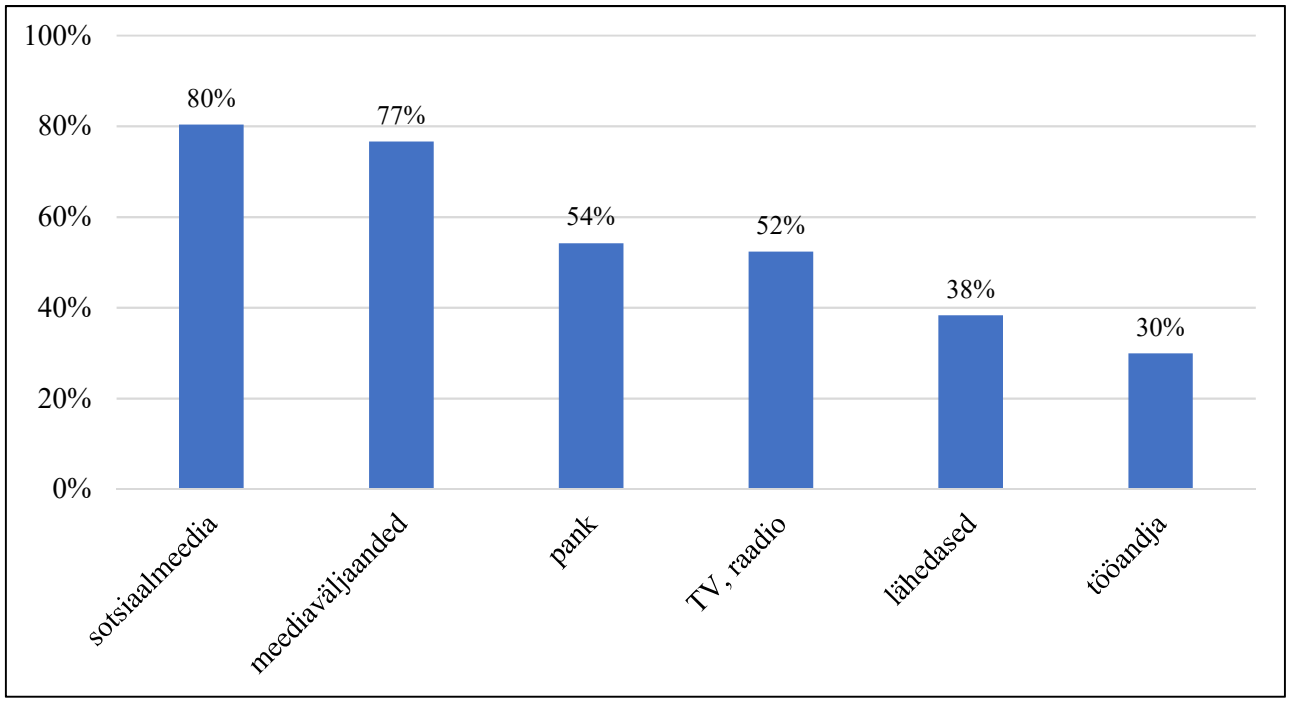
Kampaania mäletamine	Oskus tuvastada investeerimispettus				Oskus tuvastada telefonipettus			
	ei nõustu	pigem ei nõustu	pigem nõus	nõus	ei nõustu	pigem ei nõustu	pigem nõus	nõus
ei mäleta	6%	16%	47%	26%	1%	1%	40%	53%
mäletab	0%	8%	43%	41%	0%	5%	41%	51%

Allikas: autori koostatud kogutud andmete põhjal

Nendest tulemustest saab järeldada, et tänu Pangaliidu kampaaniale tõusid küll inimeste teadlikkus pettustest ning teadmised, mida pettuse avastamise korral teha. Küll aga ei saa väita, et kampaania oleks mõjutanud uuringus osalejaid täiendavalt enda andmete ja seadmete turvalisuse eest hoolitsema, vaid seda tehakse olenemata kampaania mäletamisest. Samuti ei sõltu kampaania mäletamisest oskus tuvastada telefonipettust ega investeerimispettust.

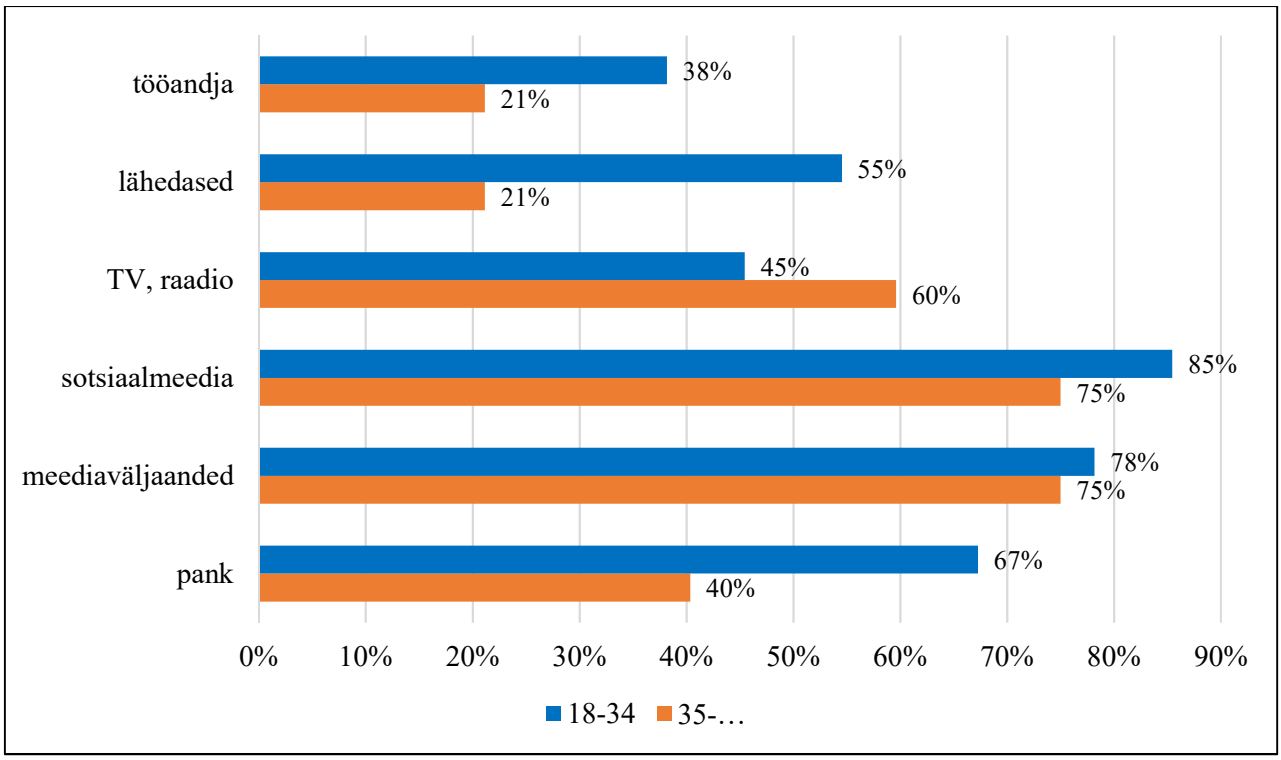
3.2. Pettuste kohta saadava info allikate analüüs

Kõige enam on saanud uuringus osalenud inimesed infot pettuste kohta sotsiaalmeediast ja meediaväljaannetest ning kõige vähem on saadud infot lähedastelt ning tööandjalt. (Joonis 5)



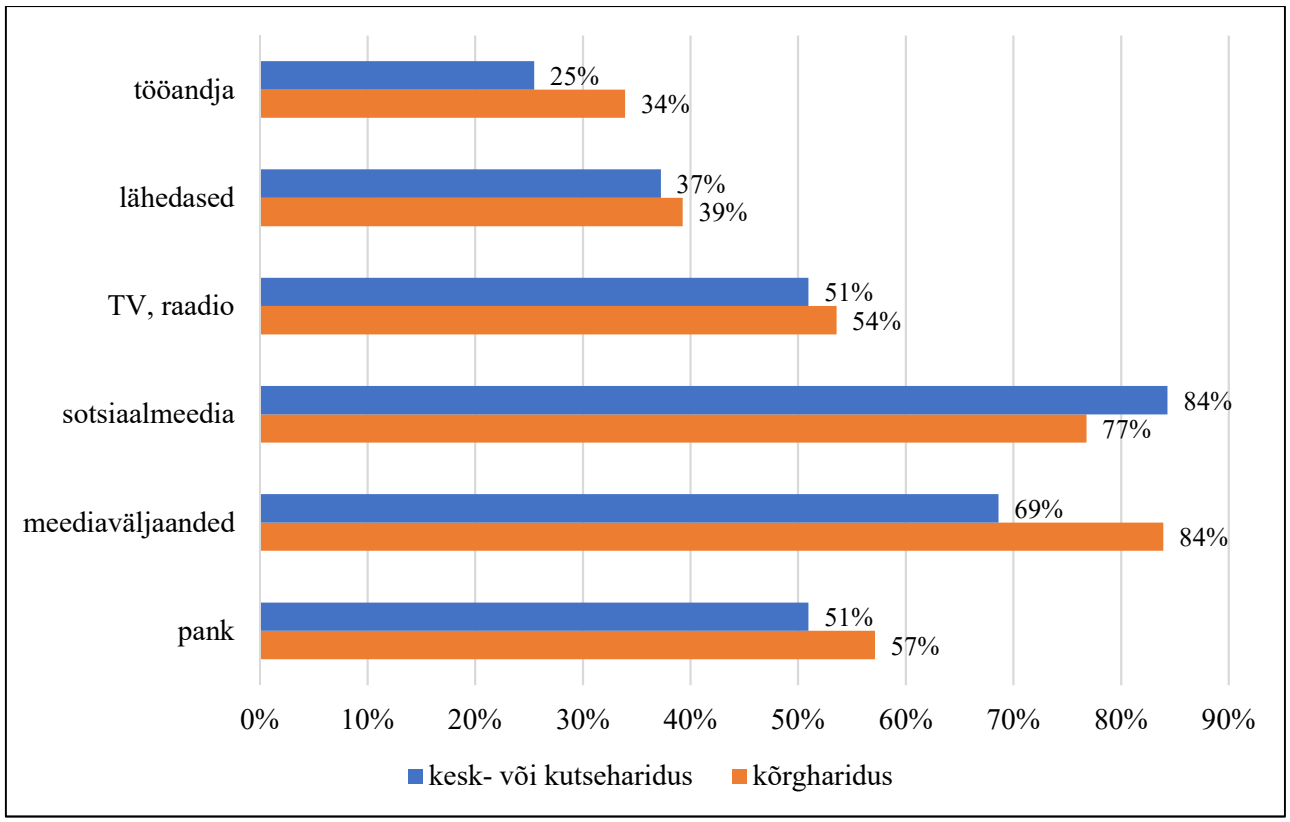
Joonis 5. Pettuste kohta saadava info allikad valimi lõikes
Allikas: autori koostatud kogutud andmete põhjal

Nooremasse vanuserühma kuuluvad uuringus osalenud on saanud pettuste kohta infot enamatest allikatest võrreldes vanemasse vanuserühma kuuluvate inimestega. Nooremate inimeste hulgas on 34% enam neid, kes on saanud infot pettuste kohta lähedastelt, 27% võrra enam neid, kes on saanud infot pangast, 17% võrra enam neid, kes on saanud infot tööandjalt ja 10% võrra enam neid, kes on saanud infot sotsiaalmeediast. Seevastu üle 35-aastaste hulgas oli võrreldes noorematega 15% võrra enam neid, kes on saanud pettuste kohta infot televisioonist ja raadiost. (Joonis 6)



Joonis 6. Pettuste kohta saadava info allikad vanusegruppide lõikes
Allikas: autori koostatud kogutud andmete põhjal

Kõrgharidusega uuringus osalejad on saanud keskharidusega vastanutega võrreldes pettuste kohta infot enamatest allikatest. Lähedastelt ning televisioonist ja raadiost on saadud haridustasemete lõikes infot sarnasel määral. Meediaväljaannetest on saanud infot pettuste kohta 15% rohkem ning tööandjalt 9% rohkem kõrgharidusega inimesi võrreldes keskharidusega uuringus osalejatega. Küll aga on keskharidusega inimeste hulgas rohkem neid, kes on saanud pettuste kohta infot sotsiaalmeediast. (Joonis 7)



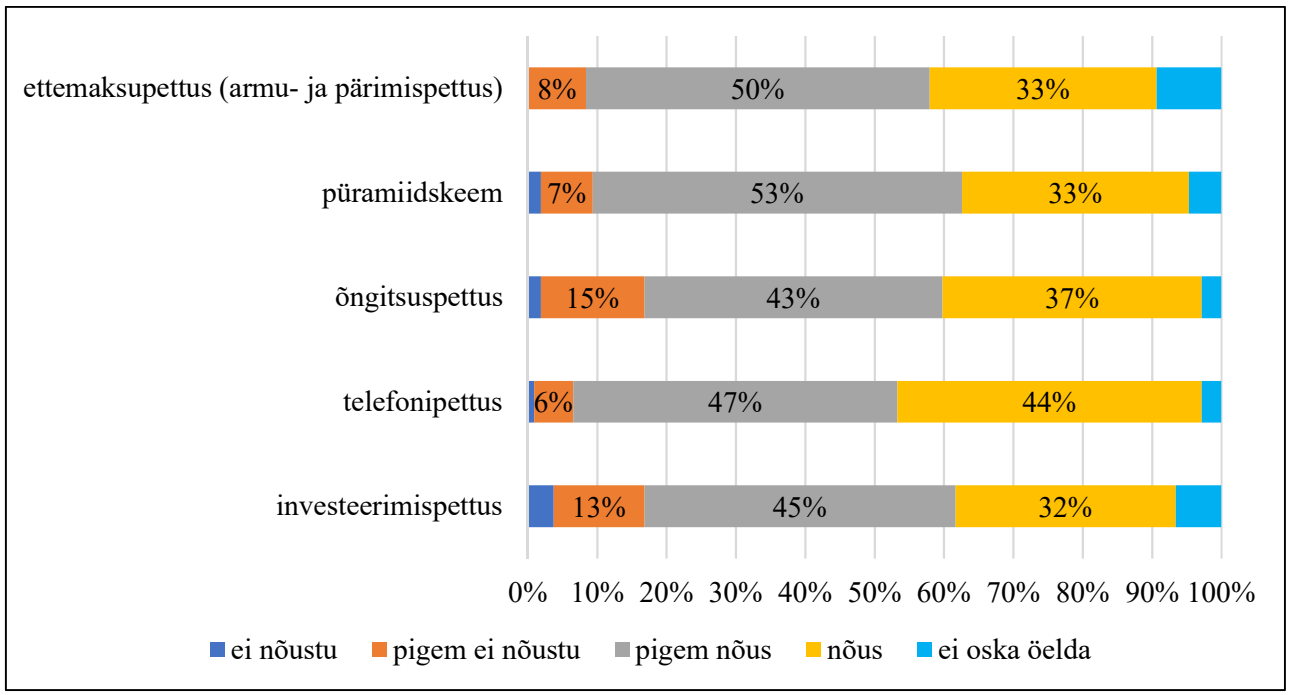
Joonis 7. Pettuste kohta saadava info allikad haridustasemete lõikes
Allikas: autori koostatud kogutud andmete põhjal

Sotsiaalmeedia ja meediaväljaanded on peamised allikad, kust on saadud infot pettuste kohta olenemata vastajate demograafilistest tunnustest. Nooremate inimeste jaoks on teised olulised infoallikad olnud lähedased, pank ja tööandja ning vanemate inimeste jaoks televisioon ja raadio. Kõrgharidusega inimesed on saanud võrreldes keskharidusega inimestest sagedamini infot meediaväljaannetest ning pangast ja keskharidusega inimesed sotsiaalmeediast.

3.3. Tuvastatud pettuste analüüs

Enamus küsitlusele vastanutest teab enda hinnangul, millised ohumärgid viitavad pettustele. Kõige enesekindlamad ollakse telefonipettustele viitavate ohumärkide tuvastamisel, mille puhul 44% vastanutest olid kindlad enda oskuses need ära tunda. Õngitsuspettuse ja investeerimispettuse

ohumärkide tuvastamise osas oli kõige enam inimesi kahtleval seisukohal (vastavalt 15% ja 13%) (Joonis 8)



Joonis 8. Pettustele viitavate ohumärkide tuvastamise enesehinnang
Allikas: autori koostatud kogutud andmete põhjal

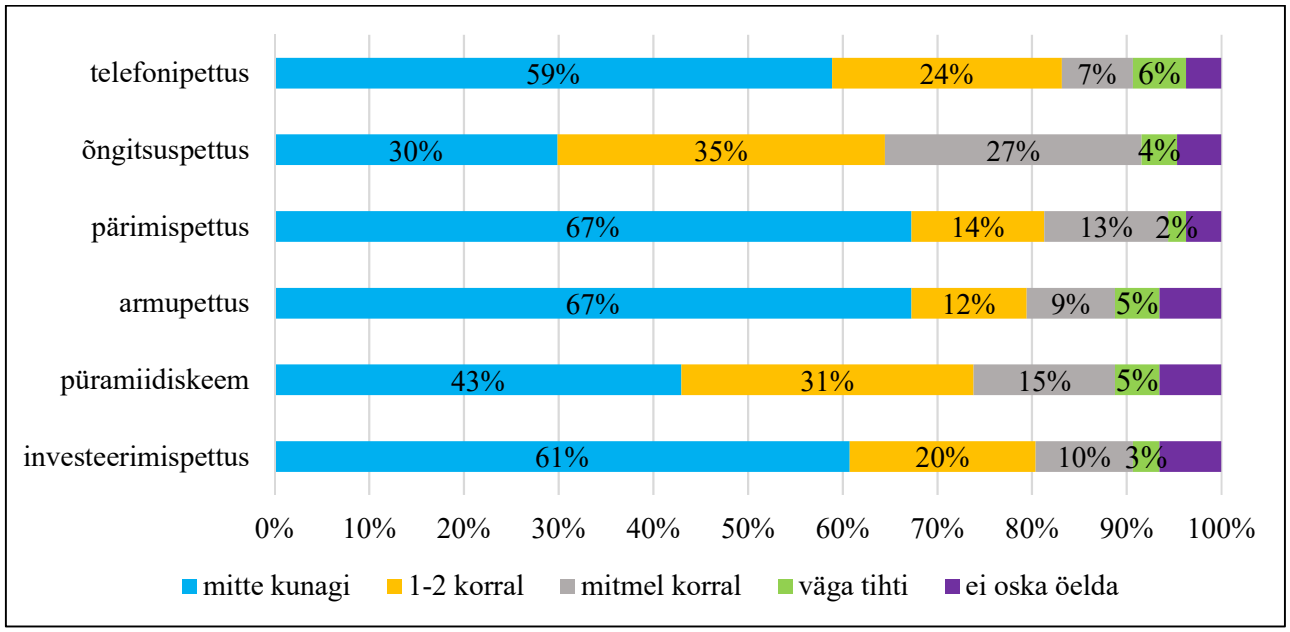
Pettustega on enim kokku puututud e-kirja kaudu. Sellele järgnevad telefonikõne, sotsiaalmeedia, internet ja SMS. 12% vastanutest ei ole pettusega kokku puutunud ning neli vastanut on kokku puutunud petturiga näost-näkku kohtumisel. (Tabel 10)

Tabel 10. Pettusega kokkupuute kanalid

Pettusega kokkupuute kanal	Arv	Osakaal
e-kiri	74	69%
telefonikõne	51	48%
sotsiaalmeedia	43	40%
internet	36	34%
SMS	26	24%
kokkupuude puudub	13	12%
näost-näkku	4	4%

Allikas: autori koostatud kogutud andmete põhjal

Enamusel vastanutest on olnud vähemalt ühel korral pettusega kokkupuude. Kõige harvem on vastanud olnud ettemaksupettuste, s.o. pärimispettuse ning armupettuse sihtmärkideks. Sellele järgnevad kokkupuude investeerimispettusega ja telefonipettusega. Kõige sagedamini on vastanud olnud püramiidiskeemi ning õngitsuspettuse sihtmärkideks. Õngitsuspettusega on ühel või kahel korral kokku puutunud 35% vastanutest ning enamatel kordadel 31% vastanutest. Püramiidiskeemidega on ühel või kahel korral olnud kokkupuude 31% vastanutest ning enamatel kordadel 20% vastanutest. (Joonis 9)



Joonis 9. Kokkupuude erinevate pettustega
Allikas: autori koostatud kogutud andmete põhjal

Eri tüüpi pettustega kokkupuude erineb vanuserühmade lõikes, kuid vähemalt korra on pettusega kokku puututud mõlemas vanuserühmas. Investeerimispettusega on kokku puutunud sagedamini vanemad inimesed. Seevastu nooremate hulgas on 5% neid, kes on investeerimispettusega kokku puutunud korduvalt. Sarnane tendents esineb ka püramiidiskeemiga kokkupuutel, millega vanemad inimesed on sagedamini kokku puutunud kui nooremad. Korduvalt ja väga tihti on püramiidiskeemiga kokkupuude olnud mõlemal vanuserühmal peaaegu võrdselt, kuid nooremate hulgas mõnevõrra rohkem.

Ka armupettustega on vanematel inimestel olnud kokkupuudet rohkem kui noorematel inimestel. 15% vanemasse vanuserühma kuuluvatest inimestest on armupettusega kokku puutunud paaril korral ja 12% korduvalt. Nooremas vanuserühmas on armupettusega kokku puutunud paaril korral 9% vastanutest ja korduvalt 7% vastanutest. Pärimispettusega on 4% vanematest inimestest kokku puutunud väga tihti, paaril korral või korduvalt on pärimispettusega kokkupuudet esinenud nooremas ja vanemas vanuserühmas võrdselt.

Vanemad inimesed on õngitsuspettusega kokku puutunud pigem harva, samas nooremate inimeste seas on rohkem neid, kes on õngitsuspettusega kokku puutunud väga tihti. Telefonipettustega on kokku puutunud pigem nooremad uuringus osalejad. Mõlemas vanuserühmas oli umbes üks neljandik neid, kes on telefonipettusega kokku puutunud paaril korral, kuid noorte seas on 11% neid, kes on sellega kokku puutunud korduvalt ja 11% on kokku puutunud telefonipettusega väga tihti. Vanemate inimeste seas oli 4% neid, kes on telefonipettusega kokku puutunud korduvalt, kuid mitte keegi sellest vanuserühmast ei ole telefonipettusega kokku puutunud väga tihti. (Tabel 11)

Tabel 11. Tuvastatud pettused vanuserühmade lõikes

Pettuse liik	Sagedus	18-34	35-…
investeerimispettus	jah, 1-2 korral	16%	23%
	korduvalt	5%	15%
	väga tihti	5%	0%
püramiidiskeem	jah, 1-2 korral	24%	38%
	korduvalt	16%	13%
	väga tihti	5%	4%
armupettus	jah, 1-2 korral	9%	15%
	korduvalt	7%	12%
	väga tihti	4%	6%
pärimispettus	jah, 1-2 korral	13%	15%
	korduvalt	13%	13%
	väga tihti	0%	4%
õngitsuspettus	jah, 1-2 korral	33%	37%
	korduvalt	24%	31%
	väga tihti	5%	2%
telefonipettus	jah, 1-2 korral	22%	27%
	korduvalt	11%	4%
	väga tihti	11%	0%

Allikas: autori koostatud kogutud andmete põhjal

Haridustasemete lõikes on eri tüüpi pettustega kokkupuude erinev. Kõrgharidusega uuringus osalejate seas on 23% investeerimispettusega paaril korral kokku puutunud ning keskharidusega inimeste seas on investeerimispettusega paaril korral kokku puutunud 16%, seevastu korduvalt on investeerimispettusega kokku puutunud pigem keskharidusega inimesed. Püramiidiskeemiga kokkupuude on sarnane investeerimispettusega kokkupuutele.

Armupettusega on korduvalt või väga tihti kokku puutunud rohkem keskharidusega inimesed, kellest 14% on armupettusega kokku puutunud korduvalt, samal ajal kui kõrgharidusega inimeste seas on korduvat kokkupuudet esinenud 5% vastanutest. Pärimispettusega on korduvalt olnud kokkupuude 16% keskharidusega inimestest ning väga tihti 4% kõrgharidusega inimestest. Õngitsuspettusega on paaril korral kokku puutunud 18% rohkem kõrgharidusega inimesi. Telefonipettusega on kokku puutunud korduvalt 16% keskharidusega inimestest ning mitte ükski kõrgharidusega inimestest, samas kõrgharidusega inimeste seas on rohkem neid, kes on telefonipettusega kokku puutunud väga tihti. (Tabel 12)

Tabel 12. Tuvastatud pettused haridustasemete lõikes

Pettuse liik	Sagedus	Kesk- või kutseharidus	Kõrgharidus
investeerimispettus	jah, 1-2 korral	16%	23%
	korduvalt	14%	7%
	väga tihti	2%	4%
püramiidiskeem	jah, 1-2 korral	27%	34%
	korduvalt	18%	13%
	väga tihti	2%	7%
armupettus	jah, 1-2 korral	12%	13%
	korduvalt	14%	5%
	väga tihti	8%	2%
pärimispettus	jah, 1-2 korral	14%	14%
	korduvalt	16%	11%
	väga tihti	0%	4%
õngitsuspettus	jah, 1-2 korral	25%	43%
	korduvalt	29%	25%
	väga tihti	4%	4%
telefonipettus	jah, 1-2 korral	24%	25%
	korduvalt	16%	0%
	väga tihti	4%	7%

Allikas: autori koostatud kogutud andmete põhjal

Pettustega puututakse kokku peamiselt erinevates digitaalsetes kanalites ning kõige enam on uuringus osalejad tuvastanud õngitsuspettuse katse. Vanematel inimestel olnud sagedasem kokkupuude investeerimispettustega, armupettustega ja püramiidiskeemiga. Seevastu nooremate inimeste hulgas on võrreldes vanemate inimestega rohkem neid, kes on investeerimispettusega kokku puutunud väga tihti. Nooremate inimeste hulgas on olnud rohkem kokkupuudet telefonipettustega. Kui võrrelda pettustega kokkupuudet haridustasemete lõikes, siis kõrgharidusega vastanute hulgas on rohkem neid, kes on eri tüüpi pettustega kokku puutunud paaril korral, samal ajal kui keskharidusega inimesed on pettuseid tuvastanud korduvalt. Väga tihti on kõrgharidusega inimesed kokku puutunud investeerimispettusega, püramiidiskeemiga, pärimispettusega ja telefonipettusega ning keskharidusega inimesed on väga tihti kokku puutunud rohkem armupettusega.

3.4. Turvameetmete rakendamise analüüs

Uuringus osalenud inimesed pööravad võrdselt tähelepanu nii enda andmete kui ka seadmete turvalisusele, kuid andmekaitsest ollakse mõnevõrra rohkem teadlikud. Kui andmete turvalisusele pigem ei pööra tähelepanu 10% vastanutest, siis seadmete turvalisusele pigem ei pööra tähelepanu 20% vastanutest. (Tabel 13)

Tabel 13. Andmete ja seadmete turvalisuse tagamine

Väärtus	Tähelepanu pööramine andmete turvalisusele		Tähelepanu pööramine seadmete turvalisusele	
	arv	osakaal	arv	osakaal
ei nõustu	4	4%	3	3%
pigem ei nõustu	11	10%	21	20%
pigem nõustun	50	47%	45	42%
nõustun	38	36%	36	34%
ei oska öelda	4	4%	2	2%

Allikas: autori koostatud kogutud andmete põhjal

Keskharidusega vastanute seas on neid, kes ei pööra enda andmete ega seadmete turvalisusele tähelepanu, erinevalt kõrgharidusega vastanutest. Keskharidusega inimeste seas on võrreldes kõrgharidusega vastanute hulgas rohkem neid, kes turvameetmete rakendamise osas on kahtleval

seisukohal ehk pigem sellega ei nõustu. Kõrgharidusega vastanute hulgas on rohkem neid, kes pigem nõustuvad turvameetmete rakendamisega. Andmete turvalisusele pigem pöörab tähelepanu 15% ja seadmete turvalisusele 17% enam kõrgharidusega vastanuid. Nii andmete kui seadmete turvalisuse tagamisega oli täielikult nõus mõnevõrra rohkem keskharidusega inimesi võrreldes kõrgharidusega inimestega. (Tabel 14)

Tabel 14. Andmete ja seadmete turvalisuse tagamine haridustasemete lõikes

Haridustase	Andmete turvalisus				Seadmete turvalisus			
	ei nõustu	pigem ei nõustu	pigem nõus	nõus	ei nõustu	pigem ei nõustu	pigem nõus	nõus
kesk- või kutseharidus	8%	16%	39%	37%	6%	24%	33%	37%
kõrgharidus	0%	5%	54%	34%	0%	16%	50%	30%

Allikas: autori koostatud kogutud andmete põhjal

Nii nooremad kui ka vanemad inimesed pööravad andmete ja seadmete turvalisusele tähelepanu, kuid nooremasse vanuserühma kuulunud küsitlusele vastanud on andme- ja seadmekaitsest mõnevõrra rohkem teadlikud. Nooremas vanuserühmas oli 13% võrra enam neid, kes andmekaitse tagamisega täielikult nõustusid ning 13% võrra enam neid, kes seadmekaitse tagamisega täielikult nõustusid. Vanemas vanuserühmas vastas 10% võrra enam inimesi, et nad pigem ei nõustu andmete turvalisuse tagamisega ja 7% võrra enam neid, kes pigem ei nõustu seadmete turvalisuse tagamisega. Mõlemas vanuserühmas on enamus märkinud, et nad pigem nõustuvad nii andmete kui ka seadmete turvalisusele tähelepanu pööramisega. (Tabel 15)

Tabel 15. Andmete ja seadmete turvalisuse tagamine vanuserühmade lõikes

Vanus	Andmete turvalisus				Seadmete turvalisus			
	ei nõustu	pigem ei nõustu	pigem nõus	nõus	ei nõustu	pigem ei nõustu	pigem nõus	nõus
18-34	5%	5%	45%	42%	4%	16%	38%	40%
35-…	2%	15%	48%	29%	2%	23%	46%	27%

Allikas: autori koostatud kogutud andmete põhjal

Andmete turvalisuse tagamise ning armupettusega ja telefonipettusega kokkupuute vahel leiti nõrk positiivne seos. Nõrk positiivne seos leiti ka seadmete turvalisuse tagamise ning armupettusega,

telefonipettusega ja õngitsuspettusega kokkupuute vahel. Selgus, et oskus pettus tuvastada on seotud varasema pettuse kogemusega. Püramiidiskeemi ja pärimispettuse tuvastamise oskuse ning nendega varasema kokkupuute vahel leiti keskmise tugevusega positiivne seos, teiste pettuste liikide korral tuvastati nõrk positiivne seos. Analüüsimisel on kasutatud Spaermani korrelatsioonikordajat (ρ). Olulisuse tõenäosuseks (*p-value*) loeti 0,05. (Tabel 16)

Tabel 16. Seos pettustega kokkupuute, turvameetmete rakendamise ning pettuse tuvastamise oskuse enesehinnangu vahel

Tuvastatud pettuse liik	Andmete turvalisus (ρ)	*p-value*	Seadmete turvalisus (ρ)	*p-value*	Hinnang oskusele pettus tuvastada (ρ)	*p-value*
investeerimispettus	0,16	0,206	0,17	0,186	0,29	0,003
püramiidiskeem	0,04	0,982	0,14	0,122	0,45	0,000
armupettus	0,21	0,027	0,23	0,027	0,37	0,000
pärimispettus	0,13	0,151	0,15	0,102	0,43	0,000
õngitsuspettus	0,08	0,581	0,22	0,031	0,29	0,000
telefonipettus	0,23	0,043	0,27	0,007	0,25	0,004

Allikas: autori koostatud kogutud andmete põhjal

Selgus, et andmete ja seadmete turvalisuse eest kantakse hoolt olenemata sellest, kas pettusega on varasem kokkupuude või mitte, ehkki kokkupuude armupettusega, õngitsuspettusega ja telefonipettusega võib tekitada vajaduse täiendavaid turvameetmeid rakendada. Turvameetmeid rakendatakse rohkem kõrgharidusega inimeste hulgas ning nooremas vanuserühmas. Teadlikkus pettustest ja hinnang oskusele pettus tuvastada on seotud varasema pettuse kogemusega, seda eriti püramiidiskeemi ja õngitsuspettuse puhul. Kõige vähem on seotud investeerimispettuse ja telefonipettuse tuvastamise oskus ning varasem kokkupuude nendega, mis võib tähendada, et vastanud on nende pettuste kohta hästi informeeritud.

Pettuse tagajärjel oli kahju kannatanud kokku seitse inimest, kellest neli kannatas rahalist kahju ning kolm moraalset kahju, sealhulgas kaks inimest oli kannatanud nii moraalset kui ka rahalist kahju. Kõik kahju kannatanud olid naised. Viis kannatanut oli keskharidusega ja kaks kõrgharidusega. Kolm

kannatanut hindasid enda finantsolukorda pigem mitterahuldavaks, kolm inimest pigem rahuldavaks ja üks rahuldavaks. Kõik kannatanud valdasid vähemalt ühte võõrkeelt, kellest neli valdas inglise keelt, kuus vene keelt ja kaks soome keelt. Kannatanutest üks inimene mäletas „Ei, aitäh!“ kampaaniat. Kahju kannatanud on kõige enesekindlamad telefonipettuste tuvastamisel ning vähem enesekindlad investeerimispettuse ja õngitsuspettuse tuvastamisel. Eri liiki pettuseid on tuvastatud ühel või kahel korral, kuid telefonipettust on kogetud enamatel kordadel. Kahju kannatanud uuringus osalejad pööravad tähelepanu nii oma andmete kui ka seadmete turvalisusele ning enamasti teavad enda hinnangul, millised tunnused ühel või teisel pettuse liigil esinevad. Pettused, mille tagajärjel kahju kannatati, olid laenupettus, lähisuhtega seotud pettus, armupettus ja „kõne pangast“ pettus.

4. ARUTELU

4.1. Pangaliidu kampaania märgatavus

Erinevat tüüpi finantspettustega kokkupuude on saanud tavapäraseks. Nii nagu inimeste töö- ja eraelu, nii on ka kelmid kolinud enda tegevusega digikeskkonda ning kasutavad mitmesuguseid meetmeid, et pääseda ligi andmetele ja finantsvarale. Antud uuringus osalejatest on 88% pettusega vähemalt ühel korral kokku puutunud. Ajal, mil telefonipettuste ja investeerimispettuste toimepanek suurenes järsult, viis Pangaliit läbi kampaania „Ei, aitäh!“, et teavitada inimesi nende pettustega seonduvatest ohtudest ning jagada informatsiooni selle kohta, kuidas pettus tuvastada ja kuidas kahju kannatamise korral käituda. Kampaania sõnumit levitati televisioonis, raadio- ja trükimeedias, otsepostituste brošüürides ning internetis (Politsei- ja Piirivalveamet 2021). „Ei, aitäh!“ kampaaniat mäletas küsitlusele vastanutest üks kolmandik, kellest enamus mäletas, milliste pettuste eest kampaania hoiatas ning on pettustest rääkinud enda lähedastega. Vähem uuriti ise pettuste kohta juurde, st külastati kodupanga või kampaania veebilehekülge. Kampaaniat mäletanud inimesed olid enesekindlad oskuses tuvastada pettuse katse, pettusele viitavate ohumärkide tundmises ning teadsid, mida teha pettuse tuvastamise korral. Mõnevõrra vähem tunti kindlust selles osas, mida teha siis, kui ollakse kannatanud pettuse tagajärjel kahju. Kampaania mäletamise osakaal oli kõrgem vanemate inimeste hulgas ning kõrgharidusega inimeste hulgas.

Kui analüüsida „Ei, aitäh!“ kampaaniat McGuire HOE mudeli (Bauman *et al.* 2008; Craig, Bauman ja Reger-Nash 2009; Kite *et al.* 2018) raamistikus, mille kohaselt toob kampaania märkamine kaasa muutused inimeste käitumises, siis antud juhul ei saa järeldada, et kampaania oleks mõjutanud inimeste oskust erinevaid pettusi tuvastada ega see ei ole neid motiveerinud pöörama tähelepanu enda andmete ja seadmete turvalisusele. Sellele vaatamata on kampaania sõnumit mõistetud, teatakse, kust vajadusel informatsiooni nende kohta juurde leida ning ollakse teadlikud pettuste liikidest ja küberturbest üleüldiselt. „Ei, aitäh!“ kampaania küll aitas teatud sihtrühmade puhul kaasa teadlikkuse

suurendamisele, kuid inimesed saavad infot pettuste kohta mitmest erinevast allikast, tänu millele ollakse pettustega seonduvaga hästi kursis.

Pettuste eest hoiatav kampaania tuleks läbi viia siis, kui pettustest on saanud laiem probleem ning tekib vajadus inimesi nendest ohtudest teavitada. Tuginedes varasematele uuringutele ning käesoleva magistritöö analüüsi tulemustele, on pikaajalist perspektiivi silmas pidades oluline inimesi järjepidevalt koolitada ning pöörata info jagamisel tähelepanu enamlevinud pettuste ohumärkidele, millele lisaks tuleb rõhutada andmekaitse ja kübeturbe olulisust. Seejuures tuleb kommunikatsiooni kohandada vastavalt erinevate sihtrühmade interneti kasutamise harjumustele ning enim kasutatavatele suhtluskanalitele, arvestada eri liiki pettuste ohvriks langemise riski sihtrühmade lõikes ning üleüldiseid trende pettuste leviku osas. Lisaks sellele peab hoiatav informatsioon olema alati nähtaval kohal kanalites, kus on suur pettusega kokkupuute risk. Eraldi tuleb pöörata tähelepanu inimeste juhendamisele selles osas, kuidas käituda pettuse katse tuvastamise korral ning juhtida tähelepanu elektrooniliste suhtluskanalite turvalisuse tagamise meetmetele jt andmekaitsega ja kübertubrega seotud teemadele. Petuskeemid on alati sammu võrra kaitsemeetmete rakendamisest ees, seega tuleks tõsta inimeste teadlikkust eelkõige ennetusmeetmete osas.

4.2. Pettuste kohta saadava info allikad

Olenemata vastajate demograafilistest tunnustest saadakse pettuste kohta kõige sagedamini informatsiooni sotsiaalmeediast ja meediaväljaannetest ning kõige harvem tööandjalt. Vanemate inimeste jaoks on olulised infoallikad veel televisioon ja raadio ning nooremate inimeste jaoks suhtlus lähedastega ja pank. Selles vanuserühmas, kus kampaania mäletamise osakaal oli kõrgem, on televisiooni ja raadio roll infoallikana olulisem. Võrreldes keskharidusega inimestega saavad kõrgharidusega inimesed infot meediaväljaannetest rohkem kui sotsiaalmeediast ja vastupidi.

Nagu selgub, saadakse infot pettuste kohta samaaegselt mitmest allikast. Vaatamata sellele, et kõik küsitlusele vastanud kasutavad pangateenuste kasutamiseks digikanaleid, on pettuste kohta saanud infot pangast pooled uuringus osalejatest. Finantsasutuste infrastruktuuri nõrkusi kasutavad petturid ära kuritegelikul teel raha teenimiseks ning raha liigutamiseks lõplikke kasusaajateni, mis muudab

finantsasutused pettuste suhtes eriti haavatavaks. Finantsasutused koostöös järelvalveorganitega on välja töötanud erinevaid meetmeid ja protsesse, et kahjude teket ennetada ja tabada kelmuste taga olevaid kuritegelikud organisatsioonid, kuid kuna enamasti teeb pettuse toimepaneku võimalikuks ohvri inimlik eksimus, siis osa vastutusest jääb inimeste endi kanda. Küll aga saavad finantsasutused teha palju selleks, et nende klientidel oleksid olemas vajalikud teadmised ja tööriistad pettuste tuvastamiseks ja kahju ennetamiseks. Oskus enda finantsseisundit juhtida ning baasteadmised investeerimismaailma toimimisest aitaksid inimestel paremini tuvastada petturlikud investeerimisvõimalused jt kiiret rikastumist võimaldavad pakkumised ja ennetada seeläbi ohvriks langemist. Noorematele vanuserühmadele suunatud kommunikatsioonis tuleks rõhutada internetis riskikäitumisega seonduvaid ohte (nt pangakaardi andmete leke) ning vanemaid inimesi hoiatada internetis tegutsevate kelmide eest, kes potentsiaalsete ohvritega otse ühendust võtavad.

Tööandjatel on võrreldes meediaväljaannetega ja sotsiaalmeediaga pettustealases teavitustöös suhteliselt väike roll. Pettuste kohta said infot tööandjalt nooremad ning kõrgharidusega uuringus osalenud. Nii nagu eraelu, on ka üha enam digitaliseeruv töökeskkond avatud erinevatele manipuleerimis- ja küberrünnakutele, mille tõttu on vajalik tööandjatel enda töötajaid järjepidevalt digivaldkonnas koolitada ja muuta seeläbi ettevõtete äriprotsessid turvalisemaks. Ettevõtetel on võimalus rakendada mitmesuguseid meetmeid andmete ja ärisaladuste kaitsmiseks, kuid sellele vaatamata jääb võimalus kannatada pettuse katse tagajärjel kahju kas teadmatusest või lohakusest, mistõttu peaks lisaks süsteemide ja seadmete hooldamisele pöörama võrdväärselt tähelepanu töötajate harimisele. Küberturbega ja manipuleerimisrünnetega seotud koolitused ja õppused peaksid ettevõtetes olema olulisel kohal olenemata ettevõtte suurusest, keerukusest või tegevusalast, kuna tänapäeval on kõik ettevõtted vähemal või rohkemal määral rünnete suhtes haavatavad. Ühtlasi aitaks töötajate koolitamine kaasa üleüldisele teadlikkuse suurenemisele pettuste ja nende tuvastamise kohta, kuna kelmid võivad kasutada sarnaseid võtteid nii ettevõtetelt kui ka üksikisikutelt informatsiooni ja finantsvarade hankimiseks.

4.3. Teadlikkus pettustest

Antud uuringus osalejate seas oli teadlikkus pettustest kõrge. Küsitlusele vastanud olid enesekindlad enda oskuses tuvastada reaalses ohuolukorras eri liiki pettused ning teavad enda hinnangul, millised ohumärgid üht või teist tüüpi pettusele viitavad. Püramiidiskeemi ja õngitsuspettuse tuvastamsie hinnang oli võrreldes teiste pettuste liikidega enam seotud sellega, kas nende pettustega on varasem kokkupuude või mitte. Tulles tagasi „Ei, aitäh!“ kampaania mõju juurde, siis on kampaania täitnud oma eesmärki investeerimispettuste ja telefonipettuste eest hoiatamisel - uuringus osalejad teavad, kuidas eristada pangatöötaja kõne või investeerimisvõimalus petturlikest kõnedest ja pakkumistest. Vaatamata sellele, et kampaania mäletamine oli uuringus osalejate seas madal, oli pettuste teema hüppeliselt suurenenud kelmuste toimepaneku tõttu ühiskonnas aktuaalne ning leidis palju meediakajastust, mis võib seletada inimeste kõrgemat teadlikkust investeerimispettustest ja telefonipettustest. Seega saab järeldada, et meediakanalite sünergia on oluline pettustealase kommunikatsiooni planeerimisel, kuna inimesed saavad infot paralleelselt mitmest allikast, mis soodustab teadmiste kinnistumist.

Uuringust selgus, et inimesed pööravad rohkem tähelepanu enda andmete turvalisusele kui seadmete turvalisusele. Turvameetmete rakendamisest on teadlikumad nooremasse vanuserühma kuulunud vastanud ning kõrgharidusega vastanud. Leiti nõrk positiivne seos õngitsuspettusega, armupettusega ning telefonipettusega kokkupuute ja kaitsemeetmete rakendamise vahel. Siit võib järeldada, et kaitsemeetmeid rakendatakse sageli ennetava meetmena olenemata sellest, kas pettusega on varasem kokkupuude või mitte. Kui võtta arvesse madalat pettuse tagajärjel kahju kannatanute arvu vastanute hulgas, siis võib eeldada, et senised meetmed on olnud pettuse ohvriks langemise ennetamiseks tõhusad. Siinkohal tuleb meeles pidada, et andmete ja seadmete suhtes kaitsemeetmete rakendamine aitab digiruumis levivate pettuse eest kaitsmisel, mitte selliste pettuste korral, kus kelm võtab ohvriga otse ühendust ning ohver annab talle vabatahtlikult ligipääsu enda arvutisse või jagab enda kohta käivat tundlikku informatsiooni. Teadlikkus pettustest on palju laiem mõiste, kui üksnes oskus tuvastada kahtlasena näivalt aadressilt tulnud e-kiri või ära tunda kelmi poolt tehtud kõne pangast. Kahju tekkimise ennetamiseks tuleb tõsta samaaegselt inimeste finantsalaseid teadmisi, arusaama andmekaitse olulisusest ja digihügieenist ning selgitada, kuidas pettuse katse tuvastamise korral käituda, et ära hoida sarnaseid olukordi tulevikus.

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli selgitada välja pettustealase kommunikatsiooni märgatavus ja teadlikkus pettustest erinevate sihtrühmade lõikes. Magistritöö probleem oli vähene arusaam pettustealase kommunikatsiooni liikumisest erinevate sihtrühmadeni. Analüüsi tulemusena selgitati välja, mil määral on Pangaliidu kampaaniat „Ei, aitäh!“ märgatud, millistest allikatest saadakse infot pettuste kohta ja milliseid pettusi ollakse võimelised enda hinnangul tuvastama.

Selgus, et „Ei, aitäh!“ kampaania märgatavus oli uuringus osalejate seas küllaltki madal, kuid sellele vaatamata on teadlikkus pettustest kõrge, st tuntakse levinumatele pettustele viitavaid ohumärke ning pööratakse tähelepanu enda seadmete ja andmete kaitsele. Pangaliidu kampaania tagajärjel tõusis küll uuringus osalejate teadlikkus telefoni- ja investeerimispettustest, kuid kõrge teadlikkus on pigem seotud pideva teavitustööga erinevates kanalites.

Kampaania märgatavus oli kõrgem vanemate inimeste hulgas, kelle jaoks olid peamisteks infoallikateks televisioon ja raadio, mis olid ühtlasi „Ei, aitäh!“ kampaaniasõnumi levitamise kanalid. Nooremad uuringus osalejad on seevastu infot saanud pigem pangast ning lähedastelt. Enim saadakse pettuste kohta infot sotsiaalmeediast ning meediaväljaannetest olenemata vastanute demograafilistest näitajatest. Seega teadlikkuse suurendamisel ja inimeste harimisel on oluline arvesse võtta eri sihtrühmade interneti kasutamise harjumusi ning info peab olema lihtsasti mõistetav ja hästi kättesaadav, seda eriti kanalites, kus pettustega kokkupuute risk on kõrge. Tööandjate roll pettuste kohta info levitamisel on väike võrreldes teiste allikatega. Tööandjatel võiks olla täna palju olulisem roll teadlikkuse suurendamisel, kuna töökeskkond on haavatav erinevat tüüpi kelmustele ning sageli kasutatakse eraisikute ja ettevõtete puhul sarnaseid meetmeid andmete ja raha hankimiseks.

Enamasti on pettusega kokku puututud e-kirja teel, sotsiaalmeedias ning telefonikõne kaudu ning enim on uuringus osalejatel esinenud kokkupuudet õngitsuspettusega. Vanemad inimesed on

võrreldes noorematega kokku puutunud rohkem investeerimispettusega, armupettusega ja püramiidiskeemiga. Nooremas vanuserühmas paistab silma sage kokkupuude investeerimispettusega ja telefonipettusega. Keskharidusega uuringus osalejad sagedamini pettustega kokku puutunud võrreldes kõrgharidusega osalejatega.

Peamised järeldused:

- Kampaania märgatavus oli madal, kuid sellele vaatamata on teadlikkus eri tüüpi pettuste ja nendele viitavate ohumärkide kohta kõrge.
- Finantspettustealases kommunikatsioonis tuleb rõhutada küberturbe tagamise olulisust ning harida inimesi selles osas, milliste meetmetega on võimalik ennetada pettuse ohvriks langemist.
- Info jagamisel tuleb arvestada eri sihtrühmade interneti kasutamise harjumusi, peamiseid suhtlus- ja infokanaleid, eri tüüpi pettuse ohvriks langemise riski ning digipädevuse taset.
- Oluline on kasutada kommunikatsioonis mitut kanalit samaaegselt ja sõnumi sisu kohandada vastavalt konkreetsele sihtrühmale selliselt, et sõnum oleks meeldejääv.
- Senine kommunikatsioon on olnud tõhus, kuid turvalisuse tagamiseks peab see ka tulevikus olema järjepidev, hoiatav info peab olema vajalikul hetkel nähtav ning see peab olema lihtsasti mõistetav.
- Tööandjad peaksid senisest enam tähelepanu pöörama enda töötajate harimisele pettuste ja küberturbe osas, mis võimaldab tõsta ettevõtte infrastruktuuri turvalisust ja kaitsta nii ettevõtet kui töötajaid rünnete eest. Äriprotsesse tuleks nende meetmetega täiendada.
- Pettustealase kommunikatsiooni tulemusena peaksid suurenema inimeste finantsalased teadmised, arusaam andmekaitse olulisusest ja digihügieenist.

Selle magistritöö tulemusi on võimalik rakendada pettustealase kommunikatsiooni planeerimisel ning ettevõtetes küberturbealaste protsesside täiendamisel. Küsitlust levitati sotsiaalmeedias, mistõttu võib eeldada, et vastanud omavad teatud tasemel digipädevusi. Lisaks kasutavad nad panga teenuseid peamiselt digikanalites. Seega võiks edaspidi sarnasesse uurimusse püüda kaasata ka neid, kes kasutavad pangateenuseid peamiselt kontorivõrgu või kõnekeskuse vahendusel. Lisaks tasub uurida,

kuidas SSE/SME segmendi ettevõtted panustavad enda töötajate digipädevuste arendamisse ja äriprotsesside turvalisuse tagamisse seoses võimaliku pettuste ohuga.

SUMMARY

NOTICEABILITY OF PRECAUTIONARY COMMUNICATION ABOUT FINANCIAL FRAUDS WITH THE EXAMPLE OF THE „NO, THANK YOU!“ CAMPAIGN

Hedi Remm

As a result of financial fraud, both individuals and businesses suffer significant losses. This is despite the fact that both businesses and individuals have been constantly informed about fraud and its various forms. Businesses, including financial institutions and payment service providers, are constantly supplementing their processes and infrastructure with various measures to prevent fraud in order to protect themselves and their customers, but as falling victim to fraud is often the result of human error, it is important to raise people's awareness and increasing their readiness to detect active fraud attempts. In 2021, the number of telephone and investment frauds increased sharply. Driven by this, the Estonian Banking Association conducted a “No, Thank You!” campaign in 2021, which warned people about the “call from the bank” and other frauds. The campaign lasted from August 2021 to the end of September. Despite the fact that committing frauds appear to have decreased, scammers continue to seek opportunities to gain illicit assets through various schemes, the most common of which are various types of phishing, prepayment and investment frauds.

The problem of this master's thesis is the lack of understanding of the flow of fraudulent communication to different target groups. The aim of the master's thesis is to find out the noticeability of fraud-related communication and awareness of frauds by different target groups. The following research questions were formulated:

1) To what extent has Estonian Banking Association campaign been noticed?
2) From what sources do people get information about financial fraud?
3) What kind of frauds do people think they are able to detect?

The research was based on the McGuire HOE (hierarchy of effects) model. The hierarchy is formed by the causal relationship between the source variables of the campaign and the results of the campaign. This model has been tested in the analysis of health promotion campaigns, proving the usefulness of this model in the analysis of public service announcement campaigns. In addition, the theoretical part discussed the nature of communication, McGuire's persuasive communication matrix, the visibility of an advertising campaign and the theory of routine activities. Moreover, an overview of the different types of fraud, fraud prevention measures and factors predicting the fall victim to fraud has been provided.

Quantitative research was used to answer the research questions. Data were collected through anonymous survey. Answers were analyzed using descriptive statistics and correlation analysis. The questionnaire was based on aforementioned HOE model adapted to the purpose of the research and the research questions. The survey was carried out in Estonian language, a total of 107 people responded to the survey. Majority of them have recognized an active fraud attempt, mostly in digital channel. 35% of respondents remembered the campaign, thereby awareness was higher among older age group. Both the impact of the “No, Thank You!” campaign conducted by the Estonian Banking Association and the general awareness of fraud were analyzed.

It was concluded that, regardless of whether the campaign was remembered or not, the awareness of fraud was high among the respondents and they were confident in their ability to detect fraud in a real situation of danger. In most cases, information on fraud is obtained from several sources, the most important sources being social media and media publications. Younger people also get information from the bank and older people from television and radio. Participants in the survey received the least information from the employer. Therefore, employers could play a greater role in raising awareness. In conclusion, it seems that there is no one-size-fits-all solution to raising awareness of frauds as it includes people's financial knowledge, understanding of the importance of data protection and digital hygiene.

The results of this study can be applied to the planning of fraud-related communication and to the improvement of cyber security processes in companies. In the future, a similar study could be conducted among people who use banking services mainly through branch office network or call

center. In addition, it is worth examining how companies in the SSE/SME segment contribute to the development of their employees' digital competencies and to the security of their business processes in relation to the risk of possible fraud.

KASUTATUD ALLIKAD

Algab finantspettuste vastane kampaania „Ei, aitäh!“. Politsei- ja Piirivalveamet. Kättesaadav: https://www.politsei.ee/et/uudised/algab-finantspettuste-vastane-kampaania-ei-aitaeh-2455, 19. jaanuar 2022

Aleroud, A., Zhou, L. (2017). *Phishing environments, techniques, and countermeasures: A survey.* Computers & Security, 68, 160–196.

Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., van Moorsel, A. (2019). *Consumer-facing technology fraud: Economics, attack methods and potential solutions. Future Generation Computer Systems*, 408-427.

Bachmann, T. (2009). *Reklaamipsühholoogia.* Tallinn: Ilo.

Barker, R. (2018). *Knowledge Management to Prevent Fraudulent E-Banking Transactions*. Communitas, 23 (3), 71-86.

Barker, R. (2020). *The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention.* South African Journal of Business Management, 51 (1), 1.

Bauman, A., Bowles, H. R., Huhman, M., Heitzler, C. D., Owen, N., Smith, B. J., Reger-Nash, B. (2008). Testing a Hierarchy-of-Effects Model: Pathways from Awareness to Outcomes in the VERB™ Campaign 2002–2003. *American Journal of Preventive Medicine*, 34 (6), 249-256.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junge, M., Hartel, P. (2018). *On the anatomy of social engineering attacks: A literature-based dissection of successful attacks.* Journal of Investigative Psychology and Offender Profiling, 15 (1), 20-45.

Cohen, L. E., Felson, M. (1979). *Social Change and Crime Rate Trends: A Routine Activity Approach.* American Sociological Review, 44 (4), 588-608.

Copes, H., Kerley, K. R., Huff, R., Kane, J. (2010). *Differentiating identity theft: An exploratory study of victims using a national victimization survey.* Journal of Criminal Justice, 38 (5), 1045-1052.

Cotoc, C.-N., Nitu, M., Scheau, M. C., Cozma, A.-C. (2021). *Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States.* Economic and Financial Crimes, 9(6):120.

Craig, C. L., Bauman, A., B. Reger-Nash, B. (2009). Testing the hierarchy of effects model: ParticipACTION's serial mass communication campaigns on physical activity in Canada. *Health Promotion International*, 25 (1), 14-23.

Cross, C., Kelly, M. (2016). *The problem of "white noise": examining current prevention approaches to online fraud.* Journal of Financial Crime, 23 (4), 806-818.

Deliema, M., Shadel, D., Pak, K. (2020). *Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors*. Journal of Consumer Research, 46 (5) 904–914.

Dens, N., Pelsmacker, P., Goos, P., Aleksandrovs, L., Martens, D. (2018). *How consumers' media usage creates synergy in advertising campaigns*. International Journal of Market Research, 60 (3), 268–287.

Dillard, J. P., Peck, E. (2000). *Affect and Persuasion: Emotional Responses to Public Service Announcements*. Communication Research, 27 (4), 416-495.

Dong, X., Chang, Y., Fan, X. (2017). *Effects of the characteristics of online multimedia synergy on consumers' message acceptance and message response*. Online Information Review, 41 (5), 710-727.

Drew, J. M., Farrell, L. (2018). *Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs*. Police Practice and Research, 19 (6), 537-549.

"Ei, aitäh" kampaania koduleheküIg. Eesti Pangaliit. Kättesaadav: https://eiaitah.ee/, 28. jaanuar 2022

Engels, C., Kumar, K., Dennis, P. (2020). *Financial literacy and fraud detection.* The European Journal of Finance, 26 (4-5), 420-442.

Euroopa Keskpank (2021). *Seventh report on card fraud.* Kättesaadav: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html, 29. jaanuar 2022

Euroopa Komisjon (2017). *Strengthened EU rules to tackle money laundering, tax avoidance and terrorism financing enter into force.* Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1732, 22. jaanuar 2022

Euroopa Komisjon (2020). *Survey on "scams and fraud experienced by consumers".* Kättesaadav: https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf, 10. oktoober 2021

FATF (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. Kättesaadav: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-for-aml-cft.html, 29. jaanuar 2022

Freiermuth, M. R. (2011). *Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting.* Discourse & Communication, 5 (2), 123-145.

Herrero, J., Torres, A., Vivas, P., Hidalgo , A., Rodríguez, F. J., Urueña, A. (2021). *Smartphone Addiction and Cybercrime Victimization in the Context of Lifestyles Routine Activities and Self-Control Theories: The User's Dual Vulnerability Model of Cybercrime Victimization.* International Journal of Environmental Research and Public Health, 18 (7), 3763.

Hoffmann, A. O., Birnbrich, C. (2012). *The impact of fraud prevention on bank-customer relationships. An empirical investigation in retail banking*. International Journal of Bank, 30 (5), 390-407.

Investment Fraud. FBI. Kättesaadav: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/investment-fraud, 15. jaanuar 2022

Johannessen, J.-A. (2021). Main Conclusions: Communication as Social Theory. J.-A. Johannessen (toim), *Communication as Social Theory* (111-116). Bingley: Emerald Publishing Limited.

Jones, K. S., Armstrong, M. E., Tornblad, M. K., Namin, A. S. (2021). *How social engineers use persuasion principles during vishing attacks.* Information & Computer Security, 29 (2), 314-33.

Kadoya, Y., Khan, M. S. (2020). *The rising phenomenon of financial scams: evidence from Japan*. Journal of Financial Crime, 20 (2), 387-396.

Kite, J., Gale, J., Grunseit, A., Li, V., Bellew, W., Bauman, A. (2018). From awareness to behaviour: Testing a hierarchy of effects model on the Australian Make Healthy Normal campaign using mediation analysis. *Preventive Medicine Reports*, 12, 140-147.

Lacey, D., Goode, S., Pawada, J., Gibson, D. (2020). *The application of scam compliance models to investment fraud offending.* Journal of Criminological Research, Policy and Practice, 6 (1), 65-81.

Lastdrager, E. (2014). *Achieving a consensual definition of phishing based on a systematic review of the literature*. Crime Science, 3 (9).

Lasswell, H.D. (1948). The structure and function of communication in society. L. Bryson (toim), *The Communication of Ideas* (37-51). New York: Harper and Row.

Leukfeldt, R., Jansen, J. (2015). *Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands*. International Journal of Cyber Criminology, 9 (2), 173–184.

Lim, J. S., Ri, S. Y., Egan, B. D., Biocca, F. A. (2015). *The cross-platform synergies of digital video advertising: Implications for cross-media campaigns in television, Internet and mobile TV.* Computers in Human Behavior, 48, 463-472.

Lokanan, M. E. (2014). *The demographic profile of victims of investment fraud: A Canadian perspective*. Journal of Financial Crime, 21 (2), 226-242.

McGuire, W. J. (2012). McGuire's Classic Input-Output Framework for Constructing Persuasive Messages. R. E. Rice, A. K. Charles (toim), *Public Communication Campaigns* (133-146). California: SAGE Publications.

McQuail, D., Windahl, S. (2015). *Communication models for the study of mass communications.* Routledge.

Nan, X. (2008). *The Influence of Liking for a Public Service Announcement on Issue Attitude.* Communication Research, 35 (4), 503-528.

Nami, S., Shajari, M. (2018). *Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors*. Expert Systems with Applications, 110, 381-392.

O'Connor, A. M., Judges, R. A., Lee, K., Evans, A. D. (2021). *Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience.* Journal of Elder Abuse & Neglect, 33 (3), 181-205.

O'Keefe, G. J., Reid, K. (1990). *The Uses and Efiects of Public Service Advertising*. Public Relations Research Annual, 2: 1-4, 67-91.

"Ole IT-vaatlik" kampaania koduleheküIg. Riigi Infosüsteemi Amet. Kättesaadav: https://www.itvaatlik.ee/, 28. jaanuar 2022

Panigrahi, S., Kundu, A., Sural, S., Majumdar, A. (2009). *Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning*. Information Fusion, 10 (4), 354-363.

Rahapesu Andmebüroo Aastaraamat 2020-2021

Reurink, A. (2018). *Financial Fraud: A Literature Review*. Journal of Economic Surveys, 32 (5), 1292–1325.

Riigi Infosüsteemi Ameti Küberturvalisuse Aastaraamat 2021

Romberg, A. R., Bennett, M., Tulsiani, S., Simard, B., Kreslake, J. M., Favatas, D., Vallone, D. M., Hair, E. C. (2020). *Validating Self-Reported Ad Recall as a Measure of Exposure to Digital Advertising: An Exploratory Analysis Using Ad Tracking Methodology*. International Journal of Environmental Research and Public Health, 17 (7), 2185.

Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27, 379–423.

Shen, W., Wang, S., Yu, J., Liu, Z., Yuan, Y., Lu, F. (2020). *The influence of advertising creativity on the effectiveness of commercial and public service advertisements: A dual-task study*. Applied Cognitive Psychology, 35 (5), 1308-1320.

Solovei, A., Van den Putte, B. (2020). *The effects of five public information campaigns: The role of interpersonal communication*. Communications, 45 (1), 586-602.

What Are Identity Theft and Identity Fraud? The United States of America Department of Justice. (2021). Kättesaadav: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud, 14. jaanuar 2022

Whitty, M. T. (2013). *The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam*. The British Journal of Criminology, 53 (4), 665-684.

Whitty, M. T. (2019). *Predicting susceptibility to cyber-fraud victimhood*. Journal of Financial Crime, 26 (1), 277-292.

Whitty, M. T. (2020). *Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims.* European Journal on Criminal Policy and Research, 26, 399–409.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H. N. (2020). *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study.* Journal of Computer Information Systems.

LISAD

Lisa 1. Küsimustik

Tere!

Minu nimi on Hedi. Õpin Tallinna Tehnikaülikoolis juhtimise ja turunduse õppekaval ning olen kirjutamas enda magistritööd finantspettustest. Uurimistöö käigus soovin saada teada, kuivõrd on märgatud pettuste eest hoiatavat informatsiooni ning milline on inimeste teadlikkus erinevatest pettustest. Olen sulle väga tänulik, kui vastad allolevale küsimustikule. Küsimustik koosneb peamiselt valikvastustega küsimustest ning vastamine võtab aega umbes 10 minutit. Kõik vastused on anonüümsed ja neid kasutatakse üldistavalt, statistilise analüüsi läbiviimiseks.

JAOTIS 1

1. Palun märkige enda vanus
    a. 18-24
    b. 25-34
    c. 35-44
    d. 45-54
    e. 55-...
2. Palun märkige enda sugu
    a. naine
    b. mees
3. Kuivõrd rahul olete hetkel enda finantsolukorraga?
    1. ei ole üldse rahul
    2. -
    3. -

    4. olen väga rahul
4. Palun märkige enda viimane lõpetatud haridusaste
    a. põhiharidus
    b. keskharidus ja/või kutseharidus
    c. kõrgharidus
5. Palun märkige, milliseid keeli valdate vähemalt suhtlustasemel
    a. inglise keelt
    b. vene keelt
    c. muu
6. Milliseid kanaleid kasutate kõige sagedamini pangateenuste kasutamiseks?
    a. mobiilirakendus
    b. internetipank
    c. klienditoe telefon
    d. pangakontor
    e. muu
7. Millistest allikatest olete saanud infot finantspettuste kohta?
    a. pangast
    b. meediaväljaannetest
    c. sotsiaalmeediast
    d. televisioon, raadio
    e. pereliikmetelt, sõpradelt või tuttavatelt
    f. tööandjalt
    g. mitte kuskilt
    h. muu
8. Pangaliit viis 2021. aastal läbi teavituskampaania "Ei, aitäh!". Kas mäletate sellist kampaaniat?
    a. jah (liikuge küsimuse nr. 9 juurde)
    b. ei (liikuge küsimuse nr. 12 juurde)

JAOTIS 2

9. Meenutades "Ei, aitäh!" kampaaniat, palun märkige, milliste järgnevate väidetega nõustute ja millistega mitte.

   Vastusevariandid: jah, ei

   a. Mäletan, milliste pettuste eest kampaania hoiatas
   b. Olen külastanud kampaania veebilehte
   c. Olen külastanud enda kodupanga pettuste eest hoiatavat veebilehte
   d. Olen rääkinud finantspettuste teemal enda lähedastega

10. Meenutades "Ei, aitäh!" kampaaniat, kuivõrd nõustute järgnevate väidetega?

    Vastusevariandid: ei nõustu üldse, pigem ei nõustu, pigem nõustun, ei oska öelda

    a. Sain teada, millised ohumärgid viitavad pettusele
    b. Oskan pettuse katse ära tunda, kui olen sattunud sihtmärgiks
    c. Tean, kuidas pettuse avastamise korral tegutseda
    d. Tean, mida teha siis, kui olen kannatanud kahju

11. Kas nõustute, et tänu "Ei, aitäh!" kampaaniale tõusis teie teadlikkus finantspettustest?

    1. ei nõustu üldse
    2. -
    3. -
    4. nõustun täielikult

JAOTIS 3

12. Millistes kanalites olete tuvastanud pettuse katse?

    a. e-kiri
    b. SMS
    c. sotsiaalmeedia
    d. internet (bännerid, otsingumootori tulemused jne)
    e. telefonikõne
    f. näost-näkku kohtumine

g. kokkupuude puudub
h. muu

13. Kas oskaksite enda hinnangul ära tunda järgnevad pettused?

Vastusevariandid: ei nõustu üldse, pigem ei nõustu, pigem nõustun, ei oska öelda

a. investeerimispettus
b. püramiidiskeem
c. armupettus
d. pärimispettus
e. andmete õngitsemine
f. "Kõne pangast" tüüpi pettus

14. Kas olete viimase aasta jooksul ära tundund mõne järgnevatest pettustest ehk kas olete olnud kelmidele sihtmärgiks?

Vastusevariandid: ei, mitte kunagi, jah, ühel või kahel korral, jah, mitmel korral, jah, seda on juhtunud väga tihti, ei oska öelda

a. investeerimispettus
b. püramiidiskeem
c. armupettus
d. pärimispettus
e. andmete õngitsemine
f. "Kõne pangast" tüüpi pettus

15. Kuivõrd nõustute järgnevate väidetega?

Vastusevariandid: ei nõustu üldse, pigem ei nõustu, pigem nõustun, ei oska öelda

a. Olen viimasel ajal rohkem tähelepanu pööranud enda andmete turvalisusele
b. Olen viimasel ajal rohkem tähelepanu pööranud enda seadmete turvalisusele
c. Tean, millised tunnused viitavad investeerimispettusele
d. Tean, millised tunnused viitavad telefonipettusele
e. Tean, millised tunnused viitavad õngitsuspettusele
f. Tean, millised tunnused viitavad püramiidiskeemile
g. Tean, millised tunnused viitavad armu- või pärimispettusele

16. Kas olete kannatanud finantspettuse tagajärjel kahju?

Vastusevariandid: jah, ei, ei oska öelda

a. Olen kannatanud rahalist kahju
b. Olen kannatanud moraalset kahju

17. Palun nimetage, millise pettusega oli tegu

Lisa 2. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina Hedi Remm

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

„Finantskelmuste eest hoiatava kommunikatsiooni märgatavus „Ei, aitäh!“ kampaania näitel“,

mille juhendaja on Algis Perens,

1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2 üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

---

10. mai 2022

[1] *Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. jq 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.*